



ユーザーガイド

AWS License Manager



AWS License Manager: ユーザーガイド

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

Amazon の商標とトレードドレスは、Amazon 以外の製品またはサービスとの関連において、顧客に混乱を招いたり、Amazon の名誉または信用を毀損するような方法で使用することはできません。Amazon が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

Table of Contents

とは何ですか 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
開始	8
設定	8
にサインアップする AWS アカウント	8
管理アクセスを持つユーザーを作成する	9
License Manager の使用を開始する	10
License Manager の使用	11
セルフマネージドライセンス	12
パラメータとルール	13
ベンダーライセンスからのルールの作成	15
セルフマネージドライセンスを作成する	16
セルフマネージドライセンスを共有する	18
セルフマネージドライセンスを編集する	22
セルフマネージドライセンスを非アクティブ化する	23
セルフマネージドライセンスを削除する	24
ライセンスルール	24
セルフマネージドライセンスと AMI の関連付け	25
セルフマネージドライセンスと AMI の関連付けの解除	27
使用状況レポート	27
使用状況レポートの作成	27
使用状況レポートの編集	29
使用状況レポートの削除	29
ライセンスタイプ変換	30
適格なライセンスタイプ	31
前提条件	40
ライセンスタイプを変換する	43
テナンシー変換	53
トラブルシューティング	55
リソースグループをホストします	56
ホストリソースグループの作成	57

ホストリソースグループの共有	58
ホストリソースグループへのDedicated Hostsの追加	58
ホストリソースグループのインスタンスを起動する	59
ホストリソースグループの変更	60
ホストリソースグループからの Dedicated Host の削除	60
ホストリソースグループを削除します。	61
インベントリ検索	61
インベントリ検索の使用	62
インベントリの自動検出	68
ライセンスの付与	70
付与されたライセンスを表示する	71
付与されたライセンスを管理する	71
使用権限を配布する	75
権限の受理とアクティベーション	76
ライセンスステータス。	79
購入者アカウントのメトリクス	80
販売者が発行したライセンス	81
使用権限管理	82
ライセンス使用量	82
要件	83
出品者が発行したライセンスの作成	85
顧客へのライセンスの付与	86
AWSアカウントを使用せずに顧客の一時的な認証情報を入手する	87
使用ライセンス	88
販売者が発行したライセンスの削除	89
ユーザーベースのサブスクリプション	89
前提条件	91
考慮事項	94
対応ソフトウェア	95
開始	98
ディレクトリ設定の変更	109
VPC 設定の変更	110
ユーザーの関連付けを解除する	110
ユーザーの登録解除	111
インスタンスを終了する	111
ディレクトリの削除	112

トラブルシューティング	113
Linux サブスクリプション	115
検出を管理する	116
インスタンスを表示する	121
請求情報	123
使用状況メトリクスとアラーム	124
設定	128
マネージドライセンス	128
Linux サブスクリプション	130
ユーザーベースのサブスクリプション	130
委任された管理者	131
ダッシュボード	136
License Manager のモニタリング	138
CloudWatch によるモニターリング	138
CloudWatch アラームの作成	140
CloudTrail を使用した API コールのログ記録	140
CloudTrailのLicense Manager情報	141
ライセンスLicense Managerのログ・ ファイルエントリーについて	142
セキュリティ	143
データ保護	144
保管中の暗号化	145
ID およびアクセス管理	145
ユーザー、グループ、ロールを作成する	145
IAM ポリシーの構造	146
License Manager の IAM ポリシーを作成する	147
ユーザー、グループ、およびロールに許可を付与する	148
サービスにリンクされたロール	149
コアロール	150
管理アカウントロール	152
メンバーアカウントのロール	155
ユーザーベースのサブスクリプションロール	157
Linux サブスクリプションロール	159
AWS管理ポリシー	161
AWSLicenseManagerServiceRolePolicy	161
AWSLicenseManagerMasterAccountRolePolicy	163
AWSLicenseManagerMemberAccountRolePolicy	167

AWSLicenseManagerConsumptionPolicy	168
AWSLicenseManagerUserSubscriptionsServiceRolePolicy	169
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	170
ポリシーの更新	171
ライセンス署名	174
コンプライアンス検証	175
耐障害性	176
インフラストラクチャセキュリティ	177
VPC エンドポイント(AWS PrivateLink)	177
License Maneger用のインターフェイスVPCエンドポイントの作成	178
License Maneger 用のVPCエンドポイントポリシーを作成する	178
トラブルシューティング	180
クロスアカウント検出エラー	180
管理アカウントは、自己管理ライセンスとリソースの関連付けを解除することはできません。	180
Systems Managerインベントリが古い	180
登録解除されたAMIの見かけ上の存続	181
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	181
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	181
クロスアカウント検出を無効化できない	181
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	181
AWS Organizations アカウントのリンクは失敗します。	182
ドキュメント履歴	183
.....	clxxxviii

とは何ですか AWS License Manager?

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

クラウド・インフラストラクチャーを構築する際 AWS、BYOL (BYOL) を活用することでコストを節約できます。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、サービスと直接連携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軽減します AWS。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。

AWS License Manager では、チェックアウトしたすべてのエンタイトルメントの数を管理することで、ライセンスを一元的に追跡し、複数のリージョンにわたって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、指標やイベントを通じて ISV に追跡できます。CloudWatchISV 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 Data Exchange](#) [AWS Marketplace](#) と統合されており、[AWS Identity and Access Management \(IAM\)](#)、AWS Service Quotas [AWS Organizations](#)、AWS リソースタギング [AWS CloudFormation](#)、およびの各サービスと統合されています。[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 (ISV) は、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、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。販売している ISV は、トランザクションワークフローの一部として、AWS Marketplace ライセンスの自動作成と配布のメリットを享受できます。ISV 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顧客向けにライセンスを有効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。

IAM ID を使用するか AWS License Manager、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、ライセンスを作成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は、ライセンス資格をそれぞれの組織の ID AWS にさらに再配布できます。AWS 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、配布されたライセンスの基礎となる IAM ID に基づいて実行することも、サービスを通じて生成される長期間有効なトークンに基づいて実行することもできます。AWS License Manager AWS License Manager

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](#)— AWS ライセンスを消費するコマンドの処理方法を決定する企業契約の条件に基づいてライセンスルールを定義するのに使用されます。
- [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](#)— AWS Marketplace、AWS Data Exchange、または自社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。
- [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 提供されているライセンスと Bring Your Own License モデル (BYOL) の間でライセンスの種類を変更する場合に使用します。
- [License Manager でのインベントリ検索](#)— 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。AWS Systems Manager
- [License Manager のユーザーベースのサブスクリプション](#) - 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 の Linux サブスクリプション](#) - 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、AWS Organizations およびと統合されています。

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

License Manager をと共に使用すると AWS Systems Manager、外部でホストされている物理サーバまたは仮想サーバ上のライセンスを管理できます。AWS License Manager、AWS Organizations をと共に使用すると、すべての組織アカウントを一元管理できます。

さらに、ソフトウェアをと統合した販売者から AWS Marketplace、AWS Data Exchange、または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、エンタイトルメントと呼ばれる使用権を特定のユーザーに配布できます。AWS アカウント

License Manager は、Amazon RDS for Oracle、Db2 vCPU ベースの BYOL ライセンス用の Amazon RDS と統合されています。この統合により、Oracle 用 RDS と Db2 DB インスタンス用の RDS の vCPU 使用率を可視化できます。このデータを使用して、データベース管理システムベンダーとのライセンス条件に基づいて消費されるライセンス数を計算できます。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](#)
- [Db2 用 RDS のライセンスオプション](#)

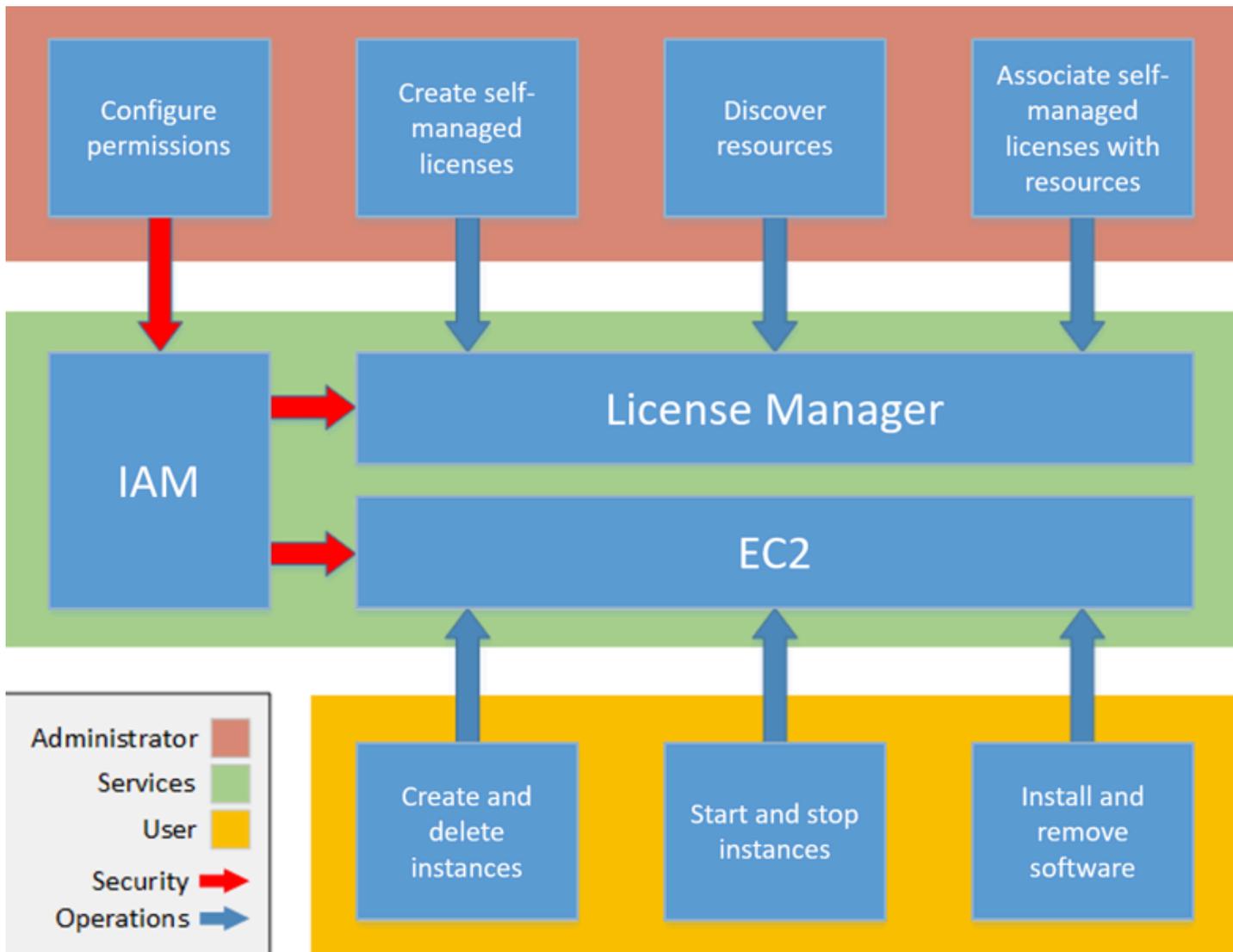
License Manegerの仕組み

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。また重要なことに、インスタンスの作成や削除が行われるAmazon EC2のコントロールプレーンなどのAWSサービスとネイティブに統合されています。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。

ライセンスのエキスパートが、組織全体のライセンスを管理し、リソースインベントリのニーズを判断し、ライセンスの調達を監督し、ライセンス使用のコンプライアンスを推進します。License Managerを使用している企業では、この作業はLicense Managerコンソールを介して統合されています。図に示すように、これには、サービスのアクセス許可の設定、セルフマネージドライセンスの作成、オンプレミスおよびクラウド上の両方のコンピューティングリソースのインベントリの取得、セルフマネージドライセンスと検出されたリソースの関連付けが含まれます。実際にはこれは、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。

の開始方法 AWS License Manager

以下のセクションでは、AWS アカウントとユーザーの設定方法と、License Manager の使用を開始する方法について説明します。AWS ベストプラクティスに従って 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 [AWS License Manager のためのアイデンティティおよびアクセス管理](#)。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。

トピック

- [設定](#)
- [で License Manager を使用するようにオンボードする AWS Management Console](#)

設定

次のセクションでは、AWS アカウントとユーザーの設定について詳しく説明します。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. <https://portal.aws.amazon.com/billing/signup> を開きます。
2. オンラインの手順に従います。

サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

にサインアップすると AWS アカウント、AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービスとリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用して [ルートユーザーアクセスが必要なタスク](#) を実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。 <https://aws.amazon.com/> の [マイアカウント] を選んで、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理できます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、 日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者 [AWS Management Console](#) として にサインインします。次のページでパスワードを入力します。

ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「[ルートユーザーとしてサインインする](#)」を参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

手順については、「IAM [ユーザーガイド](#)」の AWS アカウント「[ルートユーザーの仮想 MFA デバイスを有効にする \(コンソール\)](#)」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

手順については、「AWS IAM Identity Center ユーザーガイド」の「[AWS IAM Identity Centerの有効化](#)」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「[ユーザーガイド](#)」の「[デフォルトでユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ](#)」AWS IAM Identity Center」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

IAM Identity Center ユーザーを使用してサインインする方法については、「AWS サインインユーザーガイド」の [AWS 「アクセスポータルへのサインイン](#)」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

手順については、「AWS IAM Identity Center ユーザーガイド」の「[権限設定を作成する](#)」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

手順については、「AWS IAM Identity Center ユーザーガイド」の「[グループの参加](#)」を参照してください。

で License Manager を使用するようにオンボードする AWS Management Console

License Manager の使用を開始するには、次の手順が必要です。最初の要件が完了したら、希望するユースケースに合わせて License Manager の使用を続行できます。

License Manager の使用を開始するには

1. License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. License Manager 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 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 の起動テンプレート、AWS CloudFormation テンプレート、またはサービスカタログ製品を介して AWS Marketplace BYOL AMI 製品にライセンスルールを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では、[Systems Managerのインベントリ](#) AWSの外で実行されているアプリケーションを検出し、そのアプリケーションにライセンスルールを適用することができます。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。

お客様のAWSつのアカウントに渡るLicense Manager

License Manager を使うと、お客様のAWSアカウントをまたいでライセンスを管理することができます。AWS Organizations管理アカウント内でライセンス設定を1度作成すれば、AWS Resource

Access Manager を使ってアカウント間で共有したり、License Manager の設定を使って AWS Organizations アカウント連携させて、アカウント間で共有することができます。これにより、AWS アカウントをまたいで検出を実行して、アカウント間でのインベントリ検索も可能です。

目次

- [License Manager のセルフマネージドライセンス](#)
- [License Manager のライセンスルール](#)
- [License Manager の使用状況レポート](#)
- [License Manager でのライセンスタイプの変換](#)
- [AWS License Manager のリソースグループをホストします](#)
- [License Manager でのインベントリ検索](#)
- [ライセンスマネージャーで付与されたライセンス](#)
- [License Manager で販売者が発行したライセンス](#)
- [License Manager のユーザーベースのサブスクリプション](#)
- [License Manager の Linux サブスクリプション](#)
- [AWS License Manager での設定](#)
- [AWS License Manager のダッシュボード](#)

License Manager のセルフマネージドライセンス

セルフマネージドライセンスは License Manager の中核をなすものです。セルフマネージドライセンスは、以前は「ライセンス設定」と呼ばれていました。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。作成したルールによって、AWS ライセンスを消費するコマンドの処理方法が決まります。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。

制限

- リソースあたりのセルフマネージドライセンス数:10
- セルフマネージドライセンスの総数:25
- 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。

コンテンツ

- [セルフマネージドライセンスの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](#)
- [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を共有する](#)
- [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を非アクティブ化する](#)
- [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のパラメータとルール

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

下記を含むパラメータやルールを使用できます。

- セルフマネージドライセンス名 - セルフマネージドライセンスの名前。
- (オプション) 説明 - セルフマネージドライセンスの説明。
- ライセンスタイプ - ライセンスカウントに使用されるメトリック。サポートされている値は、[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。
- 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、および Db2 向けの Amazon RDS 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用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
 - ハードウェア専用インスタンス (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。

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)	licenseAf finitiyToHost	✓		✓	
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		✓		✓

コンソール名	API名	コア	インスタンス	ソケット	vCPUs
テナンシー	allowedTenancy	✓	✓	✓	✓
vCPUの最適化	honorVcpu Optimization				✓

ベンダーライセンスからライセンスマネージャールールを構築する

ソフトウェアベンダーライセンスの言語に基づいて、ライセンスマネージャーのルールセットを作成できます。以下の例は、実際のお客様のユースケースのブループリントを意図したものではありません。実際のライセンス契約の適用にあたっては、特定のオンプレミスサーバー環境のアーキテクチャとライセンス履歴に応じて、競合するオプションの中から選択します。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 要件や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 ソフトウェアベンダーの監査プロセスには関与しない。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。

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

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

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。

Oracle 用 Amazon RDS と Db2 データベース用 Amazon RDS に関する考慮事項

製品情報を追加して Oracle 用 Amazon RDS または Db2 データベース用 Amazon RDS の自動検出を設定する場合、以下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。
 - 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。そのためには、[除外ルールを追加] を選択し、フィルタリングするプロパティ、AWS アカウント ID とリソースタグがサポートされているプロパティを選択し、そのプロパティを識別する情報を入力します。
6. (オプション) [タグ] パネルを展開し、1 つ以上のタグをセルフマネージドライセンスに追加します。タグはキーと値のペアです。タグごとに次の情報を記入してください。
- キー - 検索可能なキー名。
 - 値 - キーの値。
7. [送信] を選択します。

コマンドラインを使用してセルフマネージドライセンスを作成するには

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

セルフマネージドライセンスを共有する

AWS Resource Access Manager を使用して、AWS 自己管理ライセンスを任意のアカウントまたは経由で共有できます。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。

サポートされるアカウントのクォータ

2023 年 10 月 14 AWS License Manager 日より前に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を下回ります。このクォータは、次のセクションで説明する API オペレーションを使用して増やすことができます。AWS RAM 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 次の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 次の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、AWS RAM 以下とのリソース共有を有効にします。

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

{
  "returnValue": true
}
```

[list-aws-service-access-for-organization](#) AWS CLI この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、AWS RAM および次のことを確認できます。

```
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

組織でこの操作が完了するまでに最大 6 AWS RAM 時間かかることがあります。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に関連付けます。

```
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 このコマンドを使用して、status ASSOCIATED リソース共有の関連付けが以下のとおりであることを検証できます。

```
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
    }
  ]
}
```

セルフマネージドライセンスを編集する

セルフマネージドライセンスの次のフィールドの値を編集できます。

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

セルフマネージドライセンスを編集するには

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

コマンドラインを使用してセルフマネージドライセンスを編集するには

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

セルフマネージドライセンスを非アクティブ化する

セルフマネージドライセンスを非アクティブ化しても、そのライセンスを使用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)
- [アップデートリンク LicenseConfiguration](#) (AWS Tools for PowerShell)

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)
- [リムーブ-リンク LicenseConfiguration](#) (AWS Tools for PowerShell)

License Manager のライセンスルール

セルフマネージドライセンスルールを作成したら、それを関連する起動メカニズムに添付して、新しいリソースのコンプライアンス違反のデプロイを直接防ぐことができます。組織内のユーザーは、指定された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 ソフトウェアベンダーの監査プロセスには参加しません。お客様はコンプライアンスに責任を負い、ライセンス契約に基づいてルールを注意深く理解しキャプチャしてLicense Manager に取り込むことに責任を負うものとします。

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

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

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

- 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 [— AMI にライセンスルールをアタッチするのが好ましくない場合、EC2 AWS CloudFormation 起動テンプレートまたはテンプレートの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。自己管理型ライセンスフィールドに 1 つ以上の自己管理型ライセンス ID を指定することで、EC2 AWS CloudFormation 起動テンプレートまたはテンプレートにルールを適用できます。

AWS ライセンストラッキングデータは、それを所有するアカウントからのみアクセス可能な機密性の高い顧客データとして扱われます。AWS はユーザーのライセンストラッキングデータにはアクセスできません。お客様はライセンス追跡データを管理し、いつでも削除することができます。

セルフマネージドライセンスと 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。

同じリージョン内の 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 はそれを追跡します。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 から起動する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ストラッキング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の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。

License Manager の使用状況レポート

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

Note

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

使用状況レポートの作成

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

セルフマネージドライセンスの概要レポート

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

リソース使用状況レポート

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

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で [使用状況レポート] を選択します。
3. [使用状況レポートを作成] を選択し、[使用状況レポートを作成] ペインでレポートのパラメータを定義します。
 - a. 使用状況レポートの [名前] と [説明] (オプション) を入力します。
 - b. ドロップダウンリストから、セルフマネージドライセンスタイプを選択します。これは、使用状況レポートがデータを生成する際のライセンスのタイプです。
 - c. 生成するレポートタイプを選択します。
 - d. License Manager がレポートを発行する頻度を選択します。[毎日 1 回]、[毎週 1 回] または [毎月 1 回] を選ぶことができます。
 - e. (オプション) [タグ] を追加して、使用状況レポートリソースを追跡します。
4. [使用状況レポートを作成] を選択します。

新しい使用状況レポートは 60 分以内にレポートの公開を開始します。

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

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

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

使用状況レポートの編集

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

使用状況レポートを編集するには

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

更新された使用状況レポートは、1 時間以内に新しいレポートを生成します。

Note

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

使用状況レポートの削除

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

Note

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

使用状況レポートを編集するには

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

License Manager でのライセンスタイプの変換

License Manager を使用すると、ビジネスニーズの変化に応じて、AWS 提供されたライセンスと自分のライセンス使用モデル (BYOL) または自分のサブスクリプション使用モデル (BYOS) の間でライセンスタイプを変更できます。ライセンスタイプは、既存のワークロードを再デプロイすることなく変更できます。

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

オンプレミスのワークロードを Amazon EC2 に移行してください

移行中に、ワークロードを Amazon Elastic Compute Cloud (Amazon EC2) にデプロイし、AWS 提供されたライセンスを使用できます。移行が完了したら、License Manager のライセンスタイプ変換を使用して、インスタンスのライセンスタイプを変更します。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 または BYOS に変更することができます。

ライセンス契約が終了したワークロードの継続実行

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

コストの最適化

小規模なワークロードや不規則なワークロードでは、AWS 提供されたライセンス (ライセンス込み) インスタンスの方が費用対効果が高い場合があります。BYOL または BYOS を使用することを選択した場合、これらのオプションにはより長い期間の契約が必要になる場合があります。この場合、License Manager のライセンスタイプ変換を使用して、インスタンスを付属のライセンスに切り替え、ライセンス関連のコストを最適化することができます。インスタンスが独自の仮

想マシン (VM) イメージから起動された場合は、BYOL または BYOS に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 Pro にサブスクリプションを追加すると、長期間にわたってセキュリティアップデートが提供されます。詳細については、Canonical のドキュメントの「[Ubuntu Pro](#)」を参照してください。

トピック

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

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

- [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](#)
- [Linux の対象となるサブスクリプションタイプ](#)

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)	RunInstances:0800
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	RunInstances:0002
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	RunInstances:0202
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	RunInstances:0006
SQL Server Standard (ライセンスインクルード)	RunInstances:0006

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:0102
SQL Server Enterprise (ライセンスインクルード)	

メディアの互換性

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

ソース	Target	
	BYOL	ライセンスインクルード
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、「[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	Target					
	BYOL としての Windows Server	ライセンスインクルードとしての Windows Server	BYOL としての Windows Server	ライセンスインクルードとしての Windows Server	BYOL としての Windows Server	ライセンスインクルードとしての Windows Server
			BYOL としての SQL Server	BYOL としての SQL 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 SQL Server
BYOL としての Windows サーバー (お客様のメディア)	不要	はい	不要	あり ¹	サポートされていません	あり ¹
ライセンスインクルードとしての Windows Server (お客様のメディア)	あり ²	不要	はい ^{1, 2}	不要 ³	サポートされていません	あり ¹

ソース	Target					
ライセンス インクルードとしての Windows Server (AWS 提供 されたイ メージ)	いいえ ^x	不要	いいえ ^x	不要 ³	サポートさ れていませ ん	あり ¹
BYOL と しての Windows サーバー (お客様の メディア)	不要 ⁴	はい	不要	はい	サポートさ れていませ ん	はい
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)	あり ²	不要 ⁴	あり ²	不要	サポートさ れていませ ん	はい
BYOL とし ての SQL サーバー (お客様の メディア)						

ソース	Target					
ライセンス インクルードとしての Windows Server (AWS 提供 されたイ メージ)	いいえ x	不要 ⁴	いいえ x	不要	サポートさ れていませ ん	はい
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)	サポートさ れていませ ん	サポートさ れていませ ん	サポートさ れていませ ん	サポートさ れていませ ん	サポートさ れていませ ん	サポートさ れていませ ん
ライセンス インクル ードとし ての SQL Server						

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

ソース	Target					
ライセンス インクルードとしての Windows Server (AWS 提供 されたイ メージ)	いいえ ^x	はい ⁵	いいえ ^x	はい	サポートさ れていませ ん	不要
ライセンス インクルードとし ての SQL Server (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。

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。

次の Ubuntu バージョンではライセンスタイプ変換を使用できます。

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

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

Linux の変換パス

サポートされている Ubuntu LTS のバージョンであれば、どれでも Ubuntu Pro に変換できます。Ubuntu Pro から Ubuntu LTS に変換する必要がある場合は、AWS Support 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。

変換の前提条件

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条件があります。

トピック

- [全般](#)
- [Windows](#)
- [Linux](#)

全般

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

- は License Manager にオンボード AWS アカウント する必要があります。 [の開始方法 AWS License Manager](#) を参照してください。
- ライセンスタイプを変換する前に、対象となるインスタンスが停止状態になっている必要があります。詳細については、「Amazon EC2 ユーザーガイド」の「[インスタンスの停止と起動](#)」を参照してください。
- ターゲットインスタンスで停止保護が有効になっていると、変換プロセスは失敗します。詳細については、「[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 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。

Windows

Windows インスタンスは、次の前提条件を満たす必要があります。

- Amazon 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。

- 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。

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。

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

License Manager は、ライセンスタイプ変換の一環として、セルフマネージドライセンスに関連付けられているリソースを更新する場合があります。具体的には、タイプ License Included の自動検出ルールを使用するセルフマネージドライセンスの場合、License Manager は、license included の自動検出ルールがリソースを明示的に除外している場合、ライセンスタイプ変換のリソースとライセンスの関連付けを解除します。

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

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

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。
 1. Ubuntu LTS
 2. Windows BYOL
 3. 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

特定のコマンドを実行し AWS CLI、次のステップで必要な出力をすべて受信するように、[awscli](#) を更新する必要がある場合があります。

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

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

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

i 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 AWS KMS サーバーから独自の KMS サーバーに切り替える必要があります。

⚠ Important

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

インスタンスのライセンスタイプを BYOL からライセンスインクルードに変換するには、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 からライセンスインクルードに変換する

複数の製品を同時に切り替えることができます。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
```

Linux のライセンスタイプを変換する

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

トピック

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

ライセンスタイプの変換に関する考慮事項

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

- ライセンスタイプを Ubuntu Pro に変換するには、インスタンスが Ubuntu LTS を実行している必要があります。

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

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。
 1. Ubuntu LTS
 2. Windows BYOL
 3. 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、「[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

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

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

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

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

Ubuntu Pro に変換する

インスタンスを Ubuntu LTS から Ubuntu Pro に変換する場合、Canonical サーバーからライセンストークンを取得し、Ubuntu Pro Client をインストールするために、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が必要です。詳細については、「[変換の前提条件](#)」を参照してください。

Ubuntu LTS を Ubuntu Pro に変換するには:

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、AWS Support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。

テナンシー変換

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

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

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

ホストリソースグループテナンシータイプに移行するには、アカウントに少なくとも1つのホストリソースグループが必要です。ホストリソースグループ内でインスタンスを起動するには、そのインスタンスに、ホストリソースグループに関連付けられているものと同じライセンスセットが必要です。詳細については、「[AWS License Managerのリソースグループをホストします](#)」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、Red Hat(RHEL)、および SUSE (SLES) ライセンスに含まれる課金コードは、共有テナンシーおよびハードウェア専用インスタンスで許可

されています。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>
```

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.](#)
- [CreateLicenseConversionTaskForResource オペレーションを呼び出すときにエラー \(InvalidParameterValueException\) が発生しました。ResourceId - \[インスタンス\] はライセンスタイプを変更するために無効な状態です。](#)
- [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、「[変換の前提条件](#)」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。

CreateLicenseConversionTaskForResource オペレーションを呼び出すときにエラー (InvalidParameterValueException) が発生しました。ResourceId - [インスタンス] はライセンスタイプを変更するために無効な状態です。

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「[変換の前提条件](#)」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。

AWS License Managerのリソースグループをホストします

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。

目次

- [ホストリソースグループの作成](#)
- [ホストリソースグループの共有](#)
- [ホストリソースグループへのDedicated Hostsの追加](#)
- [ホストリソースグループのインスタンスを起動する](#)
- [ホストリソースグループの変更](#)
- [ホストリソースグループからの Dedicated Host の削除](#)
- [ホストリソースグループを削除します。](#)

ホストリソースグループの作成

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設定してください。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。

ホストリソースグループの共有

ホストリソースグループをAWS Organizationsで共有するためにAWS Resource Access Managerを使用できます。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](#)を参照してください。

ホストリソースグループへのDedicated Hostsの追加

既存のホストをホストリソースグループに追加するには、AWS Management Console、AWS CLI、またはAWSAPIから行うことができます。ホストを追加するには、AWS Dedicated Host およびホストリソースグループを作成したアカウントの所有者でなければならない。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とします。以下の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。

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:

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. ホストリソースグループ名の一覧から、Dedicated Hostを追加したいホストリソースグループの名前をクリックします。
4. Dedicated Hostsを選択します。
5. [Add] を選択します。
6. 1つまたは複数の Dedicated Hosts を選択して、ホストリソースグループに追加します。
7. [Add] (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。

ホストリソースグループの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。

ホストリソースグループの変更

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。

ホストリソースグループからの Dedicated Host の削除

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日後にホストからインスタンスを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ーゾーンで Dedicated Host を検索することもできます。
6. [Remove] (削除) を選択します。
7. もう一度確認のために削除を選択します。

ホストリソースグループを削除します。

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。ライセンスルールをこれらのサーバーに添付すると、License Manager AWS ダッシュボードでサーバーとともにそれらを追跡できます。

License Manager はこれらのサーバーの起動時または終了時にライセンスルールを検証することはできません。AWS サーバー以外の情報を保持するには up-to-date、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と、組織アカウントからのインベントリデータを集約し、AWS Glue

高速なクエリエクスペリエンスを提供するための Amazon Athena が必要です。詳細については、「[AWS 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。

コンテンツ

- [インベントリ検索の使用](#)
- [インベントリの自動検出](#)

インベントリ検索の使用

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設定](#)
- [インベントリ検索を使用する](#)
- [セルフマネージドライセンスへの自動検出ルールの追加](#)
- [セルフマネージドライセンスとインベントリ検索の関連付け](#)
- [セルフマネージドライセンスとリソースの関連付けの解除](#)

インベントリ検索の設定

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 をアカウントに統合することで、クロスアカウントインベントリ検出を有効にします。AWS Organizations 詳細については、「[AWS License Manager での設定](#)」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してください。

- License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
- 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。
- (オプション) 次のようにフィルターオプションを指定して検索結果を効率化できます。

Amazon EC2 リソース

フィルター名	説明	論理演算子	サポートされる値
リソース ID	リソースの ID。	Equals, Not equals	
アカウント ID	AWS リソースを所有するアカウントの 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	
ライセンスに含まれる名前	含まれているライセンスの種類。	Equals, Not equals	•

フィルター名	説明	論理演算子	サポートされる値
			SQL Server Enterprise <ul style="list-style-type: none">• SQL Server Standard• SQL Server Web• Windows Server Datacenter
タグ	リソースに割り当てられるメタデータタグキーとオプション値。 注: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	<ul style="list-style-type: none">oracle-eeoracle-seoracle-se1oracle-se2db2-sedb2-ae

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

Amazon RDS データベース製品ライセンスの詳細については、Amazon 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。

セルフマネージドライセンスへの自動検出ルールの追加

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、「[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

- License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
- [インベントリ検索] ページを開きます。
- 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 (オラクル向けの RDS、Db2 向けの RDS 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 の場合は、12 AWS 桁のアカウント ID を値として指定します。タグにはキーバリューのペアを入力します。
 - c. ステップ7 を繰り返して、ルールを追加します。
8. [追加] を選択します。

セルフマネージドライセンスとインベントリ検索の関連付け

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を関連付ける] を選択します。
4. [セルフマネージドライセンス名] で、セルフマネージドライセンスを選択します。
5. (オプション) [セルフマネージドライセンスをすべてのメンバーアカウントと共有] を選択します。
6. [関連付ける] を選択します。

セルフマネージドライセンスとリソースの関連付けの解除

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。

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。自動検出のルールは、[UpdateLicenseConfiguration](#) API コマンドを使用して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 をアカウントに統合して、クロスアカウントインベントリ検索を有効にします。AWS Organizations 詳細については、「[AWS License Manager での設定](#)」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、「[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。
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 (オラクル向けの Amazon RDS や Db2 向けの Amazon RDS 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 の場合は、12 AWS 桁のアカウント ID を値として指定します。タグにはキーバリューのペアを入力します。
 - c. ステップ 7 を繰り返して、ルールを追加します。
8. 完了したら [追加] を選択し自動検出ルールを適用します。

ライセンスマネージャーで付与されたライセンス

付与されたライセンスとは、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これらのライセンスの使用を管理し、エンタイトルメントと呼ばれる使用権を特定のAWSアカウントに配信するためにAWS License Managerを使用できます。

AWS Data Exchange 製品に配布されているデータライセンスは、AWS Data Exchangeを通じてAWSアカウントに対して利用可能です。AWS Marketplaceからライセンスを配信する前に、サブスクリプションの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AWSアカウントにエンタイトルメントを配布し、受信者が付与されたライセンスを承諾してアクティベートすると、サブスクリプションはAWS Marketplaceを通じてAWSアカウントで利用可能になります。アカウントには、製品へのアクセス権もあります。例えば、ライセンス管理者が Amazon マシンイメージ(AMI)をAWS Marketplaceから購入し、お客様のAWSアカウントにエンタイトルメントを配布した場合、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](#)
- [付与されたライセンスを管理する](#)
- [使用権限を配布する](#)
- [権限の受理とアクティベーション](#)
- [ライセンスステータス。](#)
- [購入者アカウントのメトリクス](#)

付与されたライセンスを表示する

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

マイライセンス

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

ライセンスの概要 (組織管理者用)

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

集約されたライセンス (組織管理者用)

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

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。ライセンスをどのように受け入れ、アクティブにするかは、AWS Marketplace からのライセンスであるか、お客様のアカ

ウントが AWS Organizations の組織のメンバーアカウントであるかどうか、また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とAWSの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AWS Marketplace以外のエンティティである場合、最初の付与ステータスは [Pending acceptance] (承認保留)です。次のいずれかを実行します。
 - [Accept & activate license(ライセンスの承認とライセンス有効化)]を選択します。その結果権限ステータスは[Active(アクティブ)] になります。
 - [Accept license(ライセンスの承認)]を選択します その結果権限ステータスは[Disabled](無効)になります。ライセンスを使用する準備ができたなら、[Activate license](ライセンスの有効化)を選択します。
 - [Reject license](ライセンスの拒否)を選択します。結果として権限ステータスは[Rejected] (拒否)となります。ライセンスを拒否した後は、ライセンスをアクティブできません。

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

Console (Aggregated licenses)

組織内のすべてのアカウントに付与されたライセンスを集計して表示できます。

Important

組織全体のビューを使用して付与されたライセンスを表示するには、まず AWS License Manager コンソールの設定を使用して AWS Organizations をリンクする必要があります。詳細については、「[AWS License Manager での設定](#)」を参照してください。

AWS Organizations のアカウント全体の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、[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 AWS Marketplace 以外のエンティティの場合は、次のいずれかの操作を行います。
 - [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

AWS CLI を使用して、付与されたライセンスを操作することができます。

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](#)

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。AWS Organizations の詳細については、「[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。

- 指定したアカウントのみを含む AWS アカウント。
- 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 AWS CLI を使用して使用権限を配布できます。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. 権限受信者の AWS アカウント の ID、AWS Organizations OU の ID もしくは ARN、または AWS Organizations の ID もしくは 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

AWS CLI を使用して使用権限を配布できます。AWS License Manager API を使用するとき、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。

権限の受理とアクティベーション

付与されたライセンスに対して権限が作成されると、その権限は受信者に配布されます。権限の受信者が付与されたライセンスを使用するには、ライセンスが承諾され、アクティブになる必要があります。

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] することを選択できます。承認されているが、まだアクティブになっていない権限のステータスは Disabled です。承認済みおよび有効化された権限のステータスは Active です。

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

Tip

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

AWS Marketplaceからの同じ製品に対して2つのライセンスを同時にアクティベート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。AWS Marketplace から提供された権限を有効化すると、有効な権限を置き換えるかどうかのオプションが表示される場合があります。

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

権限を有効化するには (コンソール)

1. 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

AWS CLI を使用して、付与されたライセンスを操作することができます。

AWS CLI を使用して配布された権限を操作するには

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

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

購入者アカウントのメトリクス

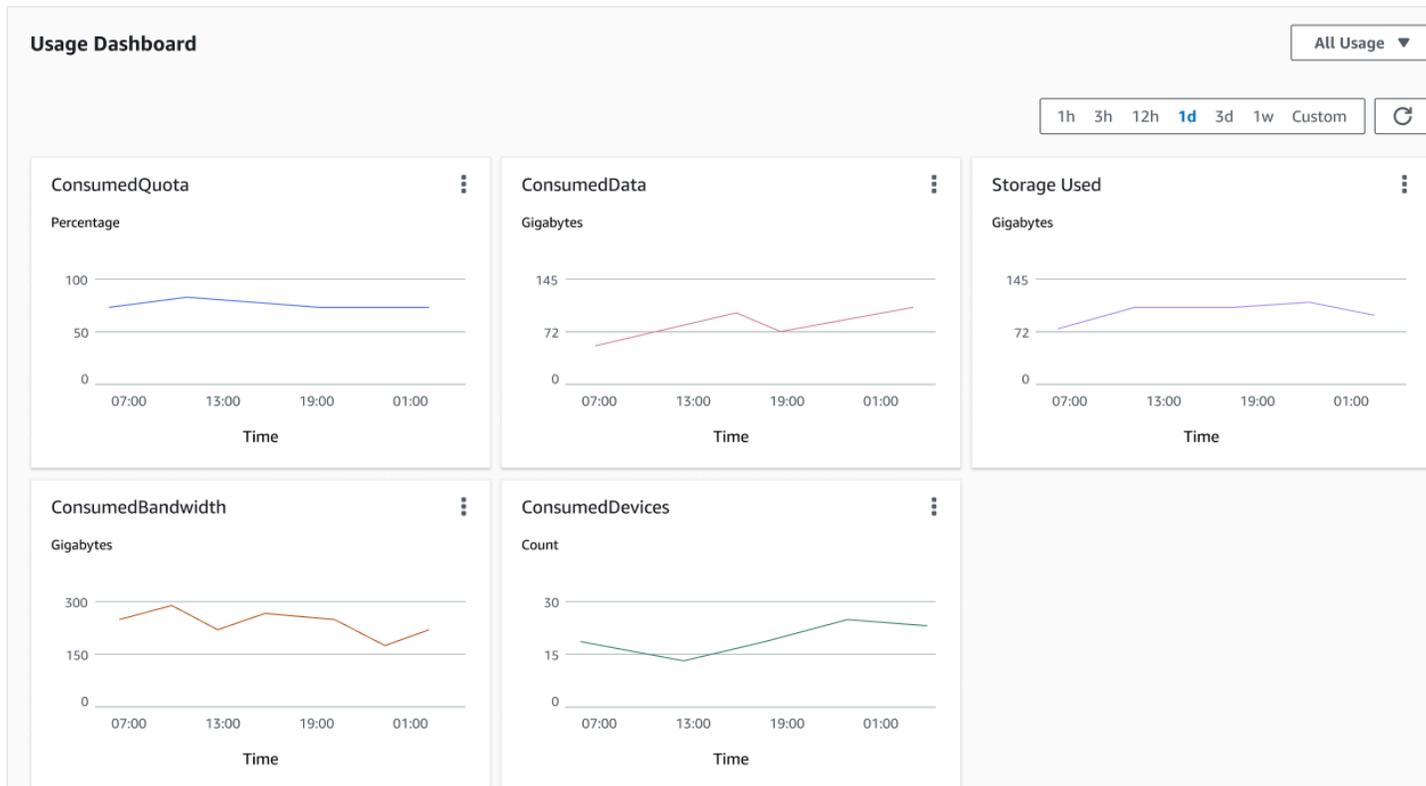
販売者が発行したライセンスの権限が [使用状況レコードの送信を許可] に設定されている場合、License Manager は販売者アカウント、ルート購入者アカウント、および使用状況の記録対象となるアカウントに CloudWatch メトリクスを出力します。購入者アカウントとは、販売者が発行したライセンスを購入した、または付与された AWS アカウントです。詳細については、「[顧客へのライセンスの付与](#)」を参照してください。

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。



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、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 AWS License Manager を使用することができます。発行者は、License Managerダッシュボードを使用して、販売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。

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として、アシンメトリックの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、AWS IAM アイデンティティ、または License Manager によって生成されたベアートークンを使用して、お客様にライセンスを配信することができます。を使用したお客様 AWS アカウントは、ライセンスエンタイトルメントを AWS それぞれの組織のアイデンティティとして、お客様にライセンスを配信することができます。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。

使用権限管理

License Manager は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取り込みます。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。

ライセンス使用量

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。

要件

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。

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

```
]
}
```

License Managerと統合する場合は、AWSアカウントはAWS Marketplaceの外で販売されたライセンスを消費できません。ソフトウェアアプリケーションが License Manager API を呼び出すためのロールを作成する必要があります。例えば、AWSCLIを使用できます。まず、[create-role](#)コマンドを使って、AWSLicenseManager消費ロールを作成します。

```
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
```

以下はtrust-policy-document.jsonです。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "openid-license-manager.amazonaws.com"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringLike": {
          "openid-license-manager.amazonaws.com:sub": "66a9bbf5-0896-460f-a1a9-
de535dcc175b"
        }
      }
    }
  ]
}
```

次に、[attach-role-policy](#)コマンドでAWSAWSLicenseManager消費ポリシー AWSのマネージドポリシーをAWSLicenseManager消費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
```

出品者が発行したライセンスの作成

AWS Management Console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 キーを入力] - License Manager はこのキーを使って発行者の署名と確認を行います。詳細については、「[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。

顧客へのライセンスの付与

新しいライセンスを追加した後、AWS Management Console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、お客様がAWSアカウントをお持ちでない場合、License Manager APIを使用してお客様が[ライセンスを消費](#)できるようにすることもできます。

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] - ライセンス受取人の 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エンタイトルメントを他の AWS アカウントに配布できる場合は、[配布] を選択します。

- AWS ID や認証情報を使用せずに共有ライセンスを認証するには、[オンプレミストークン生成を許可] を選択します。
 - 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]- ライセンスの AWS リージョン。
6. 許可の作成を選択します。

AWSアカウントを使用せずに顧客の一時的な認証情報を入手する

AWSアカウントがないお客様向に対しても、AWSアカウントを持つお客様と同じ方法でエンタイトルメントを使用することができます。以下の手順で、AWSアカウントを持っていないお客様の一時的なAWS認証情報を取得します。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、前のステップでGetAccessTokenから受け取ったアクセストークンと、作成したAWSLicenseManagerConsumptionRole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したい特定のライセンス資格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。

使用ライセンス

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

販売者が発行したライセンスの削除

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 Management Console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. [Delete] (削除) をクリックします。確認を求められたら、「**delete**」を入力し、[削除] を選択します。

License Manager のユーザーベースのサブスクリプション

のユーザーベースのサブスクリプションでは AWS License Manager、完全準拠のライセンスソフトウェアサブスクリプションを購入できます。ライセンスは Amazon から提供され、ユーザーごとのサブスクリプション料金がかかります。Amazon EC2 は、サポート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利用するには、[AWS Directory Service for Microsoft Active Directory](#) (AWS Managed Microsoft AD) のユーザー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。

目次

- [前提条件](#)
- [考慮事項](#)
- [ユーザーベースのサブスクリプションのソフトウェア](#)
 - [ユーザーベースのサブスクリプションでサポートされるソフトウェア](#)
 - [Microsoft Visual Studio](#)
 - [Microsoft Office](#)
 - [サポートされている AMI からの起動](#)
 - [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の開始方法](#)
 - [ステップ 1: AWS Directory Service for Microsoft Active Directory および仮想プライベートクラウド \(VPC\) を設定する](#)
 - [ステップ 2: 製品をサブスクライブする](#)
 - [ステップ 3: 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する](#)
 - [ステップ 4: 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 5: ユーザーベースのサブスクリプションのインスタンスに接続する](#)
- [ユーザーベースのサブスクリプションのディレクトリ設定を変更する](#)
- [ユーザーベースのサブスクリプションの VPC 設定を変更する](#)
- [ユーザーベースのサブスクリプションからユーザーの関連付けを解除する](#)
- [ユーザーベースのサブスクリプションからユーザーの登録を解除する](#)
- [ユーザーベースのサブスクリプションを提供する EC2 インスタンスを終了する](#)

- [ユーザーベースのサブスクリプションで使用するディレクトリを削除する](#)
- [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](#)
 - [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](#)
 - [ライセンスコンプライアンスに関するトラブルシューティング](#)
 - [インスタンスの接続に関するトラブルシューティング](#)
 - [ドメインへの参加に失敗した場合のトラブルシューティング](#)
 - [Systems Manager の接続に関する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](#)

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。

- 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 コンソールの [ユーザーベースのサブスクリプション] セクションに、必要なサービスリンクロールを作成する権限を License Manager に付与することに同意することを求めるプロンプトが一度だけ表示されます。License Manager に権限を付与したら、[作成] を選択してサービスリンクロールを作成します。詳細については、「[AWS 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。
- 共有されている AWS Managed Microsoft AD ディレクトリが作成されている必要があります。AWS Managed Microsoft AD ディレクトリはサポートされていません。ディレクトリの作成の詳細については、AWS Managed Microsoft AD 「AWS Directory Service ユーザーガイド」の[AWS Managed Microsoft AD 「前提条件」](#) および [AWS Managed Microsoft AD 「ディレクトリの作成」](#) を参照してください。
- ユーザーベースのサブスクリプションを利用するには、ユーザーを AWS Managed Microsoft AD ディレクトリまたはセルフマネージド Active Directory に関連付ける必要があります。
 - 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。
 - セルフマネージドディレクトリの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は双方向のフォレストトラストを確立する必要があります。

あります。詳細については、「AWS Directory Service 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。

- ディレクトリ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。
- 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 ([VPC エンドポイント](#)) 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 AWS Systems Manager と通信でき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[「Systems Manager の EC2 インスタンスのセットアップ」](#)を参照してください。
- License Manager は、 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 AWS Managed Microsoft AD 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 IPv4 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を許可していることを確認してください。詳細については、「AWS Directory Service 管理ガイド」の[「ステップ 1: AWS Directory Service for Microsoft Active Directory および仮想プライベートクラウド \(VPC\) を設定する」](#) 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。

- ユーザーベースのサブスクリプションに登録 AWS Managed Microsoft AD する への追加の VPCs の DNS 転送を設定する必要があります。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。
- ユーザーベースのサブスクリプションで Microsoft Office に登録する場合は、次のことを行う必要があります。
 - 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。
 - 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。

- インバウンド TCP ポート 1688 接続を許可する VPC エンドポイントのセキュリティグループを特定または作成します。このセキュリティグループは、仮想プライベートクラウドの設定時に指定されます。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 の設定時にユーザーに代わって作成した 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。
- 承認された接続元からのインバウンド TCP ポート 3389 接続を許可する、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用のセキュリティグループを特定または作成します。このセキュリティグループでは、VPC エンドポイントに到達するためのアウトバウンド TCP ポート 1688 接続も許可する必要があります。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。

ユーザーベースのサブスクリプションを初めて使用するための準備を行っている場合は、前提条件をすべて満たしてから「[ユーザーベースのサブスクリプションの開始方法](#)」を参照してください。既にユーザーベースのサブスクリプションを設定していて、これらの製品を AWS Managed Microsoft AD に追加して Microsoft Office 製品用に VPC を設定する場合は、前提条件をすべて満たしてから「[ユーザーベースのサブスクリプションのディレクトリ設定を変更する](#)」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。

Warning

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を正常なステータスに AWS Systems Manager するには、によって管理される必要があります。さらに、インスタンスはユーザーベースのサブスクリプションライセンスを有効化でき、ライセンスアクティベーション後もコンプライアンスを維持できる必要があります。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「[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を作成するには、ユーザーまたはロールに次のアクセス許可が必要です。
 - `ec2:CreateNetworkInterface`
 - `ec2>DeleteNetworkInterface`
 - `ec2:DescribeNetworkInterfaces`
 - `ec2:CreateNetworkInterfacePermission`
 - `ec2:DescribeSubnets`
 - `ds:DescribeDirectories`
 - `ds:AuthorizeApplication`
 - `ds:UnauthorizeApplication`
 - `ds:GetAuthorizedApplicationDetails`
 - `ds:DescribeDomainControllers`
- Microsoft Office 製品のユーザーベースのサブスクリプションを作成するには、ユーザーまたはロールに次の追加のアクセス許可も必要です。
 - `ec2:CreateVpcEndpoint`
 - `ec2>DeleteVpcEndpoints`
 - `ec2:DescribeVpcEndpoints`
 - `ec2:ModifyVpcEndpoint`
 - `ec2:DescribeSecurityGroups`

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利用する場合、以下の考慮事項が適用されます。

- Win Remote Desktop Services SAL ライセンスは、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とは別に使用することはできません。
- 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、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。
- 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場合があります。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

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。

- 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。詳細については、「[ユーザーベースのサブスクリプション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。
- Microsoft Office 製品を使用してディレクトリを設定する場合、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 VPC エンドポイントのリソースをすべて削除する場合は、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、「[ユーザーベースのサブスクリプション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、「[ユーザーベースのサブスクリプションで使用するディレクトリを削除する](#)」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、「[ユーザーベースのサブスクリプションを提供する EC2 インスタンスを終了する](#)」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。
- サービスを機能させるため、License Manager 用に作成された 2 つの Elastic Network Interface (ENI) は変更または削除しないでください。
- License Manager が AWS Managed Microsoft AD ディレクトリの AWS リザーブド組織単位 (OU) で作成するオブジェクトは、変更または削除しないでください。
- ユーザーベースのサブスクリプション用にデプロイされたインスタンスは、AWS Systems Manager によるマネージドノードであり、同じドメインに属する必要があります。Systems Manager によるインスタンスの継続的な管理については、このガイドの「[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のソフトウェア

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クラス (RDS SAL) の単一サブスクリプションが必要です。サポートされているソフトウェアの使用状況は、License Manager によって追跡されます。詳細については、「[ユーザーベースのサブスクリプションの開始方法](#)」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 2022
- Windows Server 2019
- Windows Server 2016

ユーザーベースのサブスクリプションでサポートされるソフトウェア

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

Microsoft Visual Studio

Microsoft 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

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

サポートされている AMI からの起動

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 OS プラットフォームバージョン (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. <https://console.aws.amazon.com/marketplace> で AWS Marketplace コンソールを開きます。
2. ナビゲーションペインで、[サブスクリプションの管理] を選択します。
3. サブスクリプションの結果を効率化するために、サブスクリプション名の全部または一部を検索できます。例えば、Office LTSC Professional Plus 2021、Visual Studio Enterprise 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。

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、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、「AWS Directory Service 管理ガイド」の「[管理者アカウントのアクセス権限](#)」を参照してください。

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、「[ユーザーベースのサブスクリプションの開始方法](#)」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の開始方法

以下の手順では、ユーザーベースのサブスクリプションの利用を開始する方法を詳しく説明します。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、「[前提条件](#)」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用に AWS Managed Microsoft AD ディレクトリをすでに設定していて、Microsoft Office も使用したい場合は、「」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の VPC 設定を変更する](#)。

ステップ

- [ステップ 1: AWS Directory Service for Microsoft Active Directory および仮想プライベートクラウド \(VPC\) を設定する](#)
- [ステップ 2: 製品をサブスクライブする](#)
- [ステップ 3: 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する](#)
- [ステップ 4: 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 5: ユーザーベースのサブスクリプションのインスタンスに接続する](#)

ステップ 1: AWS Directory Service for Microsoft Active Directory および仮想プライベートクラウド (VPC) を設定する

License Manager AWS Managed Microsoft AD 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 [VPC](#) が必要です。ユーザーは設定済みの製品にしか登録できないため、ディレクトリを設定する際には、ユーザーベースのサブスクリプションに必要な製品をすべて選択する必要があります。AWS Managed Microsoft AD ディレクトリを登録すると、License Manager は 2 つの Elastic Network Interface (ENIs) を作成し、サービスが 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でディレクトリと通信できるようにします。

⚠ 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、「[前提条件](#)」を参照してください。

ユーザーベースのサブスクリプションで 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 への追加の VPCs の AWS Managed Microsoft AD 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 AWS Managed Microsoft AD が次のように設定された独自の [VPC](#) が必要です。

次の方法のいずれかを使用して、ユーザーベースのサブスクリプションで使用する環境を設定できます。

Console (Active Directory)

ユーザーベースのサブスクリプション AWS Managed Microsoft AD 用に [VPC](#) を設定するには (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. 左側のナビゲーションペインで [設定] を選択するか、バナーの [設定を開く] を選択して [設定] ページに移動します。

3. [設定] ページの AWS Managed Microsoft AD セクションで、[設定] を選択します。
4. [AWS マネージドディレクトリ名と ID] では、ユーザーベースのサブスクリプションを作成したいユーザーを含むディレクトリを選択します。
5. [製品名と ID] では、必要な製品を選択し、[設定] を選択します。

[設定] を選択すると、[設定] ページの AWS Managed Microsoft AD セクションに、[ステータス] が [設定中] の [ディレクトリ ID] が表示されます。設定プロセスが完了すると、[ステータス] に [設定済み] と表示され、残りの手順に進むことができます。

Console (Active Directory and VPC)

ユーザーベースのサブスクリプション AWS Managed Microsoft AD 用に を設定するには (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. 左側のナビゲーションペインで [設定] を選択するか、バナーの [設定を開く] を選択して [設定] ページに移動します。
3. [設定] ページの AWS Managed Microsoft AD セクションで、[設定] を選択します。
4. [AWS マネージドディレクトリ名と ID] では、ユーザーベースのサブスクリプションを作成したいユーザーを含むディレクトリを選択します。
5. [製品名と ID] では、必要な製品を選択します。
6. [仮想プライベートクラウド] では、追加設定用の VPC を選択します。
7. [vpc-x のサブネット] では、VPC エンドポイントをプロビジョニングするサブネットを少なくとも 1 つ選択します。
8. [vpc-x のセキュリティグループ] では、VPC エンドポイントに関連付けるために作成したセキュリティグループを選択し、[設定] を選択します。

[設定] を選択すると、[設定] ページの AWS Managed Microsoft AD および [仮想プライベートクラウド] セクションに、[ステータス] が [設定中] の [ディレクトリ ID] と [VPC ID] が表示されます。設定プロセスが完了すると、各 [ステータス] に [設定済み] と表示され、残りの手順に進むことができます。

AWS CLI

ユーザーベースのサブスクリプション AWS Managed Microsoft AD 用に を設定するには (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 AWS Managed Microsoft AD として 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 AWS Managed Microsoft AD と VPC を設定するには (AWS CLI)

を ID プロバイダー AWS Managed Microsoft AD 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-1234567890ab"
```

使用可能なソフトウェア製品の詳細については、「[ユーザーベースのサブスクリプションのソフトウェア](#)」を参照してください。

ステップ 2: 製品をサブスクライブする

で設定済み製品をサブスクライブするには AWS Marketplace

必要な製品でディレクトリを設定したら、必要な製品への登録が必要になる場合もあります。[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。

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。Windows Server 2008 以前では Terminal Services と呼ばれていた Microsoft リモートデスクトップサービス (RDS) は、ユーザーがネットワーク接続を介してリモートコンピュータまたは仮想マシンを制御できるようにする Microsoft Windows のコンポーネントの 1 つです。RDS により、ユーザーはグラフィカルデスクトップや Windows アプリケーションにリモートアクセスできます。

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。

 Note

RDS SAL ライセンスは、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とは別に使用することはできません。詳細については、「[考慮事項](#)」を参照してください。

次のリンク 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 2021](#)
- [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登録するには

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

条件に同意する場合は、製品のサブスクリプションを処理する必要があります。サブスクリプションが完了するまで、進行中というメッセージが表示されます。必要な他の設定済み製品でもこの手順を繰り返すことができます。必要なすべての製品のサブスクリプションが有効になったら、その製品へのユーザーのサブスクリプションに進むことができます。

Note

AWS Billingでまだ終了していない ([保留中] の請求ステータスとマークされている) 請求期間については、ユーザー数および関連費用の推定請求額が表示されるまで 48 時間かかります。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 3: 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、AWS Systems Manager はそのインスタンスをドメインに参加させ、リソースの追加設定と強化を試みます。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、準備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、「[前提条件](#)」および「[ユーザーベースのサブスクリプションのトラブルシューティング](#)」を参照してください。

ユーザーベースのサブスクリプションでインスタンスを起動するには

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 AWS Managed Microsoft AD ディレクトリ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たら、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、ユーザーが製品を利用できるように製品を提供します。

ステップ 4: ユーザーをユーザーベースのサブスクリプションインスタンスに関連付ける

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

Note

各ユーザーは、Windows Server Remote Desktop Services サブスクライバーアクセスライセンス (RDS SAL) と使用する製品の両方に登録している必要があります。[ステップ 2: 製品をサブスクライブする](#) で説明されているように、アカウントが RDS SAL に登録している場合、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 がサブスクライブされることになります。

License Manager の [製品] ページにはアクティブなサブスクリプションが表示され、[Marketplace のサブスクリプションステータス] には [アクティブ] と表示されます。License Manager の製品の詳

細ページには、[ステータス] が [サブスクライブ済み] のアクティブなユーザーサブスクリプションが表示されます。

⚠ Important

ディレクトリに製品が設定されていない場合は、コンソールの上部に通知バーが表示され、ディレクトリの設定を調整するように指示されます。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所有する必要があります。[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

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

ユーザーを製品に登録してインスタンスに関連付けるには

1. 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. ユーザーを関連付けるインスタンスを選択し、[ユーザーを登録して関連付け] を選択します。
4. ディレクトリに存在するユーザー名を最大 5 つ指定し (信頼できるドメインに存在する場合は [ドメイン名] を含む)、[登録して関連付け] を選択します。

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

ユーザーを製品に登録する

次のいずれかの方法を使用して、ユーザーを製品に登録できます。

Console

ユーザーを製品に登録するには (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. 左側のナビゲーションペインの [ユーザーベースのサブスクリプション] で、[製品] を選択します。
3. ユーザーに登録する [Marketplace のサブスクリプションステータス] が [アクティブ] の製品を選択し、[ユーザーに登録] を選択します。
4. ディレクトリに存在するユーザー名を最大 5 つ指定し (信頼できるドメインに存在する場合は [ドメイン名] を含む)、[サブスクリプション] を選択します。

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

AWS CLI

ユーザーを製品に登録する (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に登録できます。

```
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 (AWS CLI) を搭載した製品にユーザーに登録するには

[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、「[ユーザーベースのサブスクリプションのソフトウェア](#)」を参照してください。

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

ユーザーをインスタンスに関連付ける

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

Important

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

Console

ユーザーをインスタンスに関連付けるには (コンソール)

1. 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. ユーザーを関連付けるインスタンスを選択し、[ユーザーを関連付け] を選択します。
4. ディレクトリに存在するユーザー名を最大 5 つ指定し (信頼できるドメインに存在する場合は [ドメイン名] を含む)、[関連付け] を選択します。

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

AWS CLI

ユーザーをインスタンスに関連付けるには (AWS CLI)

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 のユーザーに関連付けることで、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、「[ユーザーベースのサブスクリプションのソフトウェア](#)」を参照してください。

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

ステップ 5: ユーザーベースのサブスクリプションの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。ユーザーに関連付けられた ID を使用して製品を利用するには、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利用するには、インスタンスの [関連付けのステータス] 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。

ユーザーベースのサブスクリプションのディレクトリ設定を変更する

License Manager の設定ページで設定したディレクトリから、ユーザーベースのサブスクリプション用の製品を追加または削除できます。Microsoft Office 製品を使用している場合は、License Manager がこれらのサブスクリプションの [VPC エンドポイント](#) を作成する必要があるため、異なる手順となります。

Microsoft Office 製品のないディレクトリ設定を変更するには

1. License Manager コンソールを開きます (<https://console.aws.amazon.com/license-manager/>)。
2. 左のナビゲーションペインの [設定] を選択します。
3. [設定] ページの AWS Managed Microsoft AD セクションで、[編集] を選択します。
4. [製品名と ID] で、必要に応じて他の製品を選択して以前の選択をクリアしてから、[変更を保存] を選択します。

Microsoft Office 製品のあるディレクトリ設定を変更するには

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 [設定] を選択するか、バナーの [設定を開く] を選択して [設定] ページに移動します。
3. [設定] ページの AWS Managed Microsoft AD セクションで、[編集] を選択します。
4. [製品名と ID] で、Microsoft Office を含む必要な製品を選択します。
5. [仮想プライベートクラウド] では、追加設定用の VPC を選択します。
6. [vpc-**x** のサブネット] では、VPC エンドポイントをプロビジョニングするサブネットを少なくとも 1 つ選択します。
7. [vpc-**x** のセキュリティグループ] では、VPC エンドポイントに関連付けるために作成したセキュリティグループを選択し、[変更を保存] を選択します。

[変更を保存] を選択すると、[設定] ページの AWS Managed Microsoft AD および [仮想プライベートクラウド] セクションに、[ステータス] が [設定中] の [ディレクトリ ID] と [VPC ID] が表示されます。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前に、ディレクトリの [ステータス] が [設定済み] になり、VPC の [ステータス] が [アクティブ] になるまで待つ必要があります。

ユーザーベースのサブスクリプションの VPC 設定を変更する

Microsoft Office 製品を追加した場合は、VPC の設定を変更できます。License Manager は、リソースがアクティベーションサーバーに到達し、コンプライアンスを維持できるように、指定されたサブネットにユーザーに代わって [VPC エンドポイント](#) を作成します。少なくとも 1 つのサブネットを指定する必要があります。詳細については、「[前提条件](#)」を参照してください。

Note

VPC 設定は、ディレクトリに Microsoft Office 製品が設定されている場合にのみ変更できます。詳細については、「[ユーザーベースのサブスクリプションの開始方法](#)」を参照してください。

すべての VPC エンドポイントを削除する場合は、「[考慮事項](#)」を参照してください。

ディレクトリ設定を変更するには

1. License Manager コンソールを開きます (<https://console.aws.amazon.com/license-manager/>)。
2. 左のナビゲーションペインの [設定] を選択します。
3. [設定] ページの [設定済みの仮想プライベートクラウド] セクションで、[編集] を選択します。
4. 設定した VPC のサブネットとセキュリティグループを必要に応じて変更し、[変更を保存] を選択します。

ユーザーベースのサブスクリプションからユーザーの関連付けを解除する

ユーザーとインスタンスの関連付けを解除して、リソースへのアクセスを削除できます。

Note

ディレクトリからユーザーを削除しても、ユーザーの関連付けやサブスクリプションは変更されません。License Manager のユーザーと製品の詳細ページと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。

ユーザーベースのサブスクリプションのユーザー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。

ユーザーベースのサブスクリプションからユーザーの登録を解除する

製品からユーザーの登録を解除してアクセスを削除し、そのユーザーに対する製品への課金を停止できます。

Important

登録を解除する前に、まず現在関連付けられているインスタンスからユーザーの関連付けを解除する必要があります。

ユーザーベースのサブスクリプションからユーザーの登録を解除するには

1. 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。

ユーザーベースのサブスクリプションを提供する EC2 インスタンスを終了する

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が不要になった場合は、削除できます。これは、インスタンスの終了と呼ばれます。まず、すべてのユーザーとインスタンスの関連付けを解除してから、Amazon EC2 コンソールからインスタンスを終了します。

Note

サブスクリプションの料金が発生しないようにするには、ユーザーとインスタンスとの関連付けを解除する必要があります。詳細については、「[ユーザーベースのサブスクリプション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。

ユーザーベースのサブスクリプションを提供するインスタンスを特定して終了するには

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 ID を選択してインスタンスの詳細ページにアクセスします。
4. インスタンス ID はインスタンスを終了するときに必要になるため、書き留めてください。
5. すべてのユーザーとインスタンスの関連付けを解除します。
6. 「[インスタンスの終了](#)」に記載されている手順に従います。

ユーザーベースのサブスクリプションで使用するディレクトリを削除する

今後ユーザーベースのサブスクリプションで使用しないディレクトリは、削除できます。License Manager からディレクトリを設定を削除しても、ディレクトリ自体は削除されません。ディレクトリを削除すると、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はできません。

Important

License Manager からディレクトリを削除する前に、まずユーザーの関連付けを解除し、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を終了する必要があります。

ディレクトリを削除するには

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の [設定] を選択します。
3. 「設定」ページの AWS Managed Microsoft AD 「」セクションで、「の削除」を選択します。

4. 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、[ステータス] が [設定中] の [ディレクトリ ID] が表示されます。設定プロセスが完了したら、そのディレクトリが AWS Managed Microsoft AD セクションから削除されるはずですが。

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

- [インスタンスのコンプライアンスに関するトラブルシューティング](#)
- [ライセンスコンプライアンスに関するトラブルシューティング](#)
- [インスタンスの接続に関するトラブルシューティング](#)
- [ドメインへの参加に失敗した場合のトラブルシューティング](#)
- [Systems Manager の接続に関するトラブルシューティング](#)
- [Systems Manager Run Command のトラブルシューティング](#)

インスタンスのコンプライアンスに関する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、「[前提条件](#)」を参照してください。

ライセンスコンプライアンスに関する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ディレクトリを設定した場合は、リソースが License Manager が作成する VPC エンドポイントに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。分析するパスのプロトコルとして 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。

インスタンスの接続に関するトラブルシューティング

ユーザーが RDP 内の製品を利用するには、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に RDP を使用して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。Amazon EC2

ドメインへの参加に失敗した場合のトラブルシューティング

ユーザーは、License Manager 設定で設定されたディレクトリから、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。

Systems Manager の接続に関する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。管理 AWS Systems Manager 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。

License Manager の Linux サブスクリプション

AWS License Manager には、所有して AWS で実行している商用 Linux サブスクリプションを表示および管理する機能があります。ライセンスの使用状況は、AWS Organizations のすべての AWS リージョンおよびアカウントで追跡できます。データが検出されて集計されると、商用 Linux サブスクリプションを使用しているすべてのインスタンスを把握できるようになります。さらに、検出されたサブスクリプションデータは Amazon CloudWatch ダッシュボードとして License Manager コンソールに表示されます。アカウントが Organizations にある場合は、メンバーアカウントを管理タスクの委任管理者として登録できます。詳細については、「[委任された管理者](#)」を参照してください。

次のような複数のサブスクリプションの使用状況を追跡できます。

- Red Hat Enterprise Linux (RHEL) (サブスクリプション込み)
- 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

Linux サブスクリプションでは、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。License Manager はこのモデルを使用して、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。この期間中に一部のデータが取り込まれなかった場合は、次のメトリクスの出力時に情報が配信されます。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。

目次

- [Linux サブスクリプションの検出を管理する](#)
 - [Linux サブスクリプションの検出を有効にする](#)
 - [リソース検出のステータス理由](#)
 - [Linux サブスクリプションの検出を無効にする](#)
- [検出されたインスタンスデータを表示する](#)
 - [すべてのインスタンスのデータを表示する](#)
 - [サブスクリプションごとのインスタンスのデータを表示する](#)
- [Linux サブスクリプションの請求情報](#)
- [Linux サブスクリプションの使用状況メトリクスと Amazon CloudWatch アラーム](#)
 - [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のアラームを作成する](#)
 - [Linux サブスクリプションのアラームを変更する](#)
 - [Linux サブスクリプションのアラームを削除する](#)

Linux サブスクリプションの検出を管理する

Linux サブスクリプションの検出は、License Manager コンソールを使用して管理できます。指定した AWS リージョンの Linux サブスクリプションの検出を有効にすると、オプションでこの検出を AWS Organizations のアカウントにまで拡張できます。サブスクリプションの使用状況を追跡する必要がなくなった場合は、検出を無効にすることもできます。

Note

デフォルトでは、AWS リージョンごとに 1 アカウントあたり最大 5,000 のリソースを検出して表示できます。制限の引き上げをリクエストするには、[制限の引き上げのフォーム](#)を使用してください。

トピック

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

Linux サブスクリプションの検出を有効にする

Linux サブスクリプションの検出を有効にするには、License Manager で必要な設定を行う必要があります。設定ページから、サービスにリンクされたロールを作成すると共に、どの AWS リージョンで検出を有効にするか、また AWS Organizations のアカウント全体でリソースを検出するかどうかを指定できます。

Linux サブスクリプションの検出を有効にするには

1. License Manager コンソールを開きます (<https://console.aws.amazon.com/license-manager/>)。
2. 左のナビゲーションペインの [Settings] (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、[設定] を選択します。
4. [ソース AWS リージョン] で、Linux サブスクリプションを検索するリージョンを選択します。
5. AWS Organizations のアカウント全体のサブスクリプションデータを集約する場合は、[AWS Organizations のリンクを設定] を選択します。
6. Linux サブスクリプションのサービスリンクロールを作成するためのアクセス許可を AWS License Manager に付与するオプションを確認し、承認します。
7. [設定の保存] を選択します。

リソース検出のステータス理由

AWS License Manager には、Linux サブスクリプションの検出を有効にするように選択した AWS リージョンごとのステータスと、それに対応するステータス理由が表示されます。Linux サブスクリプションを AWS Organizations とリンクしている場合、ステータス理由は以下のように異なります。

- 進行中
- [成功]
- [Failed] (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。

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

ステータス	ステータス理由	説明
	"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にリンクされたロールを作成して、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

Linux サブスクリプションの検出は AWS License Manager の設定ページから無効にできます。

Warning

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

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. 左のナビゲーションペインの [Settings] (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にリンクされたロールを削除します。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。

検出されたインスタンスデータを表示する

最初のリソース検出が完了すると、選択した AWS リージョンで検出された Linux サブスクリプションを表示できるようになります。AWS Organizations をリンクすることを選択した場合、組織全体のアカウントのデータも集計されます。AWS License Manager コンソールの [インスタンス] セクションに移動すると、データの表を表示できます。AWS License Manager コンソールの [インスタンス] セクションに移動すると、データの表を表示できます。

各インスタンスのデータには、次のものが含まれます。

- インスタンス ID - インスタンスの ID。
- インスタンスタイプ - インスタンスのタイプ。
- アカウント ID - インスタンスを所有するアカウントの ID。
- ステータス - インスタンスのステータス。
- リージョン - インスタンスが存在する AWS リージョン。
- 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。
- AMI ID - インスタンスの起動に使用される AMI の ID。

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ごとの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

選択したリージョン内の組織の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。

すべて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、[インスタンス] を選択します。

- 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
 - 使用操作
 - 製品コード
- (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ごとの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

- License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
- 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。
- [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。
- [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
 - 使用操作
 - 製品コード
- (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。

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含まれます。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 の製品コード、またはその両方を組み合わせたものが含まれます。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

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 with SQL Server Web	RunInstances:0210	✕	EC2 サブスクリプションを含む
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110	✕	EC2 サブスクリプションを含む
SUSE Linux Enterprise Server	RunInstances:000g	✕	EC2 サブスクリプションを含む
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 の使用オペレーションと AWS Marketplace の製品コードの両方が含まれています。

Linux サブスクリプションの使用状況メトリクスと Amazon CloudWatch アラーム

AWS License Manager コンソールの [サブスクリプション] セクションには、お客様が AWS で購入した、または Bring Your Own Subscription モデル (BYOS) を使用して持ち込んだ、検出済みの商用 Linux サブスクリプションが一覧表示されます。商用 Linux サブスクリプションはすべて、インスタンスごとにライセンス供与されます。

検出された Linux サブスクリプションごとに以下の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インスタンス数
- 設定された Amazon CloudWatch アラーム

概要ページから 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。

各サブスクリプションの [使用状況メトリクスとアラーム] タブには、以下の詳細が記載された [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、AWS リージョンおよび定義された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使用状況メトリクス](#)

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

Linux サブスクリプションの使用状況メトリクス

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

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

Linux サブスクリプションの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。

コンソールを使用して 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アラームを変更する

License Manager コンソールから、要件の変化に合わせて既存のアラームを変更できます。

コンソールを使用して 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アラームを削除する

License Manager コンソールから、要件の変化に合わせて既存のアラームを削除できます。

コンソールを使用して 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。

AWS License Manager での設定

AWS License Manager コンソールの [設定] セクションに、現在のアカウントの設定が表示されます。マネージドエンタイトルメントおよびセルフマネージドライセンスを組織へ配布する、クロスアカウントリソース検出を実行するなど、特定の機能を有効にするための設定を行う必要があります。

License Managerの設定を編集するには

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の [Settings] (設定) を選択します。
3. 設定または変更したい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. 設定または変更したい設定に関連するアクションを選択します。例えば、[編集] や [有効化] を選択できます。

設定のトピック

- [マネージドライセンス](#)
 - [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 \(SNS\)](#)
- [Linux サブスクリプション](#)
- [ユーザーベースのサブスクリプション](#)
 - [AWS Managed Microsoft AD](#)
 - [仮想プライベートクラウド](#)
- [委任された管理者](#)
 - [委任管理者のサポートされるリージョン](#)
 - [委任された管理者の登録](#)
 - [委任管理者の登録解除](#)

マネージドライセンス

マネージドライセンスでは次の設定が利用できます。

アカウントの詳細

アカウントの詳細を確認すると、アカウントタイプ、AWS Organizations のアカウント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 の共有 ARN などの情報を確認できます。このセクションでは、AWS Organizations アカウントを連動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で配布するには、[AWS Organizations アカウントへのリンク] 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化するには、管理アカウントにサインインしていて、AWS Organizations ですべての機能が有効になっている必要があります。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、管理アカウントで AWS Resource Access Manager リソース共有が作成され、セルフマネージドライセンスをシームレスに共有することができます。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オンにすると、AWS Organizations が自動的に連動して、すべてのアカウント間でリソース検出を行うようになります。

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

- Amazon S3 バケットにインベントリを格納する [リソースデータリンク](#)。

- 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

以下の AWS リージョン では、ソフトウェアの使用状況を検出するために Systems Manager インベントリのインベントリデータをクエリしたり、集計したりするために Amazon Athena や AWS Glue は必要ありません。

- アジアパシフィック (ジャカルタ)
- イスラエル (テルアビブ)

Simple Notification Service (SNS)

License Manager から通知とアラートを受信するように 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。

Linux サブスクリプション

Linux サブスクリプションの設定を構成して、サブスクリプションの検出と集計をどのように実行するかを制御できます。Linux サブスクリプションを検出したいリージョンと、AWS Organizations のアカウント全体のサブスクリプションデータを集計するかどうかを選択できます。詳細については、「[License Manager の Linux サブスクリプション](#)」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

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

ユーザーベースのサブスクリプションを使用するには、License Manager で AWS Managed Microsoft AD を設定する必要があります。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](#)」を参照してください。

仮想プライベートクラウド

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は、License Manager で 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、「[License Manager のユーザーベースのサブスクリプション](#)」を参照してください。

委任された管理者

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。この方法を使用すると、組織内に License Manager 向けの委任管理者が 1 人設定されます。

AWS CLI または SDK を使用すると、License Manager のサポートされている各機能の委任管理者として、組織内のさまざまなメンバーアカウントを登録できます。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、「[組織への AWS アカウントの招待](#)」と「[AWS Organizations で信頼されたアクセスを有効にする](#)」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

自分が所有して AWS リージョン 全体で運営している商用の Linux サブスクリプション、および AWS Organizations のアカウントの表示や管理といった管理タスクを実行できます。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せん。

[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。

委任管理者のサポートされるリージョン

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)
- ヨーロッパ (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)

委任された管理者の登録

AWS CLI または AWS Management Console を使用して委任管理者を登録できます。

Console

AWS License Manager コンソールを使用して委任された管理者を登録するには、以下のステップを実行します。

1. AWS 管理アカウントの管理者としてサインインします。
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

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、以下のステップを実行します。

1. コマンドラインから、以下の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
```

AWS CLI 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、以下のステップを実行します。

1. コマンドラインから、以下の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
```

委任管理者の登録解除

委任管理者は、AWS CLI または AWS Management Console を使用して登録を解除できます。

Console

AWS License Managerコンソールを使用して代理管理者の登録を解除するには、以下のステップを実行します。

1. AWS管理アカウントの管理者としてサインインします。
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. [Remove] (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

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、以下のステップを実行します。

1. コマンドラインから、以下の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
```

AWS CLI 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、以下のステップを実行します。

1. コマンドラインから、以下の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。

AWS License Manager のダッシュボード

License Manager コンソールの [ダッシュボード] セクションには、各セルフマネージドライセンス、付与されたライセンス資格、ユーザーベースのサブスクリプションのサブスクライブユーザー、および実行中のインスタンスに関連するライセンス消費量を追跡するための使用状況の詳細が表示されます。ダッシュボードにはまた、ライセンスルール違反によるアラートも表示されます。

概要

[概要] セクションには、ライセンスに関する以下の詳細が表示されます。

ライセンスの付与

この地域でこのアカウントに付与されたライセンスの総数。

セルフマネージドライセンス

この地域でこのアカウントに付与されたセルフマネージドライセンスの総数。

販売者が発行したライセンス

この地域でこのアカウントに付与された販売者が発行したドライセンスの総数。

製品

[製品] セクションには、ユーザーベースのサブスクリプションに関する以下の詳細が表示されます。

製品名

ユーザーベースのサブスクリプションの製品名。

サブスクライブユーザー

製品のサブスクライブユーザーの数。

ライセンス付与資格

[付与されたライセンス資格] セクションには、以下の詳細が記載されています。

製品名

付与されたライセンスの製品名。

使用権限管理

使用権限の名前。

使用方法

使用権限の利用状況。

セルフマネージドライセンス

セルフマネージドライセンスには、以下の詳細が記載されています。

ライセンス名

セルフマネージドライセンスの名前。

使用権限管理

使用権限の名前。

使用方法

使用権限の利用状況。

インスタンスの使用状況

[インスタンスの使用状況] セクションには、以下の詳細が記載されています。

実行中のインスタンスの数

この地域内のこのアカウントで実行中のインスタンスの総数。

実行中のインスタンスの集計数

この地域内の 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。このグラフは、管理アカウントおよび委任された管理者アカウントにのみ表示されます。

AWS License Manager のモニタリング

Amazon CloudWatch を使用して AWS License Manager で追跡された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 を使用したライセンス使用状況のモニタリング](#)」を参照してください。

AWS CloudTrail を使用して AWS アカウント に代わって実行された API コールと関連イベントをキャプチャできます。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。AWS を呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出し日時を特定できます。詳細については、「[AWS License Managerを使用したAWS CloudTrailAPI コールのログ記録](#)」を参照してください。

目次

- [Amazon CloudWatch を使用したライセンス使用状況のモニタリング](#)
 - [Secrets Manager のメトリクスを監視するアラームを作成する](#)
- [AWS License Managerを使用したAWS CloudTrailAPI コールのログ記録](#)
 - [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 を使用したライセンス使用状況のモニタリング

Amazon CloudWatch を使用して License Manager のメトリクスの統計情報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	<p>現在のアカウントで実行されているインスタンスのうち、サブスクリプション名でグループ化されたインスタンスの総数。</p> <p>単位はカウント</p> <p>ディメンション:</p> <p>SubscriptionName : サブスクリプションの名前。</p>
AggregateRunningInstancesCount	<p>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。</p> <p>単位はカウント</p> <p>ディメンション:</p> <p>SubscriptionName : サブスクリプションの名前。</p>
TotalLicenseConfigurationUsageCount	<p>使用可能なライセンス設定の総数。</p> <p>単位はカウント</p> <p>ディメンション:</p> <ul style="list-style-type: none"> LicenseConfigurationArn : ライセンス設定の Amazon リソースネーム (ARN)。 LicenseConfigurationType : ライセンス設定のタイプ。
LicenseConfigurationUsageCount	<p>この設定の使用済みライセンスの総数。</p> <p>単位はカウント</p> <p>ディメンション:</p> <ul style="list-style-type: none"> LicenseConfigurationArn : ライセンス設定の ARN。 LicenseConfigurationType : ライセンス設定のタイプ。
LicenseConfigurationUsagePercentage	<p>このライセンス設定の使用済みライセンスをパーセンテージで表したものの。</p>

メトリクス	説明
	単位: パーセント
	ディメンション:
	<ul style="list-style-type: none">LicenseConfigurationArn : ライセンス設定の ARN。LicenseConfigurationType : ライセンス設定のタイプ。

Secrets Manager のメトリクスを監視するアラームを作成する

メトリクスが変化し、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。

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

AWSはLicense Managerでユーザー、ロール、またはAWS CloudTrailサービスが行ったアクションのレコードを提供するAWS License Manager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の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のイベントの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のコンソールの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。

CloudTrailのLicense Manager情報

CloudTrailは、アカウントを作成すると {AWS} アカウントで有効になります。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AWSサービスのイベントとともに CloudTrail イベントに記録されます。最近のイベントは、{AWS} アカウントで表示、検索、ダウンロードできます。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のイベントを含むAWSアカウントのイベントを継続的にレコードするには、追跡を作成します。追跡により、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、コンソールで追跡を作成するときに、追跡がすべてのAWSリージョンに適用されます。追跡は、AWSパーティション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 ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他のAWSの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 のサポート対象サービスと統合](#)
- [Amazon SNS の CloudTrail の通知の設定](#)
- 「[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によって記録さ

れ、[License ManagerAPIリファレンス](#) に文書記録されます。例え

ば、CreateLicenseConfiguration、ListResourceInventory、DeleteLicenseConfiguration。各アクションを呼び出すと、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、ルート認証情報と AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがローカルまたはフェデレーテッド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のサービスによって送信されたかどうか。

詳細については、「[CloudTrail ユーザーアイディエンデティ要素](#)」を参照してください。

ライセンスLicense Maneger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 のログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

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

```
{
  "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"
}
```

AWS License Manager のセキュリティ

AWSでは、クラウドのセキュリティが最優先事項です。AWSの顧客は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティは、AWSと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は、AWSクラウドでAWSのサービスを実行するインフラストラクチャを保護する責任を負います。また、AWSは、使用するサービスを安全に提供します。[AWSコンプライアンスプログラム](#)の一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。License Managerに適用するコンプライアンスプログラムの詳細については、[AWSコンプライアンスプログラムによる適用範囲の](#)。
- クラウド内のセキュリティ-お客様の責任は、使用するAWSのサービスに応じて異なります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、License Manager使用時における責任共有モデルの適用法を理解するのに役立ちます。ここでは、セキュリティとコンプライアンスの目標を満たすようにLicense Managerを設定する方法について説明します。また、License Managerリソースのモニタリングや保護に役立つ他のAWSのサービスの使用方法についても説明します。

目次

- [AWS License Manager でのデータ保護](#)
- [AWS License Manager のためのアイデンティティおよびアクセス管理](#)
- [AWS License Manager のサービスにリンクされたロールの使用](#)
- [AWS の AWS License Manager マネージドポリシー](#)
- [ライセンスの暗号化署名](#)
- [のコンプライアンス検証 AWS License Manager](#)
- [AWS License Manager での耐障害性](#)
- [AWS License Manager でのインフラストラクチャセキュリティ](#)
- [AWS License Manager とインターフェース VPC エンドポイント \(AWS PrivateLink\)](#)

AWS License Manager でのデータ保護

AWS [責任共有モデル](#) は、AWS License Manager でのデータ保護に適用されます。このモデルで説明されているように、AWS は、AWS クラウド のすべて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があります。お客様は、このインフラストラクチャでホストされているコンテンツ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のよくある質問](#)」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。

データを保護するため、AWS アカウント の認証情報を保護し、AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーをセットアップ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を各ユーザーに付与できます。また、次の方法でデータを保護することをおすすめします。

- 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 が必須です。TLS 1.3 が推奨されます。
- AWS CloudTrail で API とユーザーアクティビティロギングをセットアップします。
- AWS のサービス内でデフォルトである、すべてのセキュリティ管理に加え、AWS の暗号化ソリューションを使用します。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API により AWS にアクセスするときに FIPS 140-2 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 \(FIPS\) 140-2](#)」を参照してください。

顧客の E メールアドレスなどの機密情報や重要情報は、タグや Name フィールドなどの自由形式のフィールドに入力しないことを強くお勧めします。これには、コンソール、API、AWS CLI、または AWS SDK を使用して License Manager または他の AWS のサービス を操作する場合があります。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

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。

AWS License Manager のためのアイデンティティおよびアクセス管理

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全にコントロールするために役立つ AWS のサービスです。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 (アクセス許可を持たせる) かを制御します。IAMでは、お客様の AWS アカウントのもとにユーザーや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の許可を制御します。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

AWS アカウント 用のユーザーとグループを作成して、必要な許可を割り当てることができます。ベストプラクティスとして、ユーザーは IAM ロールを引き受けて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、「[の開始方法 AWS License Manager](#)」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、ID が AWS で実行できることとできないことを決定する許可ポリシーを持つ AWS ID であるという点で IAM ユーザーと似ています。ただし、ユーザーは 1 人の特定の人に一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。また、ロールには標準の長期認証情報 (パスワードやアクセスキーなど) も関連付けられません。代わりに、ロールを引き受けると、ロールセッション用の一時的なセキュリティ認証情報が提供されます。

IAM ポリシーの構造

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ず。
- [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、「[AWS License Manager によって定義されるアクション](#)」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:

- `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 User Subscriptions API Reference](#)
- [AWS License Manager Linux Subscriptions API Reference](#)

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。

```
{
  "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。

- AWS IAM Identity Center のユーザーとグループ:

アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「[シークレットの作成と管理](#)」の手順に従ってください。

- ID プロバイダーを通じて IAM で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する。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 \(フェデレーション\) 用のロールの作成](#)」を参照してください。

- IAM ユーザー:
 - ユーザーが設定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 ユーザー用ロールの作成](#)」を参照してください。
 - (非推奨) 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。「IAM ユーザーガイド」の「[ユーザー \(コンソール\) へのアクセス許可の追加](#)」の指示に従います。

AWS 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) [サービスリンクロール](#)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、AWSユーザーの代わりにサービスから他のサービスを呼び出す必要のあるアクセス許可がすべて含まれています。

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。

サービスにリンクされたロール

- [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

AWSServiceRoleForAWSLicenseManagerRole と呼ばれるサービスにリンクされたロールは、License Manager が AWS リソースにアクセスして、ユーザーに代わってライセンスを管理することを可能にします。

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 マネージドポリシー: AWSLicenseManagerServiceRolePolicy](#)。サービスにリンクされた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「[サービスにリンクされたロールの権限](#)」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、AWS CLI、または IAM API を使用してサービスにリンクされたロールを手動で作成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「[サービスリンクロールの作成](#)」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、サービスにリンクされた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AWSAPIでは、IAMを使用して、`license-manager.amazonaws.com`サービス名。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` のサービスにリンクされたロールの編集を許可しません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、IAMユーザーガイドの「[サービスにリンクされたロールの編集](#)」を参照してください。

License Managerのサービスにリンクされたロールを削除する

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、アクティブにモニタリングやメンテナンスがされているエンティティだけを所有します。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスにリンクされたロールのクリーンアップ

IAMを使用してサービスにリンクされたロールを削除するには、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。

サービスにリンクされたロールを手動で削除する

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](#) とも使用している場合は[AWSLicenseManagerMemberAccountRole](#)、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

`AWSServiceRoleForAWSLicenseManagerMasterAccountRole` と呼ばれるサービスにリンクされたロールは、License Manager が AWS リソースにアクセスして、ユーザーに代わって集中管理アカウントのライセンス管理アクションを管理することを可能にします。

`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 マネージドポリシー: `AWSLicenseManagerMasterAccountRolePolicy`](#)。サービスにリンクされた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「[サービスにリンクされたロールの権限](#)」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。AWS Management Consoleでクロスアカウントライセンス管理を設定すると、License Managerはサービスにリンクされたロールを自動的に作成します。

Note

License Managerでクロスアカウントsupportを利用するには、AWS Organizationsを使用する必要があります。

サービスにリンクされたロールを削除したが、再作成する必要がある場合は、同じプロセスで、アカウントにロールを再作成することができます。

サービスにリンクされたロールは、IAM コンソール、AWS CLI、または IAM API を使用して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「[サービスリンクロールの作成](#)」を参照してください。

Important

このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されません。2017年1月1日以前に License Manager を使用していた場合、サービスにリンクされた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. [Link AWS Organizations accounts] (AWS Organizations アカウントのリンク) を選択します。
4. [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AWSAPI では、IAM を使用して、`license-manager.master-account.amazonaws.com`サービス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、`AWSServiceRoleForAWSLicenseManagerMasterAccountRole` のサービスにリンクされたロールの編集を許可しません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、IAMユーザーガイドの「[サービスにリンクされたロールの編集](#)」を参照してください。

License Managerのサービスにリンクされたロールを削除する

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、アクティブにモニタリングやメンテナンスがされているエンティティだけを所有します。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールの手動による削除

IAM コンソール、AWS CLI、または AWS API を使用して、`AWSServiceRoleForAWSLicenseManagerMasterAccountRole` の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

`AWSServiceRoleForAWSLicenseManagerMemberAccountRole` と呼ばれるサービスにリンクされたロールは、License Manager がユーザーに代わって構成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ための AWS リソースにアクセスすることを可能にします。

`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 マネージドポリシー: AWSLicenseManagerMemberAccountRolePolicy](#)。サービスにリンクされた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「[サービスにリンクされたロールの権限](#)」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

サービスにリンクされたロールを手動で作成する必要はありません。設定ページでは、AWS Organizations License Manager コンソールの管理アカウントからとの統合を有効にできます。AWS CLI (`runupdate-service-settings`) または AWS API (コール) `UpdateServiceSettings` を使ってこれができます。この操作を行うと、License Manager によって、Organizations メンバーアカウントにサービスにリンクされたロールが作成されます。

サービスにリンクされたロールを削除したが、再作成する必要がある場合は、同じプロセスで、アカウントにロールを再作成することができます。

IAM コンソール、AWS CLI、または AWS API を使用してサービスにリンクされたロールを手動で作成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「[サービスリンクロールの作成](#)」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、サービスにリンクされた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. [Link AWS Organizations accounts] (AWS Organizations アカウントのリンク) を選択します。
5. [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にリンクされたロールを作成するには、IAM コンソールも使用できます。AWS CLI または AWS API で、`license-manager.member-account.amazonaws.com` サービス名を使用してサービスリンク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` のサービスにリンクされたロールの編集を許可しません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。

ただし、IAM を使用したロールの説明の編集はできません。詳細については、IAMユーザーガイドの「[サービスにリンクされたロールの編集](#)」を参照してください。

License Managerのサービスにリンクされたロールを削除する

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、アクティブにモニタリングやメンテナンスがされているエンティティだけを所有します。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールの手動による削除

IAM コンソール、AWS CLI、または AWS API を使用して、AWSServiceRoleForAWSLicenseManagerMemberAccountRole の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 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、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

AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService と呼ばれるサービスにリンクされたロールにより、License Manager は AWS Systems Manager を利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 Amazon EC2 リソースを管理したり、AWS Directory Service リソースを記述したりできます。

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 マネージドポリシー: AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)。サービスにリンクされた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「[サービスにリンクされたロールの権限](#)」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

サービスにリンクされたロールは、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。

サービスにリンクされたロールは、IAM コンソール、AWS CLI、または IAM API を使用して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「[サービスリンクロールの作成](#)」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にリンクされたロールを作成するには、IAM コンソールも使用できます。AWS CLI または AWS API で、`license-manager-user-subscriptions.amazonaws.com` サービス名を使用してサービスリンク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` のサービスにリンクされたロールの編集を許可しません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、IAM ユーザーガイドの「[サービスにリンクされたロールの編集](#)」を参照してください。

License Manager のサービスにリンクされたロールを削除する

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、アクティブにモニタリングやメンテナンスがされているエン

ティティだけを所有します。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールの手動による削除

IAM コンソール、AWS CLI、または AWS API を使用して、`AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` の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 では、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に、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

`AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` と呼ばれるサービスにリンクされたロールにより、License Manager は Amazon EC2 と AWS Organizations リソースを検出して Linux サブスクリプションの使用状況を集計できます。

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](#)。サービスにリンクされた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「[サービスにリンクされたロールの権限](#)」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

サービスにリンクされたロールは、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。

サービスにリンクされたロールは、IAM コンソール、AWS CLI、または IAM API を使用して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「[サービスリンクロールの作成](#)」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 コ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には、IAM コンソールも使用できます。AWS CLI または AWS API で、`license-manager-linux-subscriptions.amazonaws.com` サービス名を使用してサービスリンク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` のサービスにリンクされたロールの編集を許可しません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、IAM ユーザーガイドの「[サービスにリンクされたロールの編集](#)」を参照してください。

License Manager のサービスにリンクされたロールを削除する

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、アクティブにモニタリングやメンテナンスがされているエンティティだけを所有します。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールの手動による削除

IAM コンソール、AWS CLI、または AWS API を使用し

て、`AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` の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。

AWS の AWS License Manager マネージドポリシー

ユーザー、グループ、ロールにアクセス権限を追加するには、自分でポリシーを作成するよりも、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 カスタム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。すぐに使用を開始するために、AWS マネージドポリシーを使用できます。これらのポリシーは、一般的なユースケースを対象範囲に含めており、AWS アカウントで利用できます。AWS マネージドポリシーの詳細については、「IAM ユーザーガイド」の「[AWS マネージドポリシー](#)」を参照してください。

AWS のサービスは、AWS マネージドポリシーを維持および更新します。AWS マネージドポリシーの許可を変更することはできません。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 マネージドポリシーから権限を削除しないため、ポリシーの更新によって既存の権限が破棄されることはありません。

さらに、AWS では、複数のサービスにまたがるジョブ機能のためのマネージドポリシーもサポートしています。例えば、ReadOnlyAccess AWS マネージドポリシーでは、すべての AWS のサービスおよびリソースへの読み取り専用アクセスを許可します。あるサービスで新しい機能を立ち上げる場合は、AWS は、追加された演算とリソースに対し、読み込み専用の権限を追加します。ジョブ機能ポリシーの一覧と説明については、「IAM ユーザーガイド」の「[AWS 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 マネージドポリシー: AWSLicenseManagerServiceRolePolicy

このポリシーは、AWSServiceRoleForAWSLicenseManagerRole 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、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、「[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。

[アクション]	リソースARN
iam:CreateServiceLinkedRole	arn:aws:iam::*:role/aws-service-role/license-

[アクション]	リソースARN
	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-*
sns:Publish	arn:aws::sns::*:aws-license-manager-service-*
sns:ListTopics	*
ec2:DescribeInstances	*
ec2:DescribeImages	*
ec2:DescribeHosts	*
ssm:ListInventoryEntries	*

[アクション]	リソースARN
ssm:GetInventory	*
ssm:CreateAssociation	*
organizations:ListAWSServiceAccessForOrganization	*
organizations:DescribeOrganization	*
organizations:ListDelegatedAdministrators	*
license-manager:GetServiceSettings	*
license-manager:GetLicense*	*
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:List*	*

でこのポリシーのアクセス許可を表示するにはAWS Management Console、「」を参照してください[AWSLicenseManagerServiceRolePolicy](#)。

AWS マネージドポリシー: 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。

[アクション]	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-*
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/*

[アクション]	リソースARN
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。
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	*

[アクション]	リソースARN
ram:GetResourceShareAssociations	*
ram:TagResource	*
ram:CreateResourceShare	*
ram:AssociateResourceShare	*
ram:DisassociateResourceShare	*
ram:UpdateResourceShare	*
ram>DeleteResourceShare	*
resource-groups:PutGroupPolicy	*
iam:GetRole	*
iam:PassRole	arn:aws:iam::*:role/ LicenseManagerServiceResourceDataSyncRole*
cloudformation:UpdateStack	arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:CreateStack	arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*

[アクション]	リソースARN
<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 アクション用に定義されているリソースは次のとおりです。

- `arn:aws:glue:*:*:catalog`
- `arn:aws:glue:*:*:crawler/LicenseManagerResourceSynDataCrawler`
- `arn:aws:glue:*:*:job/LicenseManagerResourceSynDataProcessJob`
- `arn:aws:glue:*:*:table/license_manager_resource_inventory_db/*`
- `arn:aws:glue:*:*:table/license_manager_resource_sync/*`
- `arn:aws:glue:*:*:database/license_manager_resource_inventory_db`
- `arn:aws:glue:*:*:database/license_manager_resource_sync`

でこのポリシーのアクセス許可を表示するにはAWS Management Console、「」を参照してください[AWSLicenseManagerMasterAccountRolePolicy](#)。

AWS マネージドポリシー:

AWSLicenseManagerMemberAccountRolePolicy

このポリシーは、`AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 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、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。

[アクション]	リソースARN
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:GetLicenseConfiguration	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*
ssm:CreateAssociation	*
ssm:CreateResourceDataSync	*
ssm>DeleteResourceDataSync	*
ssm:ListResourceDataSync	*
ssm:ListAssociations	*
ram:AcceptResourceShareInvitation	*
ram:GetResourceShareInvitations	*

でこのポリシーのアクセス許可を表示するにはAWS Management Console、「」を参照してください [AWSLicenseManagerMemberAccountRolePolicy](#)。

AWS マネージドポリシー: 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、「[ライセンス使用量](#)」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 Management Console」の「[AWSLicenseManagerConsumptionPolicy](#)」を参照してください。

AWS マネージドポリシー:

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

このポリシーは、AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService 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、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。

[アクション]	リソースARN
ds:DescribeDirectories	*
ds:GetAuthorizedApplicationDetails	*
ec2:CreateTags	arn:aws:ec2:*:*:instance/* ¹
ec2:DescribeInstances	*
ec2:DescribeVpcPeeringConnections	*
ec2:TerminateInstances	arn:aws:ec2:*:*:instance/* ¹
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 Management Console、「」を参照してください[AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)。

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にリンクされたロールに添付され、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。

[アクション]	リソースARN
<code>ec2:DescribeInstances</code>	*
<code>ec2:DescribeRegions</code>	*
<code>organizations:DescribeOrganization</code>	*
<code>organizations:ListAccounts</code>	*
<code>organizations:DescribeAccount</code>	*
<code>organizations:ListChildren</code>	*
<code>organizations:ListParents</code>	*
<code>organizations:ListAccountsForParent</code>	*
<code>organizations:ListRoots</code>	*
<code>organizations:ListAWSServiceAccessForOrganization</code>	*

[アクション]	リソースARN
<code>organizations:ListDelegatedAdministrators</code>	*

でこのポリシーのアクセス許可を表示するにはAWS Management Console、「」を参照してください[AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)。

AWSマネージドポリシーへの License Manager 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 管理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
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy - 新しいポリシー	License Manager が、AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService という名前のサービスにリンクされた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 と Amazon EC2 リソースを一覧表示する License Manager 権限を提供します。	2022 年 12 月 21 日
AWSLicenseManagerUserSubscriptionsServiceRolePolicy - 既存ポリシーへの更新	License Manager が <code>ec2:DescribeVpcPeeringConnections</code> 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	2022 年 7 月 18 日

変更	説明	日付
	<p>う名前のサービスにリンクされたロールを作成する権限を追加しました。このロールは、AWS Directory Service リソースの一覧表示、Systems Manager 機能の利用、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ための License Manager の権限を付与します。</p>	
<p>AWSLicenseManagerMasterAccountRolePolicy – 既存ポリシーへの更新</p>	<p>License Manager は、AWS Resource Access Manager によって管理されるリソースグループの <code>resource-groups:PutGroupPolicy</code> 権限を追加しました。</p>	<p>2022 年 6 月 27 日</p>
<p>AWSLicenseManagerMasterAccountRolePolicy – 既存ポリシーへの更新</p>	<p>License Manager は、AWS Resource Access Manager 用の AWS マネージドポリシー <code>AWSLicenseManagerMasterAccountRolePolicy</code> 条件キーを <code>ram:ResourceTag</code> の使用から <code>aws:ResourceTag</code> に変更しました。</p>	<p>2021 年 11 月 16 日</p>
<p>AWSLicenseManagerConsumptionPolicy - 新しいポリシー</p>	<p>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。</p>	<p>2021 年 8 月 11 日</p>

変更	説明	日付
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、AWSServiceRoleForAWSLicenseManagerMemberAccountRole という名前のサービスにリンクされたロールを作成する権限が追加されていました。	2021年6月16日
AWSLicenseManagerServiceRolePolicy – 既存ポリシーへの更新	License Managerは、ライセンス設定、ライセンス、権限など、すべてのLicense Managerリソースを一覧表示する権限を追加しました。	2021年6月15日
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にリンクされたロールを作成する権限を追加しました。このロールはAWS MarketplaceLicense Managerでライセンスを作成および管理する権限を持つ。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	Systems Manager がAWSマネージドポリシーの変更の追跡を開始しました。	2021年3月9日

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には、License Manager AWS KMS key は ISV に属し、() で保護されているアシンメトリックを使用します。AWS Key Management Service AWS KMS 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。key pair プライベートな部分は決して消えません AWS KMS。の非対称暗号について詳しくは AWS KMS、[「対称鍵と非対称鍵の使用」](#)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と [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の顧客管理型の 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、AWS KMS ライセンス管理者が ARN または ID を含む消費構成を作成します。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": "ABCDEFGHJI"
  }
}
```

のコンプライアンス検証 AWS License Manager

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、コンプライアンスプログラム [AWS のサービスによる対象範囲内のコンプライアンスプログラム](#) を参照し、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、[「でのレポートのダウンロード AWS Artifact」](#)の「」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービスは、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。は、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- [セキュリティとコンプライアンスのクイックスタートガイド](#) – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS をにデプロイする手順について説明します。

- [アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ](#) — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

Note

すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「[HIPAA 対応サービスのリファレンス](#)」を参照してください。

- [AWS コンプライアンスリソース](#) – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- [AWS カスタマーコンプライアンスガイド](#) — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス、複数のフレームワーク (米国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「[デベロッパーガイド](#)」の「[ルールによるリソースの評価](#)」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。AWS Config
- [AWS Security Hub](#) – これにより AWS のサービス、内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「[Security Hub のコントロールリファレンス](#)」を参照してください。
- [Amazon GuardDuty](#) – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- [AWS Audit Manager](#) – これにより AWS のサービス、AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

AWS License Manager での耐障害性

AWS の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として構築されます。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、耐障害性、および拡張性が優れています。

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。

AWS License Manager で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 AWS がインフラストラクチャ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 AWS 環境を設計するには、「セキュリティの柱 - AWS Well-Architected Framework」の「[インフラストラクチャ保護](#)」を参照してください。

AWSが発行している 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 および TLS 1.3 をお勧めします。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートです。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。

また、リクエストは、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、[AWS Security Token Service](#) (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

AWS 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、NAT デバイス、VPN 接続、AWS Direct Connect 接続のいずれも必要とせずに ライセンスマネージャ API にプライベートにアクセスするために使用できる技術である [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": [  
    {  
      "Action": "license-manager:Describe*",  
      "Effect": "Allow",  
      "Resource": "*" }  
    ]  
}
```

```
{
  "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。

トラブルシューティング AWS License Manager

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[AWS License Manager での設定](#)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段階的なアップグレード](#)」を参照してください。

管理アカウントは、自己管理ライセンスとリソースの関連付けを解除することはできません。

組織のいずれかのメンバーアカウントにおいて

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。更新スクリプトを実行する頻度は、LicenseManagerResourceSynDataProcessJobTrigger AWS Glue 管理アカウントのコンソールで編集することで変更できます。

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は失敗します。

[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。

のドキュメント履歴 AWS License Manager

次の表では、のリリースについて説明しています AWS License Manager。

変更	説明	日付
Amazon RDS による Db2 vCPU ベースの BYOL ライセンスのサポートが追加されました	License Manager は、Amazon RDS の 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 Amazon EC2 上の Microsoft Office LTSC Professional Plus 2021 のライセンスにより、Amazon マシンイメージ (AMI) に Windows Server 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、自己管理型の Active Directory ドメインのユーザーが、ディレクトリとの信頼関係が確立された場合にユーザーベースのサブスクリプションを利用できるようにするサポートを追加しました。AWS Managed Microsoft AD	2023 年 9 月 6 日
Ubuntu LTS サブスクリプションのライセンスタイプ変換	License Manager 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

変更	説明	日付
有効なグラントの置き換え	License Manager では、グラントアクティベーション中に、付与されたライセンスに対して有効なグラントを置き換えるオプション機能が追加されました。	2023 年 3 月 31 日
Linux サブスクリプションの委任管理	License Manager で、Linux サブスクリプションの委任管理者のサポートが追加されました。	2023 年 3 月 3 日
Linux サブスクリプション	License Manager で、商用 Linux サブスクリプションの追跡が追加されました。	2022 年 12 月 21 日
Amazon CloudWatch メトリクス	License Manager は、CloudWatch ライセンス構成の使用状況とサブスクリプションに関するメトリックを出力するようになりました。	2022 年 12 月 21 日
ユーザーベースのサブスクリプション用 Microsoft Office	License Manager で、ユーザーベースのサブスクリプションのサポート対象ソフトウェアとして Microsoft Office が追加されました。	2022 年 11 月 28 日
権限の組織単位への配布	組織内の特定の OU に権限を配布します。	2022 年 11 月 17 日
組織全体のビュー (コンソール)	License Manager AWS Organizations コンソールを使用して、アカウント全体で付与されたライセンスを管理します。	2022 年 11 月 11 日

変更	説明	日付
ユーザーベースのサブスクリプション	Amazon EC2 でサポートされているユーザーベースのサブスクリプション製品を利用します。	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)	License Manager コンソールを使用して、既存のワークロードを再デプロイせずに、ライセンスタイプを「AWS提供ライセンス」と「Bring Your Own License Model (BYOL)」に変更します。	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せずに、を使用してライセンスタイプを「AWS提供ライセンス」と「BYOL (BYOL)」に変更します。 AWS CLI	2021年9月22日
権利の共有	1回のリクエストで、マネージドライセンス権限を組織全体で共有できます。	2021年7月16日
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

変更	説明	日付
自動検出除外ルール	AWS アカウント ID とタグに基づいて、License Manager の自動検出からインスタンスを除外します。	2021年3月5日
マネージドエンタイトルメント	License AWS Marketplace Managerを使用してライセンスを配布している販売元から購入した製品および販売者のライセンス資格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
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

変更	説明	日付
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
オンプレミスのリソースにライセンスを添付します	ライセンスをオンプレミスのインスタンスにアタッチすると、License Manager は定期的にソフトウェアインベントリを収集し、ライセンス情報を更新し、使用状況をレポートします。	2019年3月8日
AWS License Manager 初回リリース	初回サービス起動	2018年11月28日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。