
AWS License Manager

ユーザーガイド



AWS License Manager: ユーザーガイド

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

Amazon の商標およびトレードドレスは、お客様に混乱を招く可能性が高い方法、または Amazon の評判もしくは信用を損なう方法で、Amazon が所有しない製品またはサービスと関連付けて使用することはできません。Amazon が所有しない商標はすべてそれぞれの所有者に所属します。所有者は必ずしも Amazon と提携していたり、関連しているわけではありません。また、Amazon の後援を受けているとはかぎりません。

Table of Contents

AWS License Manager とは	1
管理された使用権限の確認	1
関連サービス	2
License Manager	3
開始方法	5
License Manager	6
ライセンス設定	7
パラメータとルール	7
ベンダーライセンスからルールを構築する	8
ライセンス設定を作成します。	9
ライセンス設定の共有	11
ライセンス設定の編集	11
ライセンス設定の無効化を行います。	11
ライセンス設定の削除	12
ライセンスルール	12
ライセンス設定と AMI の関連付け	13
ライセンス設定と AMI の関連付けの解除	13
ライセンスレポート	14
レポートジェネレータの作成	14
レポートジェネレータの編集	15
レポートジェネレータの削除	15
ライセンスタイプの変換	15
対象となるライセンスタイプ	16
Prerequisites	17
ライセンスタイプの変換	17
テナント属性変換	20
トラブルシューティング	21
ホストリソースグループ	21
ホストリソースグループの作成	22
ホストリソースグループの共有	23
ホストリソースグループでのインスタンスの作成	23
ホストリソースグループの変更	23
ホストリソースグループの削除	23
ホストリソースグループへのDedicated Host の追加	24
ホストリソースグループからDedicated Host を削除する	24
リソースインベントリ	25
リソースインベントリを検出	25
リソースインベントリの自動検出	27
許可されたライセンス	29
付与されたライセンスの管理	29
使用権限の分散	30
承認とアクティブーションの付与	31
への分散AWS Organizations	31
ライセンスのステータス	32
販売者が発行したライセンス	32
Entitlements	33
ライセンス使用量	33
Requirements	34
出品者が発行したライセンスの作成	35
顧客へのライセンスの付与	36
ユーザーの一時的な認証情報の取得AWSアカウント	36
消費されたライセンス	36
出品者が発行したライセンスの削除	37
委任された管理	37

レジスタ (コンソール)	38
登録解除 (コンソール)	39
レジスタする (AWS CLI)	39
レジスタを解除する (AWS CLI)	39
設定	40
ダッシュボード	41
セキュリティ	42
データ保護	42
保管時の暗号化	43
Identity and access management	43
ポリシーの構造	43
License Manager を使用した ISV のポリシー	44
License Manager のポリシーの例	44
サービスリンクロール	45
Core ロール	45
管理アカウントのロール	48
メンバーアカウントのロール	52
AWS 管理ポリシー	54
AWSライセンスマネージャーサービスポリシーポリシー	54
AWSライセンスマネージャーマスターアカウントポリシー	54
AWSライセンスマネージャーメンバーアカウントポリシー	54
AWSライセンスマネージャーの消費ポリシー	55
ポリシーの更新	55
ライセンス署名	56
コンプライアンス検証	57
耐障害性	57
インフラストラクチャセキュリティ	58
VPC エンドポイント (AWS PrivateLink)	58
License Manager のインターフェイス VPC エンドポイントの作成	58
License Manager の VPC エンドポイントポリシーの作成	59
トラブルシューティング	60
クロスアカウント検出エラー	60
マスターアカウントは、ライセンス構成からリソースの関連付けを解除できません	60
Systems Manager のインベントリは、最新のものではありません	60
登録解除された AMI の見かけ上の永続性	61
新しい子アカウントインスタンスがリソースインベントリに表示されるのが遅い	61
クロスアカウントモードを有効にすると、子アカウントインスタンスの表示が遅くなる	61
クロスアカウント検出を無効にすることはできません	61
子アカウントユーザーは、共有ライセンス設定をインスタンスに関連付けることができません。	61
Linking (リンク中)AWS Organizationsアカウント失敗	62
CloudTrail	63
CloudTrail のLicense Manager 情報	63
License Manager のログファイルエントリについて	64
ドキュメント履歴	65
.....	lxvii

AWS License Manager とは

AWS License Managerは、ソフトウェアベンダー (Microsoft、SAP、Oracle、IBM など) のソフトウェアライセンスをAWSオンプレミス環境と統合することができます。これにより、ライセンスの使用状況を制御および可視化できるため、ライセンスの超過分を制限し、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をAWSでは、自分のライセンス使用 (BYOL) を使用することにより、コストを削減できます。つまり、クラウドリソースで使用するために、既存のライセンスインベントリを再利用することができます。

License Manager は、ライセンス超過使用やペナルティのリスクを低減します。AWSのサービス。管理者は、ライセンスの消費についてルールベースのコントロールを使用することにより、新規および既存のクラウドのデプロイにソフトリミットまたはハードリミットを設定できます。これらの制限に基づいて、License Managerは、準拠していないサーバの使用を発生前に停止するのに役立ちます。

License Manager の組み込みダッシュボードは、ライセンス使用の継続的な可視性を提供し、ベンダー監査をサポートします。

License Manager は、仮想コア (vCPUs)、物理コア、ソケット、またはマシン数に基づいてライセンスされている、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。

とAWS 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、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。また、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ているエンドユーザーのIDと基になるリソース識別子 (利用可能な場合) も追跡します。この時系列データは、CloudWatchのメトリックスとイベントを通じてISVに追跡できます。ISVは、分析、監査、およびその他の同様の目的にこのデータを使用できます。

AWS License Managerはと統合されています [AWS Marketplace](#) および [AWSData Exchange](#)とを次のAWSサービス:[AWS Identity and Access Management \(IAM\)](#),[AWS Organizations](#)、[Service Quotas](#)、[AWS CloudFormation](#),AWSリソースへのタグ付け[AWS X-Ray](#)。

管理対象使用権限の確認

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、追跡できます。

独立系ソフトウェアベンダー (ISV) はAWS License Managerを使用して、管理されたエンタイトルメントを使用してソフトウェアライセンスとデータをエンドユーザーに管理および配布できます。発行者は、License Manager ダッシュボードを使用して、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。販売するISV AWS Marketplaceは、トランザクションワークフローの一部としてライセンスの自動作成と配布のメリットを享受できます。また、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。

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、顧客が暗号で真正性を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ます。ノードロックが必要なライセンスを持っている場合、License Managerはそのようにライセンスを消費するメカニズムを提供します。

ライセンスを作成するには、AWS License Managerで生成されたデジタル署名トークンを使用して、IAM IDを使用してエンドユーザーに配布するか、AWS License Manager。使用するエンドユーザーAWSは、

ライセンス資格をさらに再配布できます。AWSそれぞれの組織のアイデンティティ。分散エンタイトルメントを持つエンドユーザーは、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。AWS License Manager。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 (10 のチェックアウトなど) を指定します。admin-users を 1 時間。このチェックアウトは、分散ライセンスの基になる IAM ID に基づいて実行するか、AWS License Manager からAWS License Managerサービス。

関連 サービス

License Manager は Amazon EC2 と統合されているため、以下のリソースのライセンスを追跡できます。

- EC2 インスタンス
- [Dedicated Instances](#)
- [Dedicated Hosts](#)
- スポットインスタンスとスポットフリート
- [Systems Manager のマネージドインスタンス](#)

License Manager は Amazon RDS と統合されているため、Amazon RDS での Oracle ライセンスの使用状況を監視できます。詳細については、「」を参照してください。[Oracle のライセンス\(\)](#)Amazon RDS ユーザーガイド。

License Manager と併用するAWS Systems Managerでは、以外でホストされる物理サーバーや仮想サーバーのライセンスを管理できます。AWS。

License Manager を使用して、から取得した BYOL ソフトウェアを追跡できます。 [AWS Marketplace](#) 。

License Manager はAWS Organizationsを使用して、すべての組織アカウントを一元管理します。

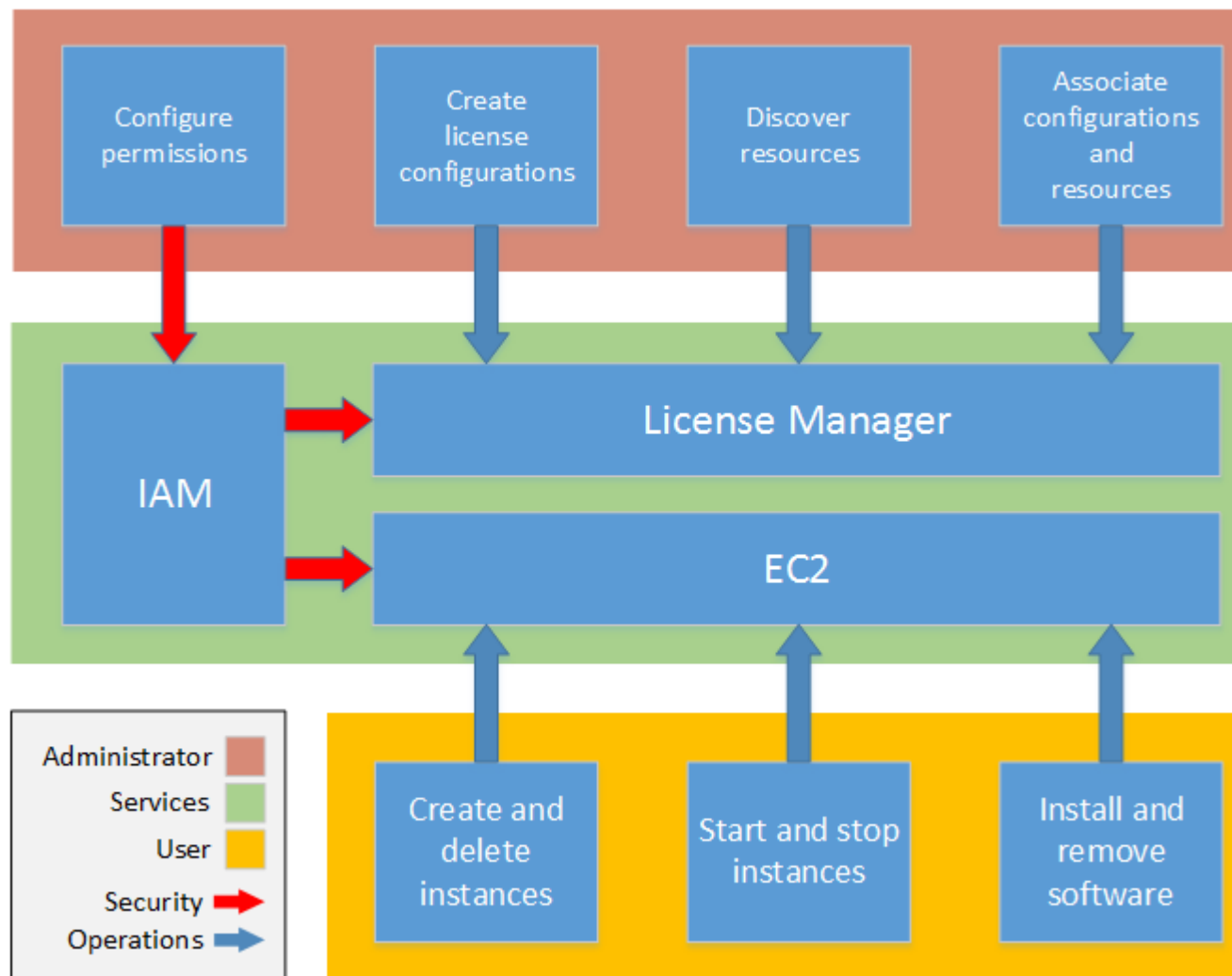
License Manager

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。その場合、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が問題になります。License Manager は、さまざまなドメインの知識をプールする方法を提供します。重要な意味では、それはまた AWS サービスの活用により、インスタンスの作成や削除を行う Amazon EC2 コントロールプレーンなどのつまり、License Manager のルールと制限は、ビジネス上および運用上の知識の獲得を行い、インスタンスの作成とアプリケーションのデプロイメントの自動制御に変換できることを意味します。

次の図は、アクセス許可を管理して License Manager を構成するライセンス管理者と、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、責任分担が区分されつつ協調されていることを示しています。



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、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、ルールベースのライセンス設定の作成、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、ライセンス設定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、あるライセンス設定を、IT 部門がすべての Amazon EC2 インスタンスデプロイメント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 を使用すると、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 は、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、ライセンスの消費量と追跡されたリソースを表示する組み込みのダッシュボードにより、レポート作成

AWS License Manager の開始方法

の使用を開始するにはAWS License Managerで、License Manager コンソールにログインします。

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/>。License Manager およびそのサポートサービスについてアクセス権限を設定するよう求められます。指示に従います。
2. ライセンス設定を作成してAMI およびインスタンスにアタッチします。
3. 組み込みのダッシュボードを使用して、インスタンスを起動し、ライセンスの使用状況を追跡します。

AWS License Manager の使用

License Manager は、インフラストラクチャが混在する企業の標準的なシナリオに適用できます。AWSリソースとオンプレミスリソースの両方を使用します このセクションを読むと、ライセンス設定の作成、ライセンスを消費するリソースのインベントリの作成、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ができるようになります。

AWS Marketplace 製品のライセンス

License Manager を使用して、ライセンスマネージャーを AWS Marketplace Amazon EC2 起動テンプレートを使用した BYOL AMI 製品AWS CloudFormationテンプレート (複数)AWS Service Catalogの製品。いずれの場合も、集中型のライセンス追跡とコンプライアンス遵守によるメリットを得ることができます。

Note

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

オンプレミスデータセンターのリソースのライセンスの追跡

License Manager を使用すると、AWSとの[Systems Manager Inventory](#)をクリックし、ライセンスルールをアタッチします。License Rules をアタッチすると、オンプレミスサーバーをAWSリソースを License Manager コンソールから削除します。

含まれるライセンスと BYOL の区別

License Manager を使用すると、製品に付属しているライセンスを持つリソースと、所有しているライセンスを使用するリソースを特定できます。これにより、BYOL ライセンスの使用状況を正確にレポートできます。このフィルタには、SSM バージョン 2.3.722.0 以降が必要です。

License ManagerAWSアカウント

License Manager を使用すると、AWSアカウント。ライセンス構成は、AWS Organizations管理アカウントを使用してアカウント間で共有し、AWS Resource Access ManagerまたはリンクによってAWS Organizationsアカウント:License Manager の設定を使用します。これにより、クロスアカウント検出を実行して、クロスアカウント検出を実行して、AWSアカウント。ただし、以下のリージョンでは、AWSアカウント:

- 中国 (北京)
- 中国 (寧夏)

目次

- [ライセンスマネージャのライセンス構成 \(p. 7\)](#)
- [ライセンスマネージャのライセンス規則 \(p. 12\)](#)
- [ライセンスマネージャでのライセンスレポート \(p. 14\)](#)
- [ライセンスマネージャでのライセンスタイプ変換 \(p. 15\)](#)
- [のホストリソースグループAWS License Manager \(p. 21\)](#)
- [License Manager のリソースインベントリ \(p. 25\)](#)
- [ライセンスマネージャで付与されたライセンス \(p. 29\)](#)
- [出品者は、でライセンスを発行しましたAWS License Manager \(p. 32\)](#)

- [委任された管理者の登録 \(p. 37\)](#)
- [License Manager の設定 \(p. 40\)](#)
- [License Manager 内のダッシュボード \(p. 41\)](#)

ライセンスマネージャのライセンス構成

ライセンス設定は、License Manager の中核をなすものです。それらにはエンタープライズ契約の条項に基づくライセンスルールが含まれています。作成するルールによって、AWSライセンスを消費するコマンドを処理します。ライセンス設定を作成する際には、組織のコンプライアンスチームと密接に協力して、お使いのエンタープライズ契約を確認してください。

Limits

- リソースあたりのライセンス設定の数: 10
- ライセンス設定の合計数: 25
- Systems Manager 管理対象インスタンスは、vCPU およびインスタンスタイプのライセンス構成に関連付ける必要があります。

目次

- [ライセンス設定パラメータとルール \(p. 7\)](#)
- [ベンダーライセンスからライセンスマネージャールを構築する \(p. 8\)](#)
- [ライセンス設定を作成します。 \(p. 9\)](#)
- [ライセンス設定の共有 \(p. 11\)](#)
- [ライセンス設定の編集 \(p. 11\)](#)
- [ライセンス設定の無効化を行います。 \(p. 11\)](#)
- [ライセンス設定の削除 \(p. 12\)](#)

ライセンス設定パラメータとルール

ライセンス設定は、パラメータ値に応じて変化する基本的なパラメータとルールで構成されます。ライセンス設定にタグを追加することもできます。ライセンス設定を作成すると、管理者は、リソースニーズの変化を反映するようにライセンスの数と使用制限を変更できるようになります。

下記を含むパラメータやルールを使用できます。

- 名前— ライセンス設定の名前。
- 説明— ライセンス設定の説明。
- ライセンスカウントタイプ— ライセンスのカウントに使用される測定単位。サポートされている値は、物理コア、vCPU、ソケット、およびインスタンスです。
- (オプション) ライセンス数— この設定によって管理されるライセンスの数。
- (オプション) ライセンス数のハードリミット— ライセンス数で表される制限の種類。ハードリミットは、コンプライアンス違反のインスタンスの起動をブロックします。ソフトリミットでは、コンプライアンス違反の起動は許可されますが、発生した場合にアラートが送信されます。
- 消費ライセンスの数: リソースによって使用されるライセンス数。
- 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— 製品の名称とバージョン [自動検出 \(p. 27\)](#)。サポートされている製品は、Windows Server、SQL Server、Oracle Database 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、計数タイプによって異なります。

- ホストへのライセンスのアフィニティ (日単位) — 指定した日数の間、ライセンス使用量をホストに制限します。範囲は 1 ~ 180 です。カウントの種類は、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、ライセンスは 24 時間以内に再利用できるようになります。
- 最大コア— リソースのコア数の最大値です。
- 最大ソケット— リソースのソケットの最大数。
- vCPUs— リソースの vCPUs の最大数。
- 最小コア— リソースの最小コア数。
- 最小ソケット— リソースの最小ソケット数です。
- vCPUs— リソースの vCPUs の最小数。
- 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。カウントの種類がコアまたはソケットの場合は、Dedicated Hostsが必要で、Dedicated Hostsがサポートされます。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、ハードウェア専用ホスト、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 CPU の最適化がサポートされています。これにより、インスタンス上の vCPUs 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、License Manager は、インスタンスタイプの vCPUs の既定数をカウントします。

次の表に、各カウントタイプで使用できるライセンスルールを示します。

コンソール名	API 名	コア	インスタンス	ソケット	vCPU
ホストへのライセンスのアフィニティ (日単位)	licenseAffinityToHost	◆		◆	
最大コア	maximumCores	◆	◆		
最大ソケット	maximumSockets		◆	◆	
vCPUs	maximumVcpus		◆		◆
最小コア	minimumCores	◆	◆		
最小ソケット	minimumSockets		◆	◆	
vCPUs	minimumVcpus		◆		◆
テナンシー	allowedTenancy	◆	◆	◆	◆
vCPU の最適化	honorVcpuOptimization				◆

ベンダーライセンスからライセンスマネージャーを構築する

License Manager のルールセットは、ソフトウェアベンダーライセンスの言語に基づいて作成できます。以下の例は、実際のユースケースのブループリントを意図している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規定は、AWS の要件や制限とも相互に影響があります。アプリケーションに必要なライセンスの数は、選択したインスタンスタイプやその他の要因によって異なります。

Important

AWS は、ソフトウェアベンダーとの監査プロセスには参加しません。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 License Manager にルールを注意深く理解してキャプチャする必要があります。

例: オペレーティングシステムライセンスの実装

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を、取得して自動化するベンダーライセンス要件と関連付けています。例の値は説明のみを目的としており、必要な値は独自のライセンス設定で指定する必要があります。

License Manager 規則	設定
ライセンスカウントタイプ	ライセンスタイプは、 に設定されます。 Cores 。
ライセンス数	コアの数は、 に設定されます。 96 。
vCPUs またはコアの最小数と最大数	最小コアは、 に設定されます。 8 。 最大コアは、 に設定されます。 16 。
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	テナンシーは、 に設定されます。 Dedicated Host 。

ライセンス設定を作成します。

ライセンス構成は、ソフトウェアベンダーとの契約のライセンス条項を表します。ライセンス設定では、ライセンスのカウント方法 (vCPUs やインスタンス数など) を指定します。また、使用量の制限も指定さ

れるため、割り当てられたライセンス数を超える使用を防ぐことができます。さらに、テナンシータイプなど、ライセンスの他の制約を指定することもできます。

Oracle Database 製品の要件

製品情報を追加してOracle Database製品の自動検出を構成する場合、次の要件が適用されます。

- サポートされているライセンス数カウントの種類はvCPU。
- 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ていません。
- ライセンス構成ごとに1つの製品バージョンを追跡できます。
- 同じライセンス構成を使用してOracle製品および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ライセンス設定を作成するには

1. License Manager コンソール (<https://console.aws.amazon.com/license-manager/>) を開きます。
2. 左のナビゲーションペインにて [ライセンス設定] を選択します。
3. [ライセンス設定の作成] を選択します。
4. [Configuration details] パネルで次の情報を入力します。
 - ライセンス設定名— ライセンス設定の名前。
 - 説明— ライセンス設定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)。
 - [数] <option>— 表示されるオプションは、ライセンスの種類によって異なります。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。
 - ライセンス制限を強制する— 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) 自動検出ルールパネルで、次の操作を行います。
 - a. 検出および追跡する各製品の製品名、製品タイプ、およびリソースタイプを選択します。 [自動検出 \(p. 27\)](#)。
 - b. Select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クリックして、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License Managerが検出した後でライセンスを再利用できるようにします。
 - c. (オプション) アカウントがOrganizations の License Manager 管理アカウントである場合は、自動検出から除外するリソースを定義する必要があります。これを行うには、 を選択します。除外ルールの追加で、フィルタリングするプロパティを選択し、AWSアカウント ID とリソースタグがサポートされている場合は、そのプロパティを識別するための情報を入力します。
6. (オプション) を展開します。タグパネルを使用して、ライセンス設定に1つ以上のタグを追加します。タグはキーと値のペアです。各タグに関する以下の情報を記述します。
 - キー— 検索可能なキー名です。
 - 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ライセンス設定を作成するには

- `create-license-configuration` (AWS CLI)

- [New-LICMLicenseConfiguration](#)(Tools for Windows PowerShell)

ライセンス設定の共有

次を使用できます。AWS Resource Access Managerを使用して、ライセンス設定を任意のAWSアカウントまたはAWS Organizations。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。

ライセンス設定の編集

ライセンス設定の次のフィールドの値を編集できます。

- 名前
- 説明
- ライセンス数
- ライセンス数のハードリミット

ライセンス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にて [ライセンス設定] を選択します。
3. ライセンス設定を選択します。
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。

コマンドラインを使用してライセンス設定を編集するには

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

ライセンス設定の無効化を行います。

ライセンス設定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。

ライセンス設定を無効化すると、実行中のインスタンスにアタッチできなくなります。無効化したライセンス設定は起動できなくなります。

ライセンス設定を無効化するには

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にて [ライセンス設定] を選択します。
3. ライセンス設定を選択します。
4. 選択アクション,Deactivate。確認を求められたら、[] を選択します。Deactivate。

コマンドラインを使用してライセンス設定を非アクティブにするには

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

ライセンス設定の削除

ライセンス設定を削除するには、まず、リソースの関連付けを解除する必要があります。新しいライセンス規則を使用して最初からやり直す必要がある場合は、ライセンス設定を削除できます。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、ライセンス設定を削除し、更新された条件を反映する新しいライセンス設定を作成し、既存のリソースに関連付けることができます。

コンソールを使用してライセンス設定を削除するには

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にて [ライセンス設定] を選択します。
3. ライセンス設定の名前を選択して、ライセンスの詳細ページを開きます。
4. 各リソースを (個別にまたは一括で) 選び、リソースの関連付けを解除する。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ライセンス設定を削除するには

- `delete-license-configuration` (AWS CLI)
- `Remove-LICMLicenseConfiguration`(Tools for Windows PowerShell)

ライセンスマネージャのライセンス規則

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

Important

AWS は、ソフトウェアベンダーとの監査プロセスには参加しません。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アタッチ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と、License Manager によって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 によってリソースの起動を妨げることができません。

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。

組織では運用やコンプライアンスへのアプローチが異なるため、License Manager では複数の起動メカニズムをサポートしています。

- ライセンス設定と AMI の手動による関連付け— 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ため、組織内での広い使用に公開する前に、ライセンスルールを AMI にアタッチ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、License Manager によって自動的に追跡されます。ライセンスルールは、現在の AMI 構築メカニズム () にアタッチすることもできます。 [Systems Manager Automation](#), [VM Import/Export](#), および [Packer](#)。
- Amazon EC2 起動テンプレートおよび AWS CloudFormation— AMI へのライセンスルールのアタッチを使用しない場合には、 [EC2 起動テンプレート](#) または [AWS CloudFormation テンプレート](#)。これらのテン

プレートを使用したデプロイメントは License Manager を使用して追跡されます。EC2 起動テンプレートでルールを適用するか、AWS CloudFormationテンプレートで 1 つ以上のライセンス構成 ID を指定することにより、ライセンス設定field.

AWS では、ライセンス追跡データをお客様の機密データとして扱います。このデータには、ライセンスを所有する AWS アカウントを通じてのみアクセスできます。AWS はお客様のライセンス追跡データにアクセスすることはできません。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。

ライセンス設定と 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、ライセンス設定と AMI を関連付ける方法を示します。この手順では、既に少なくとも 1 つのライセンス設定が行われてい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、ライセンス設定を関連付けることができます。AMI が共有されている場合は、現在のアカウントのライセンス設定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ライセンス設定に関連付けるか、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ライセンス設定に AMI を関連付けると、複数のアカウントにわたって AMI からのインスタンスの起動を追跡できます。ハード制限に達すると、License Managerは追加のインスタンスの起動をブロックします。ソフトリミットに達すると、追加のインスタンスの起動がLicense Managerによって通知されます。AMI をコピーしたり、AMI から起動されたインスタンスから AMI を作成したりするなど、別のメカニズムを使用して AMI にアクセスできないようにする必要があります。

ライセンス設定と 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にて [ライセンス設定] を選択します。
3. ライセンス設定の名前を選択し、ライセンス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 AMI。
4. 選択関連付け AMI。
5. を使用する場合利用可能な AMIで、1 つ以上の AMI を選択し、関連付け。
 - アカウントが AMI の少なくとも 1 つを所有している場合は、所有している AMI の AMI 関連付けスコープを選択するよう求められます。別のアカウントからと共有された AMI はすべて、自分のアカウントにのみ関連付けられます。[Confirm] を選択します。
 - AMI が別のアカウントから共有された場合、AMI は自分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 が関連付け AMI タブで、ライセンスの詳細ページを開きます。

ライセンス設定と 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、ライセンス設定と AMI の関連付けを解除する方法を示します。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。

ライセンス設定と 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にて [ライセンス設定] を選択します。
3. ライセンス設定の名前を選択し、ライセンス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 の関連付けを解除する。

ライセンスマネージャーでのライセンスレポート

を使用するAWS License Managerでは、ライセンス使用のスナップショットを定期的にスケジュールすることで、ライセンス構成の履歴を追跡できます。レポートジェネレータを設定することにより、License Manager は、お客様の仕様に基づいて、ライセンス設定のレポートを S3 バケットに自動的にアップロードします。複数のレポートジェネレータを設定して、環境内のさまざまな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レポートはに保存されません。License Manager レポートは S3 バケットに直接発行されます。レポートジェネレータを削除すると、レポートは S3 バケットに発行されなくなります。

レポートジェネレータの作成

レポートジェネレータを作成するときは、License Manager が追跡するライセンス構成タイプ、レポートを生成する頻度を定義する間隔、およびレポートタイプを指定します。すべてのレポートは CSV 形式で生成され、S3 バケットに発行されます。レポートジェネレータは、次のレポートタイプを 1 つ以上生成できます。

ライセンス設定レポート

このレポートタイプには、消費されたライセンス数に関する情報と、ライセンス構成に関する詳細が含まれます。追跡されたライセンス設定タイプが、ライセンス数、ライセンス規則、異なるリソースタイプ間でのライセンスの配布などの詳細とともに一覧表示されます。

リソースレポート

このレポートタイプでは、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表示されます。指定したライセンス設定タイプを使用する追跡対象の各リソースが、ライセンス ID、リソースのステータス、AWSリソースを所有するアカウント ID。

レポートジェネレータを作成するには

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、[レポート]。次に、[レポートジェネレータの作成] ペインでは、レポートのパラメータを定義します。
 - a. 「」 と入力します。名前オプションの説明あなたのジェネレータのために。
 - b. ドロップダウンリストからライセンス設定タイプを選択します。これは、レポートジェネレータがデータを生成する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。
 - e. (オプション) [タグをクリックして、レポートジェネレータリソースを追跡します。
3. Selectレポートジェネレータの作成。

新しいレポートジェネレータは、60 分以内にレポートの公開を開始します。

アカウントに関連付けられている S3 バケットがない場合は、レポートジェネレータの作成時に License Manager によってアカウントに新しい Amazon S3 バケットが作成されます。以前に有効にした場合クロスアカウントインベントリ検索レポートは、License Manager によって作成された S3 バケットに送信されます。クロスアカウントインベントリ検索が有効であった。

レポートは、以下の Amazon S3URI パターンでバケットに保存されます。

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

レポートジェネレータの編集

レポートジェネレータは、License Manager コンソールからいつでも表示および変更できます。-レポートジェネレータテーブルには、アカウント用に作成されたすべてのレポートジェネレータが一覧表示されます。テーブルから、さまざまなレポートの概要の取得、レポートジェネレータに関連付けられた Amazon S3 バケットへのピボット、レポート生成のステータスの表示を行うことができます。

レポートジェネレータを編集するには

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、[レポート]。
3. テーブルから編集するレポートジェネレータを選択し、[詳細を表示]。
4. Select編集をクリックして、レポートジェネレータを変更します。
5. レポートジェネレータに必要な変更を行い、[変更の保存]。

更新されたレポートジェネレータは、1 時間以内に新しいレポートを生成します。

Note

レポートジェネレータの名前を変更すると、新しい名前が反映されたレポートが License Manager S3 バケット内の新しいフォルダに送信されます。

レポートジェネレータの削除

レポートジェネレータを削除すると、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には影響しません。

Note

レポートジェネレータが関連付けられている場合、アカウントからライセンス設定を削除することはできません。まず、そのレポートジェネレータを削除する必要があります。

レポートジェネレータを編集するには

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、[レポート]。
3. テーブルから編集するレポートジェネレータを選択し、[詳細を表示]。
4. Select削除。このアクションは、レポートジェネレータを完全に削除します。

ライセンスマネージャでのライセンスタイプ変換

ライセンスの種類は、AWSのライセンスと Bring-Your-Own-License (BYOL) を使用することで、既存のワークロードを再デプロイする必要はありません。

ライセンスタイプの変換を使用して、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 に移行する

移行中に、ワークロードを Amazon EC2 にデプロイし、AWSライセンスが提供されます。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 BYOL に変更し、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します。

使用許諾契約の有効期限が満了してワークロードを継続する

マイクロソフトとのライセンス契約が期限切れになりつつあり、更新する予定がない場合は、License Manager のライセンスタイプ変換を使用して、BYOL からAWSライセンスが提供されます。このスイッチを使用すると、完全に準拠したソフトウェアライセンスで、ワークロードの実行を継続できます。AWS柔軟な従量制ライセンスモデルを採用しています。

コストを最適化

小規模なワークロードや不規則なワークロードでは、BYOL の実行よりもライセンスインクルードインスタンスの方が費用対効果が高い場合があります。これは、BYOL の長期コミットメントが必要になる場合があるためです。この場合、License Manager のライセンスタイプ変換を使用して、AWS は、ライセンス関連コストを最適化するためのライセンスを提供します。さらに、ワークロードが安定または予測可能な場合、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、BYOL に簡単に切り替えて、ソフトウェアベンダーから直接取得したライセンスメディアを使用できます。

ライセンスタイプ変換のトピック

- [ライセンスタイプ変換の対象となるライセンスタイプ \(p. 16\)](#)
- [Prerequisites \(p. 17\)](#)
- [ライセンスタイプの変換 \(p. 17\)](#)
- [テナント属性変換 \(p. 20\)](#)
- [ライセンスタイプ変換のトラブルシューティング \(p. 21\)](#)

ライセンスタイプ変換の対象となるライセンスタイプ

ライセンスタイプの変換は、Windows Server および SQL Server のライセンスで使用できます。

サポートされている SQL Server エディション:

- SQL Server Standard Edition
- SQL Server Enterprise Edition
- SQL Server Web Edition

変換タスクによって、インスタンスに関連付けられた使用状況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各プラットフォームの使用操作の値を示します。詳細については、「」を参照してください。[AMI 請求情報フィールド](#)。

プラットフォームの詳細	使用操作
Windows Server ライセンス込み	RunInstances:0002
Windows Server BYOL	RunInstances:0800
Windows Server ライセンス込み SQL Server Standard ライセンス込み	RunInstances:0006
Windows Server ライセンス込み SQL Server Enterprise ライセンス込み	RunInstances:0102
Windows Server ライセンス込み SQL Server Web ライセンス込み	RunInstances:0202
SQL Server (任意のエディション) に付属する Windows サーバーライセンス	RunInstances:0002

プラットフォームの詳細	使用操作
SQL Server の Windows サーバー BYOL (任意のエディション) BYOL	RunInstances:0800

Prerequisites

License Managerでライセンスタイプを変換するには、次の前提条件が満たされていることを確認します。

- あなたのAWSアカウントを License Manager にオンボーディングする必要があります。「[AWS License Manager の開始方法 \(p. 5\)](#)」を参照してください。
- ライセンスタイプを変換する前に、ターゲットインスタンスが停止状態になっている必要があります。ライセンス変換タスクが進行中の場合、ターゲットインスタンスを開始および停止できます。
- ターゲットインスタンスは、AWS Systems Manager インベントリには、以下のアクセス許可が含まれません。
 - `ssm:GetInventory`
 - `ssm:StartAutomationExecution`
 - `ssm:GetAutomationExecution`
 - `ssm:SendCommand`
 - `ssm:GetCommandInvocation`
 - `ssm:DescribeInstanceInformation`
 - `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 インベントリの詳細については、「[AWS Systems Manager Inventory](#)」。

- 元の Amazon EC2 インスタンスは、独自の仮想マシン (VM) イメージから起動する必要があります。VM を Amazon EC2 に変換する方法については、[を参照してください](#)。 [VM Import/Export](#)。 Amazon マシンイメージ (AMI) から最初に起動されたインスタンスは、ライセンスタイプを BYOL に変換することはできません。

ライセンスタイプの変換

ライセンスの種類を変換するには、AWS CLI。ライセンスタイプ変換タスクを作成すると、License Manager はインスタンスの請求製品を検証します。これらの事前検証が成功すると、License Manager はライセンスタイプ変換タスクを作成します。ライセンス変換タスクのステータスは、`list-license-conversion-tasks`および `get-license-conversion-task` AWS CLI コマンド。

License Manager は、変換タスクの一環として、カスタマー管理ライセンスに関連付けられたリソースを更新する場合があります。具体的には、お客様が管理するライセンスで、自動検出ルールが License

Includedの場合、License Manager はライセンスタイプ変換タスクのリソースとライセンスの関連付けを解除します。License Included自動検出ルールでは、リソースを明示的に除外します。

たとえば、カスタマー管理ライセンスに 2 つの自動検出ルールが含まれており、各ルールにライセンスを含む Windows Server が含まれていない場合、ライセンスタイプを BYOL からライセンスを含む Windows Server に変換すると、カスタマー管理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ルールを設定した場合、インスタンスは関連付け解除されません。

ライセンスタイプ変換タスクが成功すると、そのステータスは IN_PROGRESS ~ SUCCEEDED。License Manager でワークフロー中に問題が発生した場合、ライセンスタイプ変換タスクのステータスが FAILED し、ステータスメッセージをエラーメッセージで更新します。

Note

インスタンスの起動に使用される AMI の請求製品情報は、ライセンスタイプを変換しても変更されません。正確な請求情報を取得するには、Amazon EC2 `DescribeInstances` API。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`。

ライセンスタイプ変換のトピック

- [ライセンスタイプの変換制限](#) (p. 18)
- [ライセンスタイプは、AWS CLI](#) (p. 18)

ライセンスタイプの変換制限

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提供されており、その説明に頼る権利はありません。このドキュメントは、法的助言を構成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権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 販売店にお問い合わせください。

License Manager は、Microsoft サービスプロバイダーライセンス契約 (SPLA) に従って作成できるライセンス変換タスクの種類を制限します。ライセンスタイプ変換の対象となる制限を以下に挙げる。これは包括的なリストではなく、変更される可能性があります。

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

ライセンスタイプは、AWS CLI

ライセンスタイプ変換タスクを AWS CLI:

インスタンスのライセンスタイプの判別

1. がインストールされていることを確認し、セットアップします。AWS CLI。詳細については、「」を参照してください。[インストール](#)、[更新](#)、[アンインストール](#) [AWS CLI](#) および [設定](#): [AWS CLI](#)。
2. 実行するアクセス許可があることを確認します。 `create-license-conversion-task-for-resource` AWS CLI コマンドを実行します。このヘルプについては、[License Manager のポリシーの例](#) (p. 44)。
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、次のコマンドを実行します。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決定するインスタンスの ID に置き換えます。

```
aws ec2 describe-instances --instance-id <instance-id>
```

- 以下に、応答の例を示します。describe-instancesコマンドを実行します。
なお、UsageOperationの値は、ライセンスに関連付けられた請求情報コードです。-UsageOperationUpdateTimeは、請求コードが更新された時刻です。詳細については、「」を参照してください。 [DescribeInstances](#)のAmazon EC2 API リファレンス。

```
"InstanceId": "<instance-id>",  
"Platform details": "Windows with SQL Server Enterprise",  
"UsageOperation": "RunInstances:0800",  
"UsageOperationUpdateTime": "2021-08-16T21:16:16.000Z"
```

Note

SQL エンタープライズ BYOL を使用する Windows Server の使用操作は、同じ請求が行われるため、Windows BYOL の使用操作と同じです。

Windows ServerをライセンスからBYOLに変換する

Windows Server をライセンスから BYOL に変換しても、License Manager は Windows を自動的にライセンス認証しません。インスタンスの KMS サーバーをAWSKMS サーバーを独自の KMS サーバーに接続します。

Important

含まれているライセンスから BYOL に変換するには、元の Amazon EC2 インスタンスを独自の仮想マシン (VM) イメージから起動する必要があります。VM を Amazon EC2 に変換する方法については、を参照してください。 [VM Import/Export](#)。Amazon Machine Image (AMI) から起動されたインスタンスは、ライセンスを BYOL に変換することはできません。

Microsoft ライセンス契約を確認して、Microsoft Windows Server のライセンス認証に使用できる方法を確認します。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 構成から KMS サーバーのアドレスを取得する必要があります。

- 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
```

- ライセンスの変換後に Windows のライセンス認証を行うには、オペレーティングシステムの Windows Server KMS サーバーを独自の KMS サーバーを指す必要があります。Windows インスタンスにログインし、次のコマンドを実行します。

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

Windows ServerをBYOLからライセンスに変換する

Windows Server を BYOL から含まれているライセンスに変換すると、License Manager はインスタンスの KMS サーバーをAWSKMS サーバーです。

インスタンスのライセンスタイプを BYOL から含まれているライセンスに変換するには、次のコマンドを実行し、ARN を変換するインスタンスの ARN に置き換えます。

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

Windows Serverをライセンス付属からBYOLに変換し、SQL Server標準をBYOLからライセンス付属に変換

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

Windows Server インスタンスのライセンスタイプを、含まれているライセンスから BYOL に、SQL Server Standard を BYOL から含まれているライセンスに変換するには、次のコマンドを実行し、ARN を変換するインスタンスの ARN に置き換えます。

```
aws license-manager create-license-conversion-task-for-resource \  
--resource-arn <instance_arn> \  
--source-license-context UsageOperation=RunInstances:0002 \  
--destination-license-context UsageOperation=RunInstances:0804
```

テナント属性変換

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

- 共有
- Dedicated Instance
- Dedicated Host
- ホスト・ Resource Groups (HRG)

Dedicated Host テナンシータイプに切り替えるには、インスタンスの起動に使用できる容量を持つ Dedicated Host がアカウントにある必要があります。ホスト Resource Groups テナント属性タイプに移行するには、アカウントに少なくとも1つの HRG が必要です。

テナント属性コンバージョン制限

テナント属性変換には、以下の制限が適用されます。

- Linux 課金コードは、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許可されていません。
- Windows Server ライセンスに含まれている課金コードは、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ません。ただし、これらの課金コードは、Dedicated Hosts およびホスト Resource Groups では許可されません。
- Windows Server 以外のライセンス込みの課金コードは、専用ホストおよびホスト Resource Groups では許可されません。

インスタンスのテナント属性を変更するにはAWS CLI

インスタンスは、stoppedそのテナンシーを変更するために状態。

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テナント属性を使用するには、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hostテナント属性を使用するには、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
```

インスタンスを任意のテナンシーからhostテナンシーを使用して、特定の Dedicated Host をターゲットとする場合は、次のコマンドを実行します。

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

インスタンスを任意のテナンシーからhostテナント属性を使用するには、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

ライセンスタイプ変換タスクが不完全です

ライセンスタイプ変換タスクには、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せん。ただし、KMS サーバーがAWSKMS サーバーです。

この問題を修復するには、の手順を実行します。[EC2 Windows インスタンスで Windows のアクティベーションが失敗したのはなぜですか?](#)をクリックして、Systems Manager で Windows のライセンス認証を行います。[AWSSupport-ActivateWindowsWithAmazonLicenseAutomation Runbook](#) を使用するか、インスタンスにログインして手動でAWSKMS サーバーです。

のホストリソースグループ°AWS License Manager

ADedicated Hostは、EC2 インスタンスの容量全体が専用に割り当てられた物理サーバーです。ホストリソースグループは、単一のエンティティとして管理できる Dedicated Hosts のコレクションです。インスタンスを起動すると、License Manager はホストを割り当てて、設定した設定に基づいて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を使用して自動ホスト管理を利用することができます。

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実稼働、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 でインスタンスを直接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。

Settings

ホストリソースグループについては、次の設定を指定できます。

- ホストの自動割り当て— このホストリソースグループ内のインスタンスの起動に使用可能な容量を超える場合に、Amazon EC2 がユーザーに代わって新しいホストを割り当てることができるかどうかを示します。
- ホストの自動リリース— Amazon EC2 がユーザー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。
- ホストの自動リカバリ— 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。
- 関連付けられたライセンス設定— 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ライセンス設定。
- 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任意のインスタンスタイプを起動できます。あなたが起動した場合Nitroベースのインスタンスを起動する場合、同じホストリソースグループ内で異なるインスタンスタイプを持つインスタンスを起動できます。それ以外の場合は、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 \(p. 22\)](#)
- [ホストリソースグループの共有 \(p. 23\)](#)
- [ホストリソースグループでのインスタンスの作成 \(p. 23\)](#)
- [ホストリソースグループの変更 \(p. 23\)](#)
- [ホストリソースグループの削除 \(p. 23\)](#)
- [ホストリソースグループへのDedicated Host の追加 \(p. 24\)](#)
- [ホストリソースグループからDedicated Host を削除する \(p. 24\)](#)

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を構成して、License Manager で専用ホストを管理できるようにします。最も高価なライセンスを最大限に活用するには、1つ以上のコアまたはソケットベースのライセンス構成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には、すべてのコアまたはソケットベースのライセンス構成をホストリソースグループで許可します。

ホストリソースグループを作成するには

1. License Manager コンソール () を開きます。 <https://console.aws.amazon.com/license-manager/>。
2. 左のナビゲーションペインで、[] を選択します。ホストリソースグループ。
3. 選択ホストリソースグループの作成。
4. を使用する場合ホストリソースグループの詳細ホストリソースグループの名前と説明を指定します。
5. を使用する場合EC2 専用ホスト管理設定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
 - ホストの自動リリース
 - ホストの自動リカバリ

- (オプション) for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。
- を使用する場合ライセンス設定コアベースまたはソケットベースのライセンス設定を 1 つ以上のソケットベースのライセンス設定を選択します。
- (オプション) forタグに 1 つ以上のタグを追加します。
- [作成] を選択します。

ホストリソースグループの共有

次を使用できます。AWS Resource Access Managerを使用して、ホストリソースグループを共有できます。AWS Organizations。ホストリソースグループとライセンス設定を共有すると、メンバーアカウントは共有ホストリソースグループにインスタンスを起動できます。新しいホストは、ホストリソースグループを所有するアカウントに割り当てられます。メンバーアカウントがインスタンスを所有します。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でのインスタンスの作成

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、次を使用できます。`run-instances`コマンド。コアベースまたはソケットベースのライセンス設定を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、「」を参照してください。[ホストリソースグループにインスタンスを作成する](#)()Amazon EC2 ユーザーガイド。

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の数より小さく設定することはできません。そのタイプのインスタンスがホストリソースグループで実行されている場合は、インスタンスタイプを削除できません。

ホストリソースグループを変更するには

- License Manager コンソール () を開きます。<https://console.aws.amazon.com/license-manager/>。
- 左のナビゲーションペインで、[] を選択します。ホストリソースグループ。
- ホストリソースグループを選択してから、[] を選択します。アクション,編集。
- 必要に応じて設定を修正します。
- [Save changes] を選択します。

ホストリソースグループの削除

ホストリソースグループは、ホストがない場合は削除できます。

ホストリソースグループを削除するには

- License Manager コンソール () を開きます。<https://console.aws.amazon.com/license-manager/>。
- 左のナビゲーションペインで、[] を選択します。ホストリソースグループ。
- ホストリソースグループを選択してから、[] を選択します。アクション,削除。

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。

ホストリソースグループへのDedicated Host 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。ホストを追加するには、AWSアカウント所有者で、Dedicated Host リソースグループおよびホストリソースグループを作成しました。ホストリソースグループに、許可されたライセンス設定とインスタンスタイプがリストされている場合、追加するホストは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、再起動するとします。次の 2 つのタスクを実行する必要があります。

- [の変更](#) インスタンスをホストリソースグループを指すように設定します。
- [関連付け](#) ホストリソースグループに一致させるライセンス設定をします。

Resource Groups の詳細については、[AWS Resource Groupsユーザーガイド](#)。

次の手順を使用して、リソースグループに 1 つ以上のDedicated Hosts を追加します。

1. License Manager コンソール (<https://console.aws.amazon.com/license-manager/>) にログインします。
2. 選択ホストリResource Groups。
3. ホストリソースグループ名のリストから、Dedicated Host を追加するホストリソースグループの名前をクリックします。
4. 選択専用ホスト。
5. [Add] を選択します。
6. ホストリソースグループに追加する Dedicated Hosts を 1 つ以上選択します。
7. [Add] を選択します。

ホストの追加には 1 ~ 2 分かかる場合があります。その後、専用ホスト。

ホストリソースグループからDedicated Host を削除する

ホストリソースグループからホストを削除しても、そのホストで実行されているインスタンスはホストに残ります。ホストリソースグループにアタッチ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アタッチ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アカウントの場合、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。

次の手順を使用して、ホストリソースグループの Dedicated Host を削除します。

1. License Manager コンソール (<https://console.aws.amazon.com/license-manager/>) にログインします。
2. 選択ホストリResource Groups。
3. Dedicated Host を削除するホスト・リソースの名前をクリックします。
4. 選択専用ホスト。
5. ホストリソースグループから削除する Dedicated Host を選択します。または、ホスト ID、ホストタイプ、ホストの状態、またはアベイラビリティゾーンによって Dedicated Host を検索することもできます。

6. [削除] を選択します。
7. 選択を削除します。もう一度確認します。

License Manager のリソースインベントリ

License Manager を使用すると、オンプレミスのアプリケーションを [Systems Manager Inventory](#) をクリックし、ライセンスルールをアタッチします。これらのサーバーにライセンスルールをアタッチしたら、それらを AWS サーバーを License Manager のダッシュボードで選択します。

ただし、License Manager では、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。非についての情報を保持するには AWS サーバーを更新するには、インベントリ情報を定期的に更新する必要があります。インベントリの検索セクション [License Manager](#)。

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 により、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。インベントリデータを Systems Manager から消去すると、License Manager により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、License Manager でクリーンアップ操作を実行できるように、Systems Manager でインスタンスを手動で登録解除することをお勧めします。

Systems Manager インベントリのクエリには、リソースデータ同期によりインベントリを Amazon S3 パケット内に保存すること、Amazon Athena インベントリデータを組織アカウントから集約すること、AWS Glue を使用して、高速なクエリエクスペリエンスを提供します。詳細については、「[のサービスにリンクされたロールの使用 AWS License Manager \(p. 45\)](#)」を参照してください。

リソース在庫追跡は、組織で制限されていない場合にも役立ちます AWS ユーザーが AMI 派生インスタンスを作成したり、実行中のインスタンスに追加ソフトウェアをインストールしたりしないようにします。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およびアプリケーションを簡単に検出するための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。

目次

- [リソースインベントリを検出 \(p. 25\)](#)
- [リソースインベントリの自動検出 \(p. 27\)](#)

リソースインベントリを検出

License Manager [Systems Manager Inventory](#) 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検出します。ライセンス構成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

- [在庫検索の設定 \(p. 25\)](#)
- [インベントリ検索の使用 \(p. 26\)](#)
- [ライセンス構成への自動検出ルールの追加 \(p. 26\)](#)
- [ライセンス設定と、検出されたインベントリの関連付け \(p. 27\)](#)
- [ライセンス構成とリソースの関連付けの解除 \(p. 27\)](#)

在庫検索の設定

資源在庫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AWS Organizationsアカウント. 詳細については、「[License Manager の設定 \(p. 40\)](#)」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ライセンス設定を作成します。たとえば、Microsoft と SQL Server Enterprise のライセンス契約の条項を反映したライセンス構成を作成します。

インベントリ検索の使用

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。名前 (たとえば、「SQL Server」で始まる名前) と含まれるライセンスの種類 (たとえば、「SQL Server Web」ではないライセンス) でアプリケーションを検索できます。

リソースインベントリを検索するには

1. License Manager コンソール (<https://console.aws.amazon.com/license-manager/>).
2. ナビゲーションペインで、 を選択します。インベントリの検索。
3. 表示されるリソースのリストを絞り込むためのフィルタオプションを指定します。

Amazon EC2 リソースでは、次のフィルタと論理演算子がサポートされています。

- リソース ID— リソースの ID。論理演算子等号およびEquals。
- アカウント ID— IDAWSリソースを所有しているアカウントです。論理演算子等号およびEquals。
- プラットフォーム名— リソースのプラットフォームです。論理演算子等号,Equals,から始まる, および内容。
- アプリケーション名— アプリケーションの名前です。論理演算子等号およびから始まる。
- ライセンス込み名— 含まれるライセンスのタイプです。論理演算子等号およびEquals。想定される値は次のとおりです。SQL Server Enterprise,SQL Server Standard,SQL Server Web, およびWindows Server Datacenter。
- のタグ付け— リソースに割り当てられたタグのキーと値の組み合わせです。タグ値はオプションです。論理演算子等号およびEquals。Equalsは、クロスアカウント検出が有効になっている場合にのみ表示されます。

Amazon RDS リソースでは、次のフィルタと論理演算子がサポートされています。

- エンジンのエディション— データベースエンジンのエディション。論理演算子等号。想定される値は次のとおりです。Standard Edition,スタンダード・エディションOne,スタンダードエディションTwo, およびEnterprise Edition。
- ライセンスパック— ライセンスパックです。論理演算子等号。想定される値は次のとおりです。Spatial と Graph,アクティブData Guard,Label Security,オラクルのオンライン分析処理 (OLAP), および診断パックとチューニングパック。

詳細については、「」を参照してください。[Oracle のライセンス](#)のAmazon RDS ユーザーガイド。

ライセンス構成への自動検出ルールの追加

ライセンス設定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、「[リソースインベントリの自動検出 \(p. 27\)](#)」を参照してください。

自動検出ルールをライセンス構成に追加するには

1. License Manager コンソール () を開きます。<https://console.aws.amazon.com/license-manager/>。
2. を開くインベントリの検索ページで、

- リソースを選択し、 を選択します。自動検出ルールの追加。
- を使用する場合ライセンス設定ライセンス設定を選択します。
- 検出および追跡する製品を指定します。
- (オプション)[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クリックして、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License Managerが検出した後でライセンスを再利用できるようにします。
- (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。

Note

除外ルールは、RDS 製品 (Oracle データベースなど) には適用されません。

- [選択プロパティフィルタをオンにする場合、現在アカウント ID、およびのタグ付けがサポートされています。
 - そのプロパティを識別するための情報を入力します。以下のためにアカウント ID12 桁を指定 AWS値としてアカウント ID。を使用する場合タグキーと値のペアを入力します。
 - 手順 7 を繰り返して、ルールを追加します。
- [Add] (追加) をクリックします。

ライセンス設定と、検出されたインベントリの関連付け

管理する必要がある管理対象外のリソースを特定したら、自動検出を使用する代わりに、手動でライセンス構成に関連付けることができます。

ライセンス設定をリソースに関連付けるには

- License Manager コンソール () を開きます。 <https://console.aws.amazon.com/license-manager/>。
- を開くインベントリの検索ページで。
- リソースを選択し、 を選択します。ライセンス設定を関連付ける。
- を使用する場合ライセンス設定名ライセンス設定を選択します。
- (オプション) [Share license configuration with all my member accounts] を選択します。
- [Associate] を選択します。

ライセンス構成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項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てから、ライセンス設定を削除できます。

ライセンス設定とリソースの関連付けを解除するには

- License Manager コンソール () を開きます。 <https://console.aws.amazon.com/license-manager/>。
- 左のナビゲーションペインで [License configuration] を選択します。
- ライセンス設定の名前を選択します。
- [Associated resources] を選択します。
- ライセンス設定との関連付けを解除する各リソースを選択し、 を選択します。リソースの関連付けを解除する。

リソースインベントリの自動検出

License Manager [Systems Manager Inventory](#) を使用して、Amazon EC2 インスタンスおよびオンプレミスインスタンスのソフトウェアの使用状況を検出できます。ライセンス設定に製品情報を追加できま

す。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。に属しているインスタンスを除外できますAWSアカウント ID またはリソースタグに関連付けられた、自動検出の対象から除外される

自動検出は、新しいライセンスセット、既存のライセンス構成、またはインベントリ内のリソースに追加できます。自動検出のルールは、CLI からいつでも編集できます。[更新ライセンス二次構成API](#) コマンドを実行します。コンソールでルールを編集するには、既存のライセンス設定を削除して新しいライセンス設定を作成する必要があります。

自動検出を使用するには、ライセンス構成に製品情報を追加する必要があります。これは、検索インベントリを使用してライセンス設定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は解除されません。自動検出を構成して、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できます。

自動検出を設定したら、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。

Prerequisites

- License Manager をAWS Organizationsアカウント. 詳細については、「[License Manager の設定 \(p. 40\)](#)」を参照してください。

Note

単一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ます。

ライセンス構成の作成時に自動検出を構成するには

ライセンス構成を作成するときに、自動検出ルールと除外ルールを構成できます。詳細については、「[ライセンス設定を作成します。 \(p. 9\)](#)」を参照してください。

既存の構成に自動検出ルールを追加するには

以下のプロセスを使用して、コンソールから既存のライセンス構成に自動検出ルールを追加します。インベントリの検索ウィンドウで、リソース ID を選択し、自動検出ルールの追加。

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、[] を選択します。カスタマー管理ライセンス。
3. ライセンス設定の名前を選択して、ライセンスの詳細ページを開きます。
4. リポジトリの []検出ルールの自動化[] タブで、[自動検出ルールの追加。
5. 検出および追跡する製品を指定します。
6. (オプション) [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クリックして、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License Managerが検出した後でライセンスを再利用できるようにします。
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。

Note

除外ルールは、RDS 製品 (Oracle データベースなど) には適用されません。

- a. [選択プロパティフィルタをオンにする場合、現在アカウント ID、およびのタグ付け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。以下のためにアカウント ID12 桁を指定AWSアカウント ID を値として使用します。を使用する場合タグキーと値のペアを入力します。

- c. 手順 7 を繰り返して、ルールを追加します。
8. 完了したら、 を選択します。を追加します。をクリックして、自動検出ルールを適用します。

ライセンスマネージャで付与されたライセンス

付与されたライセンスとは、組織から購入した製品のライセンスです。AWS Marketplace、[AWSData Exchange](#)、またはソフトウェアを使用権限管理と統合した販売者から直接入手できます。ライセンス管理者は、AWS License Manager これらのライセンスの使用を管理し、使用権 (エンタイトルメント) を特定の AWS アカウント。

ライセンス管理者が AWS Marketplace license を AWS アカウントにログインし、受信者が付与されたライセンスを受け入れてアクティブ化すると、サブスクリプションは AWS アカウント経由 AWS Marketplace。アカウントはまた、製品へのアクセス権を持っています。たとえば、ライセンス管理者が Amazon マシンイメージ (AMI) を AWS Marketplace に配布し、エンタイトルメントを AWS アカウントを使用して、AMI から Amazon EC2 インスタンスを起動できます。AWS Marketplace および Amazon EC2。

データライセンス配布先 AWSData Exchange 製品は、AWS アカウント経由 AWS [Data Exchange]:

からライセンスを配布する前に AWS Marketplace サブスクリプション共有を有効にするには、サブスクリプション共有を有効にする必要があります。詳細については、「」を参照してください。[組織内でのサブスクリプションの共有](#)。

付与されたライセンスの管理

からサブスクリプションを購入した後 AWS Marketplace または AWSData Exchange、License Manager を使用してライセンスを配布する出品者から製品を購入したり、ライセンス管理者から許可を受けると、付与されたライセンスが 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、許可されたライセンスを受け入れ、アクティベートする必要があります。

ライセンスの受け入れとアクティベーション方法は、ライセンスが AWS Marketplace アカウントが、組織のメンバーアカウントである場合は、AWS Organizations と、[すべての機能組織](#)で有効になっていることを確認します。

付与されたライセンスには、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、付与された各ライセンスとその関連情報を他のリージョンに自動的に複製します。これにより、ライセンスが付与されるすべてのリージョンで一元的に表示できます。

のライセンス AWS Marketplace および AWSData Exchange

- から購入したサブスクリプションのライセンス AWS Marketplace は自動的に承認され、アクティブ化されます。
- すべての機能が有効な組織の管理アカウントで、サブスクリプションを AWS Marketplace がメンバーアカウントにライセンスを配布する場合、ライセンスはメンバーアカウントに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ブ化できます。
- 一括請求機能のみを有効にしている組織の管理アカウントが、AWS Marketplace がメンバーアカウントにライセンスを配布する場合、各メンバーアカウントはライセンスを受け入れ、アクティブ化する必要があります。

販売者からのライセンス

- License Manager を使用してライセンスを配布する販売者から購入した製品のライセンスを承認し、ライセンス認証する必要があります。
- すべての機能が有効な組織の管理アカウントが、出品者から製品を購入し、ライセンスをメンバーアカウントに配布する場合、ライセンスはメンバーアカウントで自動的に承認されます。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ブ化できます。

- 一括請求 (コンソリデーティッドビルディング) 機能のみを有効にした組織の管理アカウントが、出品者から製品を購入し、メンバーアカウントにライセンスを配布する場合、各メンバーアカウントがそのライセンスを承認してアクティブ化する必要があります。

付与されたライセンスを管理するには

- 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 [] を選択します。許可されたライセンス。
- (オプション) 表示されるライセンスの一覧を絞り込むには、次のようなフィルターオプションを使用します。
 - [製品名] — 製品の名称。
 - 発行者 — ライセンスを発行したエンティティ。たとえば、によって作成されたライセンス AWS Marketplace の発行元を持っているAWS Marketplace。
 - レコードの販売者 — 製品を販売したエンティティ。
 - [Status (ステータス)] — ライセンスのステータス。例:使用可能。
 - [付与されたステータス] — 付与されたステータス。例:受理保留。
- 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。
- ライセンス発行元が AWS Marketplace の場合、最初の許可ステータスは受理保留。次のいずれかを行ってください。
 - 選択ライセンスの承認とアクティブ化。結果として得られる付与ステータスはアクティブ。
 - 選択ライセンスの受け入れ。結果として得られる付与ステータスはDisabled。ライセンスを使用する準備ができたなら、[ライセンスのアクティブ化]。
 - 選択ライセンスの拒否。結果として得られる付与ステータスは拒否。ライセンスを拒否すると、ライセンス認証はできません。
- アクティブなライセンスの使用を停止するには、ライセンスの非アクティブ化。再度使用する準備ができたなら、[ライセンスのアクティブ化]。

コマンドラインを使用して付与されたライセンスを管理するには

- 許可を受け付ける(AWS CLI)
- grantバージョンの作成(AWS CLI)
- get grant(AWS CLI)
- list licenses(AWS CLI)
- list受信付grant(AWS CLI)
- list受信ライセンス(AWS CLI)
- 拒否-許可(AWS CLI)

使用権限の分散

ライセンス管理者の場合は、ライセンスへのアクセスを別のAWSアカウントの [] を選択します。ライセンスにつき最大 2,000 個の付与を作成できます。

許可を作成するには

- 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 [] を選択します。許可されたライセンス。
- 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。
- [] から、許可セクションで [] を選択します。許可を作成する。

5. リポジトリの [] 助成金の詳細パネルで、次の操作を行います。
 - a. 許可の目的または受取人を識別するために補助金の名前を入力します。
 - b. [] と入力します。AWS許可受信者のアカウント ID。

Note

また、AWS Organizations組織内のすべてのアカウントに一度にエンタイトルメントを付与する、組織の ID。詳細については、「[への分散AWS Organizations \(p. 31\)](#)」を参照してください。

 - c. 選択許可を作成する。
6. ライセンスの詳細ページに戻ると、許可のエントリが許可パネル。許可の最初のステータスは受理保留。ステータスが [] に変わります。アクティブ受信者が助成金を受け入れるか、拒否受信者が助成金を拒否したとき。

コマンドラインを使用して付与を作成するには

- [許可の作成](#)(AWS CLI)
- [リスト配布付与](#)(AWS CLI)

承認とアクティベーションの付与

許可されたライセンスは、使用する前に、被付与者アカウントで承認され、アクティブ化されている必要があります。

デフォルトでは、付与されたライセンスの付与詳細ページのステータスが受理保留。以下を選択することができます。Accept,承認とアクティブ化,または拒否license.

Note

同じ製品に対して 2 つのライセンスをアクティベートすることはできません。AWS Marketplace を同時にできます。サブスクリプションが 2 つある場合 (たとえば、製品およびプライベートオファラーのパブリックオファラー、または製品のサブスクライブライセンスと同じ製品の許可されたライセンスなど)、使用していないサブスクリプションを非アクティブ化してから、もう一方のサブスクリプションをアクティブ化する必要があります。

承認されているが、まだアクティブ化されていない許可のステータスはDisabled。承認された許可と有効化された許可のステータスがアクティブ。

Note

組織の管理アカウントからの許可を自動的に受け入れることができます。許可の自動承認を有効にするには、組織アカウントをAWS License Managerconsole [X 設定](#) 管理アカウントから。

への分散AWS Organizations

組織の管理アカウントで操作しているライセンス管理者が [すべての機能](#) を有効にすると、組織内のすべてのアカウントにライセンスを一度に配布できます。1 つの許可を持つすべてのアカウントにライセンスを配布するには、[使用権限の配布](#)。コンソールでは、組織 ID または組織 ARN を指定できません。組織の ARN の例を示します。arn:aws:organizations::<account-id-of-management-account>;organization/<organization-id>。ARN を使用するには[AWS License ManagerAPI](#)。

Note

ライセンスを付与するには、AWS OrganizationsID、最初にリンクする必要がありますAWS OrganizationsアカウントをAWS License Managerコンソールの設定。詳細については、「[License Manager の設定 \(p. 40\)](#)」を参照してください。

[付与の詳細] ページには、エンタイトルメントへのアクセスを許可したアカウントのリストが表示されます。ライセンスを組織に配布したら、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できます。

ライセンスのステータス

ライセンスには、次の 2 つのステータスがあります。-ライセンスのステータスで、ライセンスの全体的な可用性と共有性を示し、付与ステータスで、ライセンスを使用できる機能を示します。

ライセンスのステータス

ステータス	説明
使用可能	ライセンスは、使用して共有できます。
削除	使用許諾契約が取り消されたため、ライセンスは使用できません。
非アクティブ化中	ライセンス発行者によって非アクティブ化されているため、使用できないライセンス。
失効済み	このライセンスは、有効期限に達しているため、使用できません。

許可ステータス

ステータス	説明
受理保留	許可が作成され、許可の受信者がまだ承認していません。
Disabled	許可は受信者によって受け入れられましたが、使用のためにアクティブ化されていません。
アクティブ	助成金は、使用のために承認され、アクティブ化されました。ライセンスされたリソースを使用できます。
拒否	許可の受信者が許可を拒否しました。
削除	権限付与者が権限を削除しました。
ワークフローの完了	付与は組織への付与であり、付与を配布または取り消すワークフローが完了しました。付与の詳細には、組織内の各アカウントに対する副付与のステータスが表示されます。

出品者は、でライセンスを発行しましたAWS License Manager

独立系ソフトウェアベンダー (ISV) はソフトウェアベンダーAWS License Managerを使用して、ソフトウェアライセンスを管理し、エンドユーザーに配布できます。発行者は、License Manager ダッシュボードを使用して、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。

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、顧客が暗号で真正性を検証できるようにします。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、あなたは非対称のAWS KMSキーを作成し、アカウントに保存します。

出品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、各出品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は、次のようなさまざまなライセンスモデルをサポートしています。

- パーベチュアル—ユーザーがソフトウェアを無期限に使用することを許可する、有効期限のないライフタイムライセンス。
- フローティング-アプリケーションの複数のインスタンスとの共有可能なライセンス。ライセンスは前払いで、固定されたエンタイトルメントをそれらに追加できます。
- Subscription-特に非アクティブ化しない限り、自動的に更新できる有効期限のあるライセンス。
- 使用量に応じたもの-API リクエスト、トランザクション、ストレージ機能の数など、使用状況に基づいた特定の条件を持つライセンス。

ライセンスマネージャでライセンスを作成し、AWSIAM ID、またはLicense Managerによって生成されたベアトークンを使用します。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。分散エンタイトルメントをお持ちのお客様は、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。

Entitlements

License Managerは、ライセンス機能を使用権限管理ライセンス。エンタイトルメントは、限定された数量または無制限の数量で特徴付けられます。制限付きエンタイトルメントの例として、「40 GB のデータ転送」があります。無制限の数量エンタイトルメントの例は、「プラチナティア」です。

ライセンスは、付与されたすべてのエンタイトルメント、アクティブーションと有効期限、および発行者の詳細をキャプチャします。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、各バージョンは不変です。ライセンスのバージョンは、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制限付き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、制限された機能では、エンドユーザーが初期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「overage」フラグもサポートされます。License Managerは、使用量を追跡し、ISVに報告します。

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るライセンスを一元的に追跡できます。また、License Managerは、ユーザーのIDと、チェックアウト時に各チェックアウトに関連付けられた基になるリソース識別子(利用可能な場合)も追跡します。CloudWatch イベントを使用して、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。

- 作成-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。
- 非アクティブ化中-ライセンスが非アクティブ化されます。
- 削除-ライセンスが削除されます。

Requirements

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

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

あなたは、License Manager と統合するので、AWS アカウントは、AWS Marketplace を使用するには、ソフトウェアアプリケーションが License Manager API を呼び出せるようにするロールを作成する必要があります。たとえば、`awscli` を使用できます。AWS CLI まず、`create-role` という名前のロールを作成する AWS ライセンスマネージャ消費ロール。

```
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`。

```
{
  "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`コマンドを実行してAWSライセンスマネージャーの消費ポリシー AWS管理ポリシーをAWSライセンスマネージャ消費ロールロール。

```
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

以下の手順に従って、カスタマーに付与するライセンスのブロックを作成します。AWS Management Console。または、ライセンスを作成することもできます。[ライセンスの作成API アクション](#)。

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. 選択販売者発行ライセンス左のメニューで [
3. 選択ライセンスの作成。
4. を使用する場合ライセンスメタデータに、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 (150文字以内)
 - ライセンスの説明-オプションの説明 (最大 400 文字) で、このライセンスを他のライセンスと区別します。
 - 製品 SKU-商品のSKUです。
 - 受取人-受取人の名前 (会社または個人) 。
 - ホームリージョン-ザ・AWSライセンスのリージョン。ライセンスはグローバルに消費できますが、ライセンスはホームリージョンでのみ変更できます。ライセンスのホームリージョンは、作成後に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. を使用する場合消費の設定に、次の情報を入力します。
 - 更新頻度-毎週、毎月、またはまったく更新しないかどうか。
 - 消費の設定-選択暫定消込設定オプションライセンスを連続接続に使用するか、借用ライセンスをオフラインで使用する場合。Enter最大有効期限 (分)をクリックして、ライセンスの可用性の長さを設定します。
6. を使用する場合発行者に、次の情報を入力します。
 - 「」と入力します。AWS KMSkey-License Manager は、このキーを使用して発行者に署名し、検証します。詳細については、「[ライセンスの暗号署名 \(p. 56\)](#)」を参照してください。
 - 発行元の名前-出品者の会社名。
 - 販売者のレコード-省略可能なビジネス名。
 - 契約の URL: ライセンス契約への URL。
7. を使用する場合使用権限管理には、ライセンスが受信者に付与する機能に関する次の情報を指定します。
 - 名前-受取人の名前。
 - 単位タイプ-ユニットタイプを選択し、最大数を指定します。
 - Checkチェックインを許可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に使用します。
 - Check許可された超過数受信者が最大数を超えるリソースを使用できる場合。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. 選択ライセンスの作成。

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ら、そのライセンスをカスタマーに付与できます。AWSアカウントを使用してAWS Management Console。受信者は、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で付与されたライセンス \(p. 29\)](#)」を参照してください。

または、顧客がAWSアカウントを作成するには、License Manager API を使用して、カスタマーが消費されたライセンス (p. 36)。

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. 選択販売者発行ライセンス左のメニューで [
3. ライセンスの ID を選択して、詳細ページを開きます。
4. を使用する場合許可] で、許可を作成する。
5. を使用する場合助成金の詳細に、次の情報を入力します。
 - 許可名-助成金名 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-ザ・AWSライセンス受取人のアカウント番号。
 - ライセンス権-選択消費電力受信者が付与されたエンタイトルメントのみを使用でき、配信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。
 - ホームリージョン-ザ・AWSライセンスのリージョン。
6. 選択許可を作成する。

ユーザーの一時的な認証情報の取得AWSアカウント

あなたが持っていない顧客を持っている場合AWSアカウントでは、ユーザーに対するエンタイトルメントをAWSアカウント。以下の手順に従って、一時的なAWS認証情報を登録せずに顧客にAWSアカウント。API呼び出しは、ホームリージョンで行う必要があります。

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

1. を呼び出します。 [CreateToken](#)APIアクションを使用して、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. を呼び出します。 [GetAccessToken](#)API アクション、から受け取ったリフレッシュトークンを指定する [CreateToken](#) を使用して、一時的なアクセストークンを受信します。
3. を呼び出します。 [AssumeRoleWithWebIdentity](#)API アクション、から受け取ったアクセストークンを指定する [GetAccessToken](#) と、前のステップでAWSライセンスマネージャ消費ロールロールを使用して、一時的なAWS認証情報。

消費されたライセンス

License Manager を使用すると、複数のユーザーが 1 つのライセンスから、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。を呼び出します。 [チェックアウトライセンス](#)API アクション。以下に、パラメータの説明を示します。

- キーの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: 発行元:発行元フィンガープリント

- 製品 SKU— このライセンスの製品識別子。ライセンスの作成時にライセンス発行者によって定義されます。複数のISVにまたがって同じ製品SKUが存在する可能性があります。したがって、信頼できるキーフィンガープリントは重要な役割を果たします。

例: 1a2b3c4d2f5e69f440bae30eaec9570b1fB7358824f9dfa1a5a0daExample

- 使用権限管理— チェックアウトする機能。無制限の工程能力を指定した場合、数量は 0 になります。例:

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

- 受益者— SaaS (Software as a Service) ISV 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インスタンスにライセンスをノードロックするために使用される識別子です。

例: 21.57

出品者が発行したライセンスの削除

ライセンスを削除した後、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 か月間、読み取り専用モードでライセンス発行者とライセンス被許諾者が保持され、利用できるようになります。

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

コンソールを使用して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. 選択販売者が発行したライセンス左のメニューで [
3. ライセンスの横にあるラジオボタンを選択して、削除するライセンスを選択します。
4. [削除] を選択します。確認を求められたら、次のように入力します。 **delete** を選択し、削除。

委任された管理者の登録

組織からメンバーアカウントを委任して、他のメンバーアカウントとのライセンス構成の共有やクロスアカウントリソースの検出の実行などの管理タスクを実行できます。アカウントの一部であるメンバーアカウントのみAWS Organizations委任された管理者として登録することができます。組織に加入する方法については、「[組織への AWS アカウントの招待](#)」を参照してください。

組織ごとに 1 人の委任された管理者を登録できます。委任された管理者を登録する前に、AWS Organizations。詳細については、「[」](#)を参照してください。[で信頼されたアクセスを有効にします。AWS Organizations](#)。

Important

登録されると、委任された管理者は、組織内のアカウントが所有する EC2 インスタンスを可視化できます。

以下のようになります AWS リージョン は、License Manager の委任された管理者のサポート

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

[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。

委任された管理トピック

- [委任された管理者の登録 \(コンソール\) \(p. 38\)](#)
- [委任された管理者の登録を解除するには \(コンソール\) \(p. 39\)](#)
- [委任された管理者を登録するには \(AWS CLI\) \(p. 39\)](#)
- [委任された管理者の登録を解除するには \(AWS CLI\) \(p. 39\)](#)

委任された管理者の登録 (コンソール)

[] を使用して代理管理者を登録するにはAWS License Managerコンソールから、以下のステップを実行します。

1. サインインするAWS管理アカウントの管理者としてログインします。

2. License Manager コンソール () を開きます。 <https://console.aws.amazon.com/license-manager/>。
3. 選択設定左のナビゲーションペインから、[] を選択します。
4. []委任された管理者] で、委任された管理者。
5. 委任された管理者を登録するには、アカウント ID を入力し、委任。
6. 指定された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示すメッセージが表示されます。

委任された管理者の登録を解除するには (コンソール)

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

1. サインインするAWS管理アカウントの管理者としてログインします。
2. License Manager コンソール () を開きます。 <https://console.aws.amazon.com/license-manager/>。
3. 選択設定左のナビゲーションペインから、[] を選択します。
4. []委任された管理者] で、を削除します。。
5. 委任された管理者の登録解除に成功したことを確認するには、を削除します。をクリックします。

委任された管理者を登録するには (AWS CLI)

[] を使用して代理管理者を登録するにはAWS CLI[] で、以下のステップを実行します。

1. コマンドラインから、以下を実行します。AWS CLIコマンド:

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

2. 指定された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するには、次のコマンドを実行します。

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

委任された管理者の登録を解除するには (AWS CLI)

代理管理者の登録を解除するにはAWS CLI[] で、以下のステップを実行します。

1. コマンドラインから、以下を実行します。AWS CLIコマンド:

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

2. 指定されたアカウントが委任された管理者として正常に登録解除されていることを確認するには、次のコマンドを実行します。

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

登録解除されたアカウントはいつでも再登録できます。

License Manager の設定

設定セクション License Manager、ログインしているアカウントの設定が表示されます。管理対象のエンタイトルメントとライセンス構成の組織への配布を有効にしたり、クロスアカウントインベントリの検出を実行したりするには、設定を構成する必要があります。

License Manager の設定には以下が含まれます。

- アカウントの種類
- S3 バケット ARN
- リンクAWS Organizationsアカウントステータス
- SNS トピックの ARN
- クロスアカウントリソース検出
- リソース共有 ARN
- 委任された管理者の登録/登録解除 (該当する場合)

License Manager の設定を編集するには

1. License Manager コンソール (<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. [編集] を選択します。

管理対象のエンタイトルメントまたはライセンス構成の組織への配布を有効にする

組織の管理対象エンタイトルメントまたはライセンス設定を配布するには、[リンクAWS Organizations アカウント。管理対象エンタイトルメントの分散付与は、すべてのメンバーアカウントによって自動的に承認されます。このオプションを選択すると、サービスリンクされたロールが管理 (p. 48) および member (p. 52) アカウント。

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、AWS Organizations。詳細については、「」を参照してください。 [組織内のすべての機能の有効化\(\)](#) AWS Organizations ユーザーガイド。

この選択により、AWS Resource Access Manager リソース共有を管理アカウントに保存します。これにより、ライセンス設定をシームレスに共有できます。詳細については、 [AWS Resource Access Manager ユーザーガイド](#) を参照してください。

このオプションを無効にするには、 [UpdateServiceSettingsAPI](#)。

クロスアカウントのリソース検出をAWS Organizations

組織のクロスアカウントのリソース検出を有効にするには、[Organizations クロスアカウントのリソース検出] の横にあるチェックボックスをオンにします。クロスアカウントのインベントリ検索を有効化。クロスアカウントのインベントリ検索を有効にすると、AWS Organizationsは自動的にリンクされ、すべてのアカウントで在庫検索が実行されます。

Note

License Manager は [Systems Manager インベントリ](#) 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 インベントリが設定されているか確認します。Systems Manager インベントリへのクエリを実行するには、以下が必要です。

- [リソースデータの同期](#) Amazon S3 バケットにインベントリを格納します。
- [Amazon Athena](#) 組織のアカウントのインベントリデータを集約します。

- [AWS Glue](#)を使用して、高速なクエリエクスペリエンスを提供します。

(オプション) Amazon 簡易通知サービスの場合は、Amazon SNS トピック ARN。ARN は次の形式を使用する必要があります。

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

License Manager 内のダッシュボード

-ダッシュボードの セクションAWS License Managerコンソールには、各ライセンス設定に関連付けられたライセンス消費量を追跡するグラフが表示されます。ダッシュボードには、ライセンスルール違反によるアラートも表示されます。

ライセンス設定のグラフでは、以下の情報が利用できます。

- ライセンス設定名
- ライセンスタイプ
- 消費されたライセンス
- 残りのライセンスの数
- ルールの強制の有無
- 各テナンシータイプのホストの数

AWS License Manager でのセキュリティ

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

セキュリティは、AWS とお客様の間の共有責任です。[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 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 に適用され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対象範囲内のサービス](#)」。
- クラウド内のセキュリティ - お客様の責任は使用する AWS のサービスによって決まります。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 を使用する際の責任共有モデルの適用方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 を設定する方法を説明します。また、他のを使用する方法についても説明します。AWS License Manager のリソースのモニタリングや保護に役立つサービスの使用方法について説明します。

目次

- [AWS License Manager でのデータ保護 \(p. 42\)](#)
- [AWS License Manager の Identity and Access Management \(p. 43\)](#)
- [のサービスにリンクされたロールの使用AWS License Manager \(p. 45\)](#)
- [AWS 用の 管理ポリシーAWS License Manager \(p. 54\)](#)
- [ライセンスの暗号署名 \(p. 56\)](#)
- [AWS License Manager のコンプライアンス検証 \(p. 57\)](#)
- [AWS License Managerの耐障害性 \(p. 57\)](#)
- [AWS License Manager でのインフラストラクチャセキュリティ \(p. 58\)](#)
- [AWS License Manager とインターフェイス VPC エンドポイント \(AWS PrivateLink \) \(p. 58\)](#)

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。このモデルで説明したように、AWS は、すべての AWS クラウド を実行するグローバルインフラストラクチャを保護する責任を負います。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。このコンテンツには、使用する AWS サービスのセキュリティ設定および管理タスクが含まれます。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](#)の「AWS 責任共有モデルと GDPR」ブログ記事を参照してください。

データ保護の目的で、AWS アカウント の認証情報を共有し、AWS Identity and Access Management(IAM) である。この方法により、それぞれの職務を遂行するために必要な許可のみを各ユーザーに付与できます。また、以下の方法でデータを保護することをお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 以降が推奨されています。
- AWS CloudTrail で API とユーザーアクティビティログをセットアップします。
- AWS 暗号化ソリューションを、AWS サービス内のすべてのデフォルトのセキュリティ管理と一緒に使用します。
- 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。これにより、Amazon S3 に保存される個人データの検出と保護が支援されます。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスするときに FIPS 140-2 検証済みの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。使用可能な 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。

顧客のアカウント番号などの機密の識別情報は、[Name (名前)] フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これには、License Manager や AWS サービス、API、AWS CLI、または AWSSDK タグまたは名前を使用する自由形式のフィールドに入力したデータは、請求ログまたは診断ログに使用できます。外部サーバーへの URL を指定する場合は、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 に含めないことを強くお勧めします。

保管時の暗号化

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ます。

AWS License Manager の Identity and Access Management

AWS Identity and Access Management (IAM) とは、AWS 管理者は、アクセスを安全にコントロールするのに役立ちます。AWS リソースの使用料金を見積もることができます。IAM 管理者は、誰を認証 (サインイン) し、誰に使用を承認する (アクセス権限を持たせる) かを制御します。AWS リソースの使用料金を見積もることができます。IAM を使用すると、ユーザーおよびグループを AWS アカウント、ユーザーがタスクを実行するために必要なアクセス許可は、AWS リソースの使用料金を見積もることができます。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、IAM 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アクセス権限がありません。IAM ユーザーに License Manager のリソース管理を許可するには、アクセス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。次に、それらのアクセス権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチします。

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](#)」を参照してください。 [ポリシーとアクセス許可](#) (IAM ユーザーガイド) を参照してください。

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。各ステートメントは次のように構成されます。

```
{
  "Statement": [{
    "Effect": "effect",
    "Action": "action",
    "Resource": "arn",
```

```
"Condition":{
  "condition":{
    "key":"value"
  }
}
]
```

ステートメントは、さまざまなエレメントで構成されます。

- 効果: -effectでできるAllowまたはDeny。デフォルトでは、IAM 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許可がないため、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優先します。明示的な拒否はすべてのものをオーバーライドする。
- アクション: -actionは、アクセス許可を付与または拒否する対象とする、特定の API オペレーションです。
- リソース: リソースはアクションによって影響を受けます。License Manager API オペレーションの中には、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で特定できるものもあります。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。
- 条件: 条件はオプションです。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、「[条件キー-AWS License Manager](#)」を参照してください。

License Manager を使用した ISV のポリシー

ライセンスマネージャを使用してライセンスを配布する ISV には、次の権限が必要です。

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

License Manager のポリシーの例

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 の場合、API オペレーションの名前にプレフィックスを付けます。license-manager:。例:

- license-manager:CreateLicenseConfiguration
- license-manager:ListLicenseConfigurations

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、License Manager API オペレーションはすべて、という単語で始まる名前を指定できます。リスト以下を実行します。

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

License Manager API オペレーションをすべて指定するには、* ワイルドカードを以下のように使用します。

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

のサービスにリンクされたロールの使用AWS License Manager

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一意のタイプの IAM ロールです。サービスにリンクされたロールは、License Managerで事前定義され、他のAWSサービスをお客様に代わって行います。

サービスにリンクされたロールを使用することで、必要なアクセス許可を手動で追加する必要がなくなるため、License Managerの設定が簡単になります。License Managerは、サービスにリンクされたロールのアクセス許可を定義します。特に定義されていない限り、License Managerのみがそのロールを引き受けることができます。定義される許可は、信頼ポリシーと許可ポリシーに含まれており、その許可ポリシーを他の IAM エンティティにアタッチ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、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。

次のセクションで説明するように、License Managerアクションはサービスにリンクされた 3 つのロールに依存します。

サービスリンクロール

- [ライセンスマネージャ : コアロール](#) (p. 45)
- [ライセンスマネージャ-管理アカウントの役割](#) (p. 48)
- [ライセンスマネージャ-メンバアカウントの役割](#) (p. 52)

ライセンスマネージャ : コアロール

License Managerでは、ユーザーに代わってライセン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。

コアロールのアクセス許可

サービスにリンクされたロールAWSservicerOREAWSライセンス管理エラーLicense Manager がAWSリソースを使用して、ユーザーに代わってライセンスを管理します。

-AWSserviceOREAWSライセンス管理エラーサービスにリンクされたロールは、license-manager.amazonaws.comサービスで、ロールを引き受ける必要があります。

ロールのアクセス許可ポリシーは、License Managerが次のアクションを指定されたリソースで完了することを許可します。

アクション	リソース ARN
iam:CreateServiceLinkedRole	arn:aws:iam::*:role/aws-service-role/license-management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManage
iam:CreateServiceLinkedRole	arn:aws:iam::*:role/aws-service-role/license-manager.member-account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberA
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:ListAllMyBuckets	*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
sns:Publish	arn:aws::sns::*:aws-license-manager-service-*
sns:ListTopics	*
ec2:DescribeInstances	*
ec2:DescribeImages	*
ec2:DescribeHosts	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*
ssm:CreateAssociation	*
organizations:ListAWSServiceAccessForOrganization	*
organizations:DescribeOrganization	*
organizations:ListDelegatedAdministrators	*
license-manager:GetServiceSettings	*
license-manager:GetLicense*	*
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:List*	*

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。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許可」を参照してください。

License Manager サービスにリンクされたロールの作成

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。License Manager コンソールに初めてアクセスしたときに、License Manager 初実行のエクスペリエンスを完了すると、サービスにリンクされたロールが自動的に作成されます。

IAM コンソールを使用することもできます。AWS CLI、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ができます。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの作成」を参照してください。

Important

このサービスにリンクされたロールがアカウントに表示されるのは、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です。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、ライセンスマネージャが AWSserviceOREAWS ライセンス管理エラーアカウントには、ロールがあります。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、サービスにリンクされたロールを作成できます。

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. 選択 License Manager の使用を開始する。
3. 左 IAM アクセス許可 (ワンタイムセットアップ) フォームで、I を付与します。AWS License Manager 必須のアクセス許可[]、[続行]。

IAM コンソールを使用して、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。License Manager[] ユースケースの例 または、AWS CLI または AWS API を使用するには、IAM を使用して、`license-manager.amazonaws.com` サービス名。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、同じ IAM 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を編集する

License Manager では、AWSserviceOREAWS ライセンス管理エラーサービスにリンクされたロール サービスにリンクされたロールを作成すると、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を必要とする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のみが作成されます。ただし、手動で削除する前に、サービスにリンクされた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と AMI からライセンス設定の関連付けを解除してから、ライセンス設定を削除します。

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。失敗した場合は、数分待ってからアクションをもう一度試してください。

コアロールで使用される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にて [ライセンス設定] を選択します。
3. ご自身が所有者である特定のライセンス設定については、関連するすべての AMI とリソースの関連付けを解除します。
4. ライセンス設定ページが表示されている間に、ライセンス設定を削除します。
5. すべてのライセンス設定が削除されるまで、前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 コンソールを使用します。AWS CLI、またはAWSAPI を使用してAWSserviceOREAWSライセンス管理エラーサービスにリンクされたロール または [AWSLicenseManagerMasterAccountRole \(p. 48\)](#) および [AWSLicenseManagerMemberAccountRole \(p. 52\)](#) を使用している場合には、最初にそれらを削除します。詳細については、IAM ユーザーガイドの「サービスにリンクされたロールの削除」を参照してください。

ライセンスマネージャ-管理アカウントの役割

License Manager では、ライセンス管理を実行するには、サービス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

サービスにリンクされたロールAWSserviceOreforライセンスマネージャーマスターアカウントロールLicense Manager がAWSリソースを使用して、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します。

-AWSserviceOreforライセンスマネージャーマスターアカウントロールサービスにリンクされたロールは、`license-manager.master-account.amazonaws.com`サービスで、ロールを引き受ける必要があります。

ロールのアクセス許可ポリシーは、License Managerが次のアクションを指定されたリソースで完了することを許可します。

アクション	リソース ARN
<code>s3:GetBucketLocation</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>
<code>s3:ListBucket</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>
<code>s3:GetLifecycleConfiguration</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>
<code>s3:PutLifecycleConfiguration</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>
<code>s3:GetBucketPolicy</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>

アクション	リソース ARN
s3:PutBucketPolicy	arn:aws:s3:::aws-license-manager-service-*
s3:AbortMultipartUpload	arn:aws:s3:::aws-license-manager-service-*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
s3:GetObject	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucketMultipartUploads	arn:aws:s3:::aws-license-manager-service-*
s3:ListMultipartUploadParts	arn:aws:s3:::aws-license-manager-service-*
s3>DeleteObject	arn:aws:s3:::aws-license-manager-service-*/resource-sync/*
athena:GetQueryExecution	*
athena:GetQueryResults	*
athena:StartQueryExecution	*
glue:GetTable	*
glue:GetPartition	*
glue:GetPartitions	*
organizations:DescribeOrganization	*
organizations:ListAccounts	*
organizations:DescribeAccount	*
organizations:ListChildren	*
organizations:ListParents	*
organizations:ListAccountsForParent	*
organizations:ListRoots	*
organizations:ListAWSServiceAccessForOrganization	*
ram:GetResourceShares	*
ram:GetResourceShareAssociations	*
ram:TagResource	*
ram:CreateResourceShare	*
ram:AssociateResourceShare	*

アクション	リソース ARN
<code>ram:DisassociateResourceShare</code>	*
<code>ram:UpdateResourceShare</code>	*
<code>ram>DeleteResourceShare</code>	*
<code>iam:GetRole</code>	*
<code>iam:PassRole</code>	<code>arn:aws:iam#*:role/licenseManagerServiceRole*</code>
<code>cloudformation:UpdateStack</code>	<code>arn:aws:cloudformation:*:stack/licenseManagercrossAccountcloudDiscoveryStack/*</code>
<code>cloudformation>CreateStack</code>	<code>arn:aws:cloudformation:*:stack/licenseManagercrossAccountcloudDiscoveryStack/*</code>
<code>cloudformation>DeleteStack</code>	<code>arn:aws:cloudformation:*:stack/licenseManagercrossAccountcloudDiscoveryStack/*</code>
<code>cloudformation:DescribeStacks</code>	<code>arn:aws:cloudformation:*:stack/licenseManagercrossAccountcloudDiscoveryStack/*</code>
<code>glue:CreateTable</code>	「 」を参照。
<code>glue:UpdateTable</code>	「 」を参照。
<code>glue>DeleteTable</code>	「 」を参照。
<code>glue:UpdateJob</code>	「 」を参照。
<code>glue:UpdateCrawler</code>	「 」を参照。

† 以下に、AWS Glueアクション:

- `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`

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。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許可」を参照してください。

管理アカウントのサービスにリンクされたロールの作成

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。クロスアカウントライセンス管理をAWS Management Consoleサービスにリンクされたロールは、License Managerで自動的に作成されます。

Note

License Managerでクロスアカウントサポートを利用するには、AWS Organizations。

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

IAM コンソールを使用することもできます。AWS CLI、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ができます。詳細については、IAM ユーザーガイドの「[サービスにリンクされたロールの作成](#)」を参照してください。

Important

このサービスにリンクされたロールがアカウントに表示されるのは、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です。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、ライセンスマネージャがAWSserviceOreforライセンスマネージャマスターアカウントロールアカウントで。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、サービスにリンクされたこのロールを作成できます。

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. 選択リンクAWS Organizationsアカウント。
4. [Apply] を選択します。

IAM コンソールを使用して、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。License Manager—管理アカウントのユースケース。または、AWS CLIまたはAWSAPI を使用するには、IAM を使用して、`license-manager.master-account.amazonaws.com`サービス名。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、同じ IAM 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を編集する

License Manager では、AWSserviceOreforライセンスマネージャマスターアカウントロールサービスにリンクされたロール サービスにリンクされたロールを作成すると、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を必要とする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のみが作成されます。ただし、手動で削除する前に、サービスにリンクされた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を手動で削除する

IAM コンソールを使用します。AWS CLI, またはAWSAPI を使用してAWSserviceOreforライセンスマネージャーマスターアカウントロールサービスにリンクされたロール 詳細については、[IAM ユーザーガイド](#)の「サービスにリンクされたロールの削除」を参照してください。

ライセンスマネージャー-メンバアカウントの役割

License Managerには、管理アカウントでライセンスを管理できるサービスにリンクされたロールが必要です。

メンバアカウントロールのアクセス許可

サービスにリンクされたロールAWSserviceOLEライセンスマネージャーメンバーアカウントトロールLicense Manager がAWSユーザーに代わってが、設定された管理アカウントからライセンス管理アクションを実行することをに許可します。

-AWSserviceOLEライセンスマネージャーメンバーアカウントトロールサービスにリンクされたロールは、`license-manager.member-account.amazonaws.com`サービスで、ロールを引き受ける必要があります。

ロールのアクセス許可ポリシーは、License Managerが次のアクションを指定されたリソースで完了することを許可します。

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

サービスにリンクされたロールの作成、編集、削除をIAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。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許可」を参照してください。

License Manager のサービスにリンクされたロールの作成

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。統合を有効にすることができます AWS OrganizationsのLicense Manager コンソールで管理アカウントから設定ページで。これは、AWS

CLI(を実行`update-service-settings`) またはAWSAPI (呼び出し`UpdateServiceSettings`). そうすることで、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このロールを削除したが、再作成する必要がある場合は、同じプロセスで、アカウントにロールを再作成することができます。

IAM コンソールを使用することもできます。AWS CLI、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ができます。詳細については、IAM ユーザーガイドの「[サービスにリンクされたロールの作成](#)」を参照してください。

Important

このサービスにリンクされたロールがアカウントに表示されるのは、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です。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によって`AWSserviceOLE`ライセンスマネージャーメンバーアカウントロールアカウントには、ロールがあります。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、サービスにリンクされたロールを作成できます。

サービスにリンクされたロールを作成するには

1. 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 (<https://console.aws.amazon.com/license-manager/>) を開きます。
3. 左側のナビゲーションペインで、[Settings]、[Edit] を選択します。
4. 選択リンクAWS Organizationsアカウント。
5. [Apply] を選択します。これにより、[AWSServiceRoleForAWSLicenseManagerRole \(p. 45\)](#) および [AWSServiceRoleForAWSLicenseManagerMemberAccountRole \(p. 52\)](#) の各ロールがすべての子アカウント内に作成されます。

IAM コンソールを使用して、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。License Manager --メンバーアカウント] ユースケースの例 または、AWS CLIまたはAWSAPI で、サービスにリンクされたロールを作成するには、`license-manager.member-account.amazonaws.com`サービス名。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、同じ IAM 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を編集する

License Manager では、`AWSserviceOLE`ライセンスマネージャーメンバーアカウントトロールサービスにリンクされたロール サービスにリンクされたロールを作成すると、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を必要とする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のみが作成されます。ただし、手動で削除する前に、サービスにリンクされた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を手動で削除する

IAM コンソールを使用します。AWS CLI、またはAWSAPI を使用してAWSservicerOLEライセンスマネージャーメンバーアカウントトロールサービスにリンクされたロール 詳細については、IAM ユーザーガイドの「[サービスにリンクされたロールの削除](#)」を参照してください。

AWS 用の 管理ポリシーAWS License Manager

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。チームに必要なアクセス許可のみを提供する [IAM カスタマー管理ポリシーを作成する](#)には、時間と専門知識が必要です。すぐに使用を開始するために、AWS 管理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管理ポリシーの詳細については、IAM ユーザーガイドの[AWS管理ポリシー](#)を参照してください。

AWS サービスは、AWS 管理ポリシーを維持および更新します。AWS 管理ポリシーのアクセス許可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 管理ポリシーにアクセス許可が追加されることがあります。このタイプの更新は、ポリシーがアタッチされているすべての ID (ユーザー、グループ、ロール) に影響します。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 管理ポリシーを更新する可能性が最も高くなります。サービスは AWS 管理ポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が破棄されることはありません。

加えて AWS では、複数のサービスにまたがる職務機能のための管理ポリシーもサポートしています。例えば、ReadOnlyAccessAWS管理ポリシーでは、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、AWS は、追加されたオペレーションとリソースに対し、読み取り専用のアクセス許可を設定します。ジョブ機能ポリシーのリストと説明については、IAM ユーザーガイドのジョブ機能の「[AWS 管理ポリシー](#)」を参照してください。

AWS管理ポリシー: AWSライセンスマネージャーサービスポリシーポリシー

このポリシーは、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。AWSservicerOLEライセンス管理機能License Manager が API アクションを呼び出して、ユーザーに代わってライセンスを管理できるようにします。詳細については、「[のサービスにリンクされたロールの使用AWS License Manager \(p. 45\)](#)」を参照してください。

AWS管理ポリシー: AWSライセンスマネージャーマスターアカウントポリシー

このポリシーは、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。AWSservicerOreforライセンスマネージャーマスターアカウントトロールLicense Manager が API アクションを呼び出して、集中管理アカウントのライセンス管理を管理できるようにします。詳細については、「[のサービスにリンクされたロールの使用AWS License Manager \(p. 45\)](#)」を参照してください。

AWS管理ポリシー: AWSライセンスマネージャーメンバーアカウントポリシー

このポリシーは、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。AWSservicerOLEライセンスマネージャーメンバーアカウントトロールLicense Manager が、ユーザーに代わってが API アク

ションを呼び出して、設定された管理アカウントからライセンス管理用のアクションを呼び出せるようにします。詳細については、「[のサービスにリンクされたロールの使用AWS License Manager \(p. 45\)](#)」を参照してください。

AWS管理ポリシー: AWSライセンスマネージャーの消費ポリシー

IAM ID に `AWSLicenseManagerConsumptionPolicy` ポリシーをアタッチできます。このポリシーは、ライセンスを消費するのに必要な License Manager API アクションへのアクセスを許可するアクセス許可を付与します。詳細については、「[ライセンス使用量 \(p. 33\)](#)」を参照してください。

このポリシーの許可を確認するには、「[AWSライセンスマネージャーの消費ポリシー](#)」のAWS Management Console。

License Manager の更新をAWSマネージドポリシー

の更新に関する詳細の表示。AWS License Manager 用の管理ポリシーを、このサービスがこれらの変更の追跡を開始した以降の分について表示します このページの変更に関する自動通知を入手するには、License Manager ドキュメントの履歴ページから、RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSライセンスマネージャーの消費ポリシー (p. 55) — 新しいポリシー	License Manager は、ライセンスを消費する権限を付与する新しいポリシーを追加しました。	2021年8月11日
AWSライセンスマネージャーサービスポリシーポリシー (p. 54) — 既存ポリシーへの更新	License Manager が、委任された管理者をリストするアクセス許可と、サービスにリンクされたロールを作成するためのアクセス許可をAWSserviceOLEライセンスマネージャーメンバーアカウントロール。	2021年6月16日
AWSライセンスマネージャーサービスポリシーポリシー (p. 54) — 既存ポリシーへの更新	License Managerは、ライセンス構成、ライセンス、許可など、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
AWSライセンスマネージャーサービスポリシーポリシー (p. 54) — 既存ポリシーへの更新	License Manager が、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ためのアクセス許可を追加しました。AWS サービスロールマーケットプレイスライセンス管理。この役割は、AWS Marketplace ライセンスマネージャーでライセンスを作成および管理するための権限を持ちます。詳細については、「 」を参照してください。 のサービスにリンクされたロール AWS Marketplace の AWS Marketplace 購入者ガイド。	2021年3月9日

変更	説明	日付
License Manager が変更の追跡	License Manager が変更の追跡を開始しました。AWS管理ポリシー。	2021 年 3 月 9 日

ライセンスの暗号署名

License Manager は、ISV によって発行されたライセンスまたは AWS Marketplace ISVに代わって行われます。署名により、ベンダーはオフライン環境であっても、アプリケーション自体内のライセンスの整合性と発行元を検証できます。

License Manager は ISV に属し、非対称顧客マスターキー (CMK) を使用して、ライセンスに署名します。AWS Key Management Service(AWS KMS). 顧客管理の CMK は、数学的に関連するパブリックキーとプライベートkey pair 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 はライセンス資格をリストした JSON オブジェクトを生成し、このオブジェクトに秘密キーで署名します。署名とプレーンテキストの 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持つ当事者は、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秘密キーの所有者によって署名されていることを確認できます。key pair プライベート部分は、AWS KMS. 非対称暗号化の詳細については、「」を参照してください。AWS KMS 「」を参照してください。[対称キーと非対称キーの使用](#)。

Note

License Manager は、AWS KMS [Sign](#)および[Verify](#)ライセンスに署名および検証するときの API 操作。CMK には、キーの使用法値が「」が必要です。[SIGN_V](#)をこれらの操作で使用します。このさまざまな CMK は、暗号化および復号化には使用できません。

次のワークフローでは、暗号で署名されたライセンスの発行について説明します。

1. 左AWS KMSコンソール、API、または SDK を使用する場合、ライセンス管理者は非対称カスタマー管理型 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、「」を参照してください。[非対称 CMK の作成およびCMK 設定の選択方法](#)。
2. License Manager では、ライセンス管理者が使用コンフィギュレーションを作成します。このコンフィギュレーションには、AWS KMSARN または ID。設定では、いずれかまたは両方を指定することができます。借用および仮称オプション。詳細については、「」を参照してください。[出品者が発行したライセンスのブロックの作成](#)。
3. エンドユーザーがライセンスを取得するには、[CheckoutLicense](#)または[CheckoutBorrowLicense](#)API オペレーション。-CheckoutBorrowLicense操作は、借用設定。レスポンスの一部として、エンタイトルメントをリストする JSON オブジェクトとともに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::277886486208:license:1-6585590917ad46858328ff02dEXAMPLE",
  "licenseConsumptionToken":"306eb19afd354ba79c3687b9bEXAMPLE",
```

```
"nodeId": "100.20.15.10",  
"checkoutMetadata": {  
  "Mac": "ABCDEFGH1"  
}  
}
```

AWS License Manager のコンプライアンス検証

サードパーティの監査担当者は、セキュリティとコンプライアンスを評価します。AWSサービスの一部としてAWSコンプライアンスプログラム (SOC、PCI、FedRAMP、HIPAA など) を使用できます。

かどうかを知るためにAWS License Managerまたは他のAWSのサービスには、特定のコンプライアンスプログラムの対象となるサービスが含まれています。詳細については、[AWSコンプライアンスプログラムによる対象範囲内のサービス](#)。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。

サードパーティーの監査レポートをダウンロードするには、AWS Artifact を使用します。詳細については、[AWS Artifactにおけるレポートのダウンロード](#)を参照してください。

AWS サービスを使用する際のお客様のコンプライアンス責任は、データの機密性、企業のコンプライアンス目的、適用法規によって決まります。AWS ではコンプライアンスに役立つ以下のリソースを用意しています。

- [セキュリティおよびコンプライアンスのクイックスタートガイド](#)これらのデプロイメントガイドでは、アーキテクチャ上の考慮事項について説明し、ベースライン環境をにデプロイするための手順を説明しますAWSは、セキュリティとコンプライアンスに重点を置いています。
- [HIPAA Security and Compliance for HIPAA Security](#)— このホワイトペーパーでは、企業がAWSを使用してHIPAAに準拠するアプリケーションを作成します。

Note

すべてのサービスがHIPAAに準拠しているわけではありません。

- [AWSコンプライアンスのリソース](#)-このワークブックおよびガイド群には、貴社の所在地や業界に適用可能なものが含まれています。
- [ルールでのリソースの評価](#)(AWS Config開発者ガイド—AWS Configサービスでは、自社プラクティス、業界ガイドライン、および規制に対するリソースの設定の準拠状態を評価します。
- [AWS Security Hub](#)— このAWSサービスでは、セキュリティ状態に関する包括的な表示をAWSセキュリティ業界の標準およびベストプラクティスへの準拠を確認できます。
- [AWS Audit Manager](#)— このAWSサービスを使用すると、AWSの使用方法により、リスクの管理方法を簡素化し、規制や業界標準へのコンプライアンスを実現できます。

AWS License Manager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として、AWS License Managerによって保護されているAWSグローバルネットワークセキュリティ手順については、[Amazon Web Services: セキュリティプロセスの概要](#)ホワイトペーパー。

使用するAWSが公開している 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。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。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)

Virtual Private Cloud (VPC) と間にプライベート接続を確立できます。AWS License Manager インターフェイス VPC エンドポイントを作成することで、を使用できます。インターフェイスエンドポイントはを使用します。[AWS PrivateLink](#) このテクノロジーは、インターネットゲートウェイ License Manager NAT デバイス、VPN 接続、またはAWS Direct Connect接続。VPC のインスタンスは、パブリック IP アドレスがなくても License Manager と通信できます。VPC と License Manager 間のトラフィックは、Amazon ネットワークを離れません。

各インターフェイスエンドポイントは、サブネット内の 1 つ以上の [Elastic Network Interface](#) によって表されます。

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

License Manager 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 のインターフェイスエンドポイントを作成します。

- com.amazonaws.#####license-manager
- com.amazonaws.#####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 名を使用して、License Manager に API リクエストを実行できます。たとえば、license-manager.[region](#).amazonaws.com と指定します。

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

License Manager の VPC エンドポイントポリシーの作成

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
- このアクションを実行できるリソース

License Manager のエンドポイントポリシーの例を次に示します。このポリシーは、エンドポイントにアタッチされると、すべてのリソースのすべてのプリンシパルに対して、指定されている License Manager アクションへのアクセスを許可します。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "license-manager:*"
      ],
      "Resource": "*"
    }
  ]
}
```

詳細については、「[VPC エンドポイントを使用したサービスのアクセスコントロール](#)」を参照してください。Amazon VPC ユーザーガイド。

AWS License Manager のトラブルシューティング

以下の情報は、トラブルシューティングに役立ちます。AWS License Manager。開始する前に、License Manager のセットアップが、に記載されている要件を満たしているか確認してから実施してください。 [License Manager の設定 \(p. 40\)](#)。

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、[Search Inventory] 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 クエリ失敗-クエリ実行権限がありません。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、Athena マネージドデータカタログをAWS Glue Data Catalog。アップグレードの手順については、以下を参照してください。 [へのアップグレードAWS Glue データカタログのステップバイステップのインストール](#)。

マスターアカウントは、ライセンス構成からリソースの関連付けを解除できません

組織のメンバーアカウントが `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` サービスにリンクされたロール (SLR) であるであり、特定のライセンス設定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、該当するライセンスとメンバーアカウントのリソースの関連付けを解除できません。つまり、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、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実行できないようにする場合に検討します。

Systems Manager のインベントリは、最新のものではありません

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、License Manager は、Ping に応答しない場合であっても、マネージドインスタンスをアクティブ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 は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

アカウントを保つには、License Manager がクリーンアップ処理を実行できるように、Systems Manager 内のインスタンスの登録を手動で解除することをお勧めします。

登録解除された AMI の見かけ上の永続性

License Manager は、数時間ごとに、リソースとライセンス設定の古い関連付けを消去します。ライセンス設定に関連付けられた AMI の登録を Amazon EC2 を通じて解除しても、完全消去されるまで、完全消去されるまで、この AMI の表示が License Manager リソースインベントリ内に一時的に残ることがあります。

新しい子アカウントインスタンスがリソースインベントリに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、デフォルトでは毎日午後 1 時にお客様のアカウントを更新します。この更新後に追加されたインスタンスは、翌日の更新後に、管理アカウントリソースインベントリに表示されます。更新スクリプトの実行頻度を変更するには、`LicenseManagerResourceSynDataProcessJobTrigger()` AWS Glue コンソールに管理アカウントを割り当てます。

クロスアカウントモードを有効にすると、子アカウントインスタンスの表示が遅くなる

License Manager 内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は、数分から数時間後にリソースインベントリ内に表示されます。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にすることはできません

アカウントが、クロスアカウント検出用に構成された後、シングルアカウント検出に戻すことはできません。

子アカウントユーザーは、共有ライセンス設定をインスタンスに関連付けることができません。

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。
- 子アカウントは、管理アカウントで作成されたリソース共有から削除されました。
- ライセンス設定がリソース共有から削除されている。

Linking (リンク中)AWS Organizationsアカウント失敗

[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、管理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た。

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

AWS License Manager はおよびと統合されます。AWS CloudTrail は、ユーザー、ロール、または AWS License Manager でサービスします。CloudTrail は、License Manager のすべての API 呼び出しをイベントとしてキャプチャします。キャプチャされた呼び出しには、License Manager コンソールからの呼び出しと、License Manager API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、License Manager のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的デリバリーを有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [Event history] で最新のイベントを表示できます。CloudTrail によって収集された情報を使用して、License Manager に対して行われたリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

CloudTrail の詳細については、[AWS CloudTrail ユーザーガイド](#)。

CloudTrail の License Manager 情報

CloudTrail は AWS アカウントを作成します。License Manager でアクティビティが発生すると CloudTrail そのアクティビティは他の AWS のサービスイベント履歴。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。

のイベントの継続的な記録については、AWS License Manager のイベントなど、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡では、すべてのリージョンのイベントが AWS パーティションを作成し、指定した Amazon S3 バケットにログファイルを渡します。さらに、その他の AWS のサービスを通じて、CloudTrail ログで収集されたデータに基づき、詳細な分析やアクティビティを行うことができます。詳細については、以下を参照してください。

- [証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 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 Manager API リファレンス](#)。たとえば、`CreateLicenseConfiguration`、`ListResourceInventory` および `DeleteLicenseConfiguration` アクションでは、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、リクエストの生成者に関する情報が含まれます。この ID 情報により以下を確認できます。

- リクエストが、root 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、ロールとフェデレーテッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか。
- リクエストが、別の AWS 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 userIdentity エレメント](#)」を参照してください。

License Manager のログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できる設定です。CloudTrail ログファイルには、1 つ以上のログエントリがあります。イベントは任意の発生元からの 1 つ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に関する情報が含まれます。CloudTrail ログファイルは、パブリック API 呼び出し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。

次は、DeleteLicenseConfiguration アクションを示す CloudTrail ログエントリの例です。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAIIF2U5EXAMPLEH5AP6",
    "arn": "arn:aws:iam::O12345678901:user/Administrator",
    "accountId": "O12345678901",
    "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": "Coral/Netty4",
  "requestParameters": {
    "licenseConfigurationArn": "arn:aws:license-manager:us-east-1:O12345678901:license-configuration:lic-9ab477f4bEXAMPLE55f3ec08a5423f77"
  },
  "responseElements": null,
  "requestID": "3366df5f-4166-415f-9437-c38EXAMPLE48",
  "eventID": "6c2c949b-1a81-406a-a0d7-52EXAMPLE5bd",
  "eventType": "AwsApiCall",
  "recipientAccountId": "O12345678901"
}
```

AWS License Manager のドキュメント履歴

次の表では、AWS License Manager のリリースを説明しています。

機能	説明	日付
ライセンスタイプ変換	ライセンスの種類をAWSで提供されるライセンス使用と自分のライセンス使用 (BYOL) により、既存のワークロードを再デプロイする必要はありません。	2021年9月22日
使用権限の共有	管理されたライセンス資格を1つのリクエストで組織全体で共有できます。	2021年7月16日
ライセンスレポート	License Managerレポートジェネレーターを使用して、ライセンスタイプ設定の履歴を追跡します。	2021年5月18日
自動検出除外ルール	License Managerの自動検出からインスタンスを除外するAWSアカウントIDとタグ。	2021年3月5日
マネージド使用権限の確認	から購入した製品のライセンス資格を追跡および配布するAWS Marketplace およびライセンスマネージャを使用してライセンスを配布する出品者	2020年12月3日
アンインストールしたソフトウェアの自動アカウントティング	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	ライセンス設定とAMIをAWSアカウント。	2020年11月23日
ホストへのライセンスのアフィニティ	特定の日数の間、専用ハードウェアにライセンスを割り当てます。	2020年8月12日
Amazon RDS での Oracle デプロイの追跡	Amazon RDS で Oracle データベースエンジンエディションとライセンスパックのライセンス使用状況を追跡します。	2020年3月23日

機能	説明	日付
ホストリソースグループ	ホストリソースグループを構成して、License Manager で専用ホストを管理できるようにします。	2019 年 12 月 1 日
ソフトウェアの自動検出	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、対応するライセンス設定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
ライセンス込みの差別化と自分のライセンス使用	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基づいて、検索結果を絞り込みます。	2019 年 11 月 8 日
オンプレミスリソースへのライセンスのアタッチ	オンプレミスのインスタンスにライセンスをアタッチすると、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、使用状況を報告します。	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。