亚马逊云科技

User Guide

Amazon License Manager

Amazon License Manager: User Guide

Table of Contents

What is Amazon License Manager?

Amazon License Manager is a service that makes it easier for you to manage your software licenses from software vendors (for example, Microsoft, SAP, Oracle, and IBM) centrally across Amazon and your on-premises environments. This provides control and visibility into the usage of your licenses, enabling you to limit licensing overages and reduce the risk of non-compliance and misreporting.

As you build out your cloud infrastructure on Amazon, you can save costs by using Bring Your Own License model (BYOL) opportunities. That is, you can re-purpose your existing license inventory for use with your cloud resources.

License Manager reduces the risk of licensing overages and penalties with inventory tracking that is tied directly into Amazon services. With rule-based controls on the consumption of licenses, administrators can set hard or soft limits on new and existing cloud deployments. Based on these limits, License Manager helps stop non-compliant server usage before it happens.

License Manager's built-in dashboards provide ongoing visibility into license usage and assistance with vendor audits.

License Manager supports tracking any software that is licensed based on virtual cores (vCPUs), physical cores, sockets, or number of machines. This includes a variety of software products from Microsoft, IBM, SAP, Oracle, and other vendors.

With Amazon License Manager, you can centrally track licenses and enforce limits across multiple Regions, by maintaining a count of all the checked out entitlements. License Manager also tracks the end-user identity and the underlying resource identifier, if available, associated with each check out, along with the check-out time. This time-series data can be tracked to the ISV through CloudWatch metrics and events. ISVs can use this data for analytics, auditing, and other similar purposes.

Amazon License Manager is integrated with Amazon Web Services Marketplace and Amazon Data Exchange, and with the following Amazon services: Amazon Identity and Access Management (IAM), Amazon Organizations, Service Quotas, Amazon CloudFormation, Amazon resource tagging, and Amazon X-Ray.

Managed Entitlements

With License Manager, a license administrator can distribute, activate, and track software licenses across accounts and throughout an organization.

Independent software vendors (ISVs) can use Amazon License Manager to manage and distribute software licenses and data to end-users by means of managed entitlements. As an issuer, you can track the usage of your seller-issued licenses centrally using the License Manager dashboard. ISVs selling through Amazon Web Services Marketplace benefit from automatic license creation and distribution as a part of the transaction workflow. ISVs can also use License Manager to create license keys and activate licenses for customers without an Amazon account.

License Manager uses open, secure, industry standards for representing licenses and allows customers to cryptographically verify their authenticity. License Manager supports a variety of different licensing models including perpetual licenses, floating licenses, subscription licenses, and usage-based licenses. If you have licenses that must be node-locked, License Manager provides mechanisms to consume your licenses in that way.

You can create licenses in Amazon License Manager and distribute them to end-users using an IAM identity or through digitally signed tokens generated by Amazon License Manager. End-users using Amazon can further redistribute the license entitlements to Amazon identities in their respective organizations. End-users with distributed entitlements can check out and check in the required entitlements from that license through your software integration with Amazon License Manager. Each license check out specifies the entitlements, the associated quantity, and check-out time period such as checking out 10 **`admin-users`** for 1 hour. This check out can be performed based on the underlying IAM identity for the distributed license or based on the long-lived tokens generated by Amazon License Manager through the Amazon License Manager service.

License Manager use cases

The following are examples of the functionality provided by License Manager for various use cases:

- Self-managed licenses in License Manager – Used to define licensing rules based on the terms of your enterprise agreements which determine how Amazon processes commands that consume these licenses.
- Seller issued licenses in License Manager – Used to manage and distribute software licenses to end-users.
- Granted licenses in License Manager – Used to govern the use of licenses acquired from the Amazon Web Services Marketplace, Amazon Web Services Data Exchange, or directly from a seller who integrated their software with managed entitlements.

- License type conversions in License Manager – Used to change your license type between Amazon provided licensing and the Bring Your Own License model (BYOL) without redeploying your workloads.
- Inventory search in License Manager – Used to discover and track on-premises applications using Amazon Systems Manager Inventory and licensing rules.
- ??? – Used to purchase fully compliant Amazon provided licenses for supported software with a per user subscription fee.
- Linux subscriptions in License Manager – Used to view and manage commercial Linux subscriptions you own and run on Amazon.

Related services

License Manager is integrated with Amazon EC2, Amazon RDS, Amazon Web Services Marketplace, Amazon Systems Manager, and Amazon Organizations.

The Amazon EC2 integration allows you to track licenses for the following resources and enforce licensing rules throughout the resource lifecycle:

- Amazon EC2 instances
- Dedicated Instances
- Dedicated Hosts
- Spot Instances and Spot Fleet
- Managed nodes

When you use License Manager along with Amazon Systems Manager, you can manage licenses on physical or virtual servers hosted outside of Amazon. You can use License Manager with Amazon Organizations to manage all of your organizational accounts centrally.

Additionally, you can govern the use of licenses purchased from Amazon Web Services Marketplace, Amazon Web Services Data Exchange, or directly from a seller who integrated their software with Amazon License Manager. You can use Amazon License Manager to distribute rights of use, known as entitlements, to specific Amazon Web Services accounts.

License Manager integrates with Amazon RDS for Oracle and Amazon RDS for Db2 vCPU-based BYOL licenses. With this integration, you gain visibility into vCPU usage for your RDS for Oracle and RDS for Db2 DB instances. You can use this data to calculate the number of licenses

consumed based on your licensing terms with the database management system vendors. For more information, see the following associated links in the *Amazon RDS User Guide*.

- RDS for Oracle licensing options
- RDS for Db2 licensing options

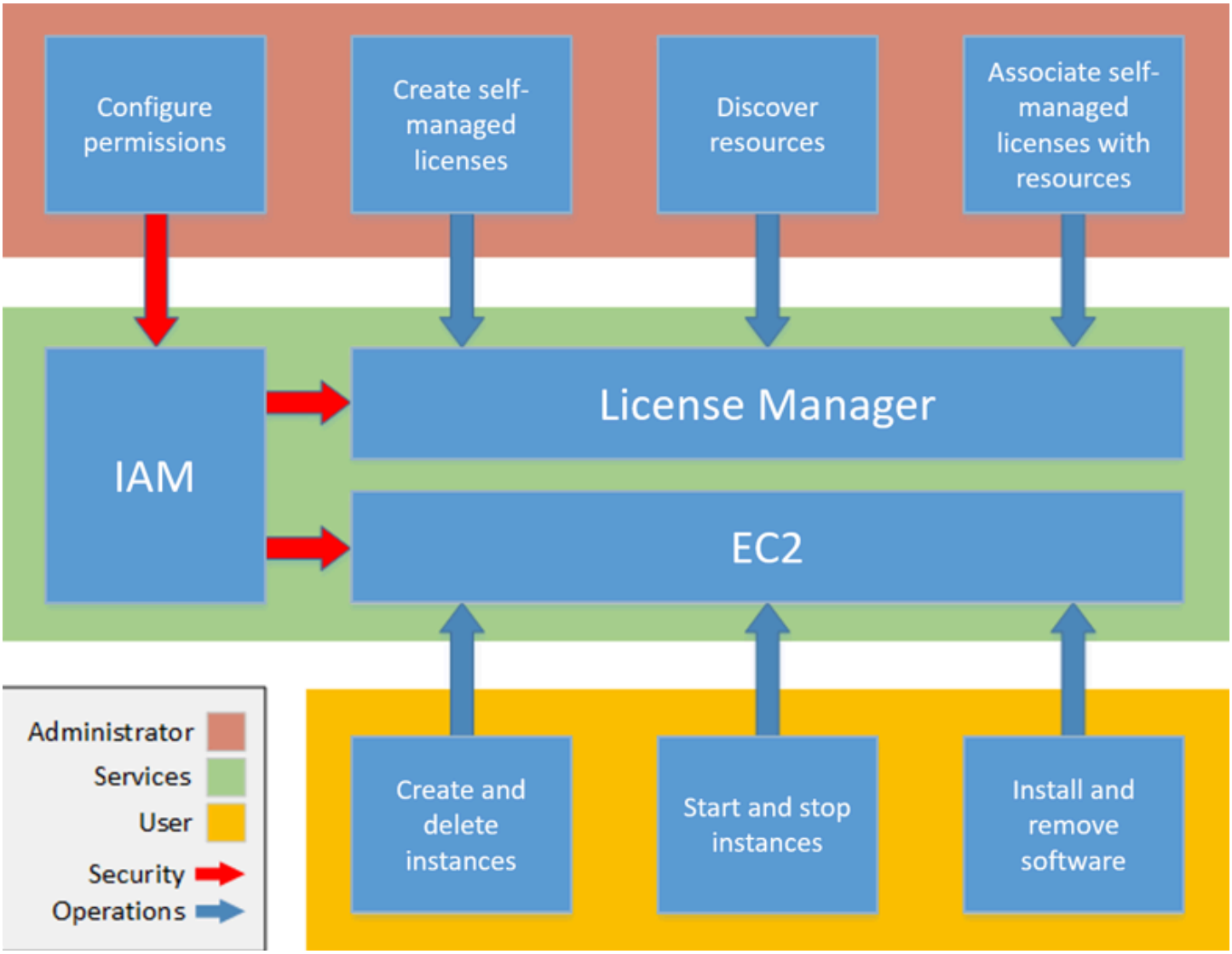
How License Manager works

Effective software license management relies on the following:

- An expert understanding of language in enterprise licensing agreements
- Appropriately restricted access to operations that consume licenses
- Accurate tracking of license inventory

Enterprises are likely to have dedicated persons or teams responsible for each of these domains. It then becomes a problem of effective communication, particularly between license experts and system administrators. License Manager provides a way of pooling knowledge from various domains. Crucially, it also integrates natively with Amazon services—for example, with the Amazon EC2 control plane where instances are created and deleted. This means that License Manager rules and limits capture business and operational knowledge, and also translate to automated controls on instance creation and application deployment.

The following diagram illustrates the distinct but coordinated duties of license administrators, who manage permissions and configure License Manager, and users, who create, manage, and delete resources through the Amazon EC2 console.



If you are responsible for managing licenses in your organization, you can use License Manager to set up licensing rules, attach them to your launches, and keep track of usage. The users in your organization can then add and remove license-consuming resources without additional work.

A licensing expert manages licenses across the entire organization, determining resource inventory needs, supervising license procurement, and driving compliant license usage. In an enterprise using License Manager, this work is consolidated through the License Manager console. As shown in the diagram, this involves setting service permissions, creating self-managed licenses, taking inventory of computing resources both on-premises and in the cloud, and associating self-managed licenses with discovered resources. In practice, this could mean associating a self-managed license with an approved Amazon Machine Image (AMI) that IT uses as a template for all Amazon EC2 instance deployments.

License Manager saves costs that would otherwise be lost to license violations. While internal audits reveal violations only after the fact, when it is too late to avoid penalties for non-compliance, License Manager prevents expensive incidents from ever occurring. License Manager simplifies reporting with built-in dashboards showing license consumption and resources tracked.

Getting started with Amazon License Manager

The following sections guide you in setting up your Amazon Web Services account and users, and how to get started with License Manager. For more information on managing permissions for users, groups, and roles to utilize License Manager while following Amazon best practices, see Identity and access management for Amazon License Manager. For more information about setting up your Amazon EC2 resources that integrate with License Manager, see Set up to use Amazon EC2 in the *Amazon Elastic Compute Cloud User Guide*.

Topics

Setting up

The following section details setting up your Amazon Web Services account and users.

Sign up for an Amazon Web Services account

If you do not have an Amazon Web Services account, use the following procedure to create one.

To sign up for Amazon Web Services

1. Open http://www.amazonaws.cn/ and choose **Sign Up**.
2. Follow the on-screen instructions.

Amazon sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to http://www.amazonaws.cn/ and choosing **My Account**.

Secure IAM users

After you sign up for an Amazon Web Services account, safeguard your administrative user by turning on multi-factor authentication (MFA). For instructions, see Enable a virtual MFA device for an IAM user (console) in the *IAM User Guide*.

To give other users access to your Amazon Web Services account resources, create IAM users. To secure your IAM users, turn on MFA and only give the IAM users the permissions needed to perform their tasks.

For more information about creating and securing IAM users, see the following topics in the *IAM User Guide*:

- Creating an IAM user in your Amazon Web Services account
- Access management for Amazon resources
- Example IAM identity-based policies

Onboard to use License Manager on the Amazon Web Services Management Console

The following procedure is required to get started with License Manager. Once the initial requirements are complete, you can proceed with using License Manager for your desired use case.

To get started with License Manager

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. You are prompted to configure permissions for License Manager and its supporting services. Follow the directions to configure the required permissions.
3. With the initial setup complete, you can proceed with using License Manager for your desired License Manager use cases.

Working with Amazon License Manager

License Manager can be applied to standard scenarios for enterprises with a mixed infrastructure of Amazon resources and on-premises resources. You can create self-managed licenses, take inventory of your license-consuming resources, associate self-managed licenses with resources, and track inventory and compliance.

Licensing for Amazon Web Services Marketplace products

Using License Manager, you can now associate licensing rules to Amazon Web Services Marketplace BYOL AMI products via Amazon EC2 launch templates, Amazon CloudFormation templates, or Service Catalog products. In each case, you benefit from centralized license-tracking and compliance enforcement.

> **Note**
>
> License Manager does not change how you obtain and activate your BYOL AMIs from Marketplace. After launching, you must provide a license key obtained directly from the seller to activate any third-party software.

Tracking licenses for resources in on-premises data centers

With License Manager, you can discover applications running outside of Amazon with the Systems Manager inventory, and then attach licensing rules to them. After licensing rules are attached, you can track on-premises servers along with Amazon resources in the License Manager console.

Differentiate between license included and BYOL

With License Manager, you can identify which resources have a license that is included with the product and which use a license that you own. This enables you to accurately report how you are using BYOL licenses. This filter requires SSM version 2.3.722.0 or later.

License Manager across your Amazon accounts

License Manager enables you to manage licenses across your Amazon accounts. You can create license configurations once in your Amazon Organizations management account and share them across your accounts using Amazon Resource Access Manager or by linking Amazon Organizations accounts using License Manager settings. This also enables you to perform cross-account discovery to search inventory across your Amazon accounts.

The following Regions do not support license management across Amazon accounts:

- China (Beijing)
- China (Ningxia)

Contents

Self-managed licenses in License Manager

Self-managed licenses are the core of License Manager. Self-managed licenses were formerly known as "license configurations". Self-managed licenses contain licensing rules based on the terms of your enterprise agreements. The rules that you create determine how Amazon processes commands that consume licenses. While creating self-managed licenses, work closely with your organization's compliance team to review your enterprise agreements.

Limits

- Number of self-managed licenses per resource: 10
- Total number of self-managed licenses: 25
- Systems Manager managed instances must be associated with vCPU and instance type self-managed licenses.

Contents

Self-managed license parameters and rules

A self-managed license consists of basic parameters and rules that vary according to the parameter values. You can also add tags to your self-managed licenses. After you create a self-managed license, an administrator can modify the number of licenses and the usage limit to reflect changing resource needs.

Available parameters and rules include the following:

- **Self-managed license name** – The name of the self-managed license.
- **(Optional) Description** – A description of the self-managed license.
- **License type** – The metric used to count licenses. Supported values are **vCPUs**, **Cores**, **Sockets**, and **Instances**.
- **(Optional) Number of <option>** – The number of licenses used by a resource.
- **Status** – Indicates whether the configuration is active.
- **Product information** – The names and versions of the products for automated discovery. The supported products are Windows Server, SQL Server, Amazon RDS for Oracle, and Amazon RDS for Db2.
- **(Optional) Rules** – These include the following. Available rules vary by counting type.
  - **License affinity to host (in days)** – Restricts license usage to the host for the specified number of days. The range is 1 to 180. The counting type must be Cores or Sockets. After the affinity period elapses, the license will be available for reuse within 24 hours.
  - **Maximum cores** – Maximum count cores for a resource.
  - **Maximum sockets** – Maximum count sockets for a resource.
  - **Maximum vCPUs** – Maximum count vCPUs for a resource.
  - **Minimum cores** – Minimum count cores for a resource.

- **Minimum sockets** – Minimum count sockets for a resource.
- **Minimum vCPUs** – Minimum count vCPUs for a resource.
- **Tenancy** – Restricts license usage to the specified EC2 tenancy. Dedicated Hosts are required if the counting type is Cores or Sockets. Shared tenancy, Dedicated Hosts, and Dedicated Instances are supported if the counting type is Instances or vCPUs. The console (and API) names are as follows:
  - **Shared** (`EC2-Default`)
  - **Dedicated Instance** (`EC2-DedicatedInstance`)
  - **Dedicated Host** (`EC2-DedicatedHost`)
  - **vCPU Optimization** – License Manager integrates with CPU optimization support in Amazon EC2, which enables you to customize the number of vCPUs on an instance. If this rule is set to True, License Manager counts vCPUs based on the customized core and thread count. Otherwise, License Manager counts the default number of vCPUs for the instance type.

The following table describes which license rules are available for each counting type.

Console name	API name	Cores	Instances	Sockets	vCPUs
License affinity to host (in days)	`licenseAffinityToHost`	✓		✓	
Maximum cores	`maximumCores`	✓	✓		
Maximum sockets	`maximumSockets`		✓	✓	
Maximum vCPUs	`maximumVcpus`		✓		✓
Minimum cores	`minimumCores`	✓	✓		
Minimum sockets	`minimumSockets`		✓	✓	
Minimum vCPUs	`minimumVcpus`		✓		✓
Tenancy	`allowedTenancy`	✓	✓	✓	✓
vCPU Optimization	`honorVcpuOptimization`				✓

Build License Manager rules from vendor licenses

You can create License Manager rule sets based on the language of software vendor licenses. The examples that follow are not intended as blueprints for actual use cases. In any real-world application of a license agreement, you choose among competing options depending on the architecture and licensing history of your particular on-premises server environment. Your options also depend on the details of your planned migration of resources to Amazon.

As much as possible, these examples are meant to be vendor-neutral, focusing instead on generally applicable questions of hardware and software allocation. Vendor licensing provisions interact as well with Amazon requirements and limits. The number of licenses required for an application varies according to the instance type chosen and other factors.

> **Important**
>
> Amazon does not participate in the audit process with software vendors. Customers are responsible for compliance and assume the responsibility of carefully understanding and capturing rules into License Manager based on their licensing agreements.

Example: Implementing an operating system license

This example involves a license for a server operating system. The licensing language imposes constraints on the type of CPU core, tenancy, and minimum number of licenses per server.

In this example, the licensing terms include the following stipulations:

- Physical processor cores determine the license count.
- The number of licenses must equal the number of cores.
- A server must run a minimum of eight cores.
- The operating system must run on a non-virtualized host.

In addition, the customer has made the following decisions:

- Licenses for 96 cores have been purchased.
- A hard limit is imposed to restrict license consumption to the quantity purchased.
- Each server needs a maximum of 16 cores.

The following table associates the License Manager rule-making parameters with the vendor licensing requirements that they capture and automate. The example values are for illustration purposes only; you would specify the values that you need in your own self-managed licenses.

License Manager Rule	Settings
License counting type	**License Type** is set to **`Cores`**.
License count	**Number of cores** is set to **96**.
Minimum / Maximum vCPUs or cores	**Minimum cores** is set to **8**. **Maximum cores** is set to **16**.
License count hard limit	**Enforce license limit** is selected.
Allowed tenancy	**Tenancy** is set to **`Dedicated Host`**.

Create a self-managed license

A self-managed license represents the licensing terms in the agreement with your software vendor. Your self-managed license specifies how your licenses should be counted (for example, by vCPUs or number of instances). It also specifies limits on your usage, so that you can prevent usage from going over the number of allocated licenses. Additionally, it can also specify other constraints on your licenses, such as the tenancy type.

Considerations for Amazon RDS for Oracle and Amazon RDS for Db2 databases

When you add product information to configure automated discovery of Amazon RDS for Oracle or Amazon RDS for Db2 databases, the following requirements apply:

- The supported license counting type is vCPU.
- Rules are not supported.
- Hard license limits are not supported.
- You can track one product version per self-managed license.

- You cannot track Amazon RDS databases and other products using the same self-managed license.

To create a self-managed license using the console

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **self-managed licenses**.
3. Choose **Create self-managed license**.
4. In the **Configuration details** panel, provide the following information:
   - **Self-managed license name** – A name for the self-managed license.
   - **Description** – An optional description of the self-managed license.
   - **License type** – The counting model for this license (**vCPUs**, **Cores**, **Sockets**, or **Instances**).
   - **Number of <option>** – The option displayed depends on the license type. When the license limit is exceeded, License Manager notifies you (soft limit) or prevents a resource from deploying (hard limit).
   - **Enforce license limit** – If selected, the license limit is a hard limit.
   - **Rules** – One or more rules. For each rule, select a rule type, provide a rule value, and choose **Add rule**. The rule types displayed depend on the license type. For example, minimum values, maximum values, and tenancy. If you do not specify a tenancy type, all are accepted.
5. (Optional) In the **Automated discovery rules** panel, do the following:
   a. Choose the product name, product type, and resource type for each product to discover and track using automated discovery.
   b. Select **Stop tracking instances when software is uninstalled** to make the license available for reuse after License Manager detects that the software was uninstalled and any license affinity period has elapsed.
   c. (Optional) If your account is a License Manager management account for an Organizations you have to option to define resources to exclude from automated discovery. To do so select **Add exclusion rule**, choose the property to filter on, Amazon account IDs and resource Tags are supported, then enter the information to identify that property.
6. (Optional) Expand the **Tags** panel to add one or more tags to your self-managed license. Tags are key/value pairs. Provide the following information for each tag:
   - **Key** – The searchable name of the key.

- **Value** – The value for the key.

7. Choose **Submit**.

To create a self-managed license using the command line

- create-license-configuration (Amazon CLI)
- New-LICMLicenseConfiguration (Amazon Tools for PowerShell)

Share a self-managed license

You can use Amazon Resource Access Manager to share your self-managed licenses with any Amazon account or through Amazon Organizations. For more information, see Sharing your Amazon resources in the *Amazon RAM User Guide*.

Supported accounts quota

If you enabled license sharing in Amazon License Manager before October 14, 2023, your quota for the maximum number of accounts License Manager supports within your organization will be less than the new default maximum. You can increase this quota by using API operations for Amazon RAM that are provided in the following section. For more information about the default quotas in License Manager, see Quotas for working with licenses in the *Amazon Web Services General Reference guide*.

Prerequisites

To complete the following procedure, you must sign in as a principal in the organization's management account that has the following permissions:

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

Increasing the supported accounts quota

The following procedure will increase your current quota for `Number of accounts per organization for License Manager` to the current default maximum.

To increase the supported accounts quota for License Manager

1. Use the describe-organization Amazon CLI command to determine your organization's ARN by using the operation:

```
aws organizations describe-organization

{
 "Organization": {
  "Id": "o-abcde12345",
  "Arn": "arn:aws:organizations::111122223333:organization/o-abcde12345",
  "FeatureSet": "ALL",
  "MasterAccountArn": "arn:aws:organizations::111122223333:account/o-
abcde12345/111122223333",
  "MasterAccountId": "111122223333",
  "MasterAccountEmail": "name+orgsidentifier@example.com",
  "AvailablePolicyTypes": [
    {
     "Type": "SERVICE_CONTROL_POLICY",
     "Status": "ENABLED"
    }
  ]
 }
}
```

2. Use the get-resource-shares Amazon CLI command to determine your organization's ARN by using the operation:

```
aws ram  get-resource-shares --resource-owner SELF --tag-filters
 tagKey=Service,tagValues=LicenseManager --region us-east-1

{
 "resourceShares": [
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "name": "licenseManagerResourceShare-111122223333",
    "owningAccountId": "111122223333",
    "allowExternalPrincipals": true,
    "status": "ACTIVE",
    "tags": [
     {
      "key": "Service",
```

```
      "value": "LicenseManager"
     }
    ],
    "creationTime": "2023-10-04T12:52:10.021000-07:00",
    "lastUpdatedTime": "2023-10-04T12:52:10.021000-07:00",
    "featureSet": "STANDARD"
  }
 ]
}
```

3. Use the enable-sharing-with-aws-organization Amazon CLI command to enable resource sharing with Amazon RAM:

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

{
 "returnValue": true
}
```

You can use the list-aws-service-access-for-organization Amazon CLI command to verify that Organizations lists service principals are enabled for License Manager and Amazon RAM:

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

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

> **Important**
>
> It can take up to six hours for Amazon RAM to finish this operation for your organization. This process must complete before you can proceed.

4. Use the associate-resource-share Amazon CLI command to associate your License Manager resources share with your organization:

```
aws ram associate-resource-share --resource-share-arn arn:aws:ram:us-
east-1:111122223333:resource-share/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --
principals arn:aws:organizations::111122223333:organization/o-abcde12345 --
region us-east-1

{
 "resourceShareAssociations": [
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "associatedEntity": "arn:aws:organizations::111122223333:organization/o-
abcde12345",
    "associationType": "PRINCIPAL",
    "status": "ASSOCIATING",
    "external": false
  }
 ]
}
```

You can use the get-resource-share-associations Amazon CLI command to validate that the resource share association's `status` is ASSOCIATED:

```
aws ram get-resource-share-associations --association-type "PRINCIPAL" --principal
 arn:aws:organizations::111122223333:organization/o-abcde12345--resource-share-
arns arn:aws:ram:us-east-1:111122223333:resource-share/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 --region us-east-1

{
 "resourceShareAssociations": [
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "resourceShareName": "licenseManagerResourceShare-111122223333",
```

```
    "associatedEntity": "arn:aws:organizations::111122223333:organization/o-
abcde12345",
    "associationType": "PRINCIPAL",
    "status": "ASSOCIATED",
    "creationTime": "2023-10-04T13:12:33.422000-07:00",
    "lastUpdatedTime": "2023-10-04T13:12:34.663000-07:00",
    "external": false
  }
 ]
}
```


Edit a self-managed license

You can edit values for the following fields in a self-managed license:

- Self-managed license name
- Description
- Number of <option>
- Enforce license type limit

To edit a self-managed license

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **self-managed licenses**.
3. Select the self-managed license.
4. Choose **Actions**, **Edit**.
5. Edit the details as needed and then choose **Update**.

To edit a self-managed license using the command line

- update-license-configuration (Amazon CLI)
- Update-LICMLicenseConfiguration (Amazon Tools for PowerShell)

Deactivate a self-managed license

When you deactivate a self-managed license, existing resources using the license are unaffected and AMIs using the license can still be launched. However, license consumption is no longer tracked.

When a self-managed license is deactivated, it must not be attached to any running instance. After deactivation, launches cannot be performed with the self-managed license.

To deactivate a self-managed license

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **self-managed licenses**.
3. Select the self-managed license.
4. Choose **Actions**, **Deactivate**. When prompted for confirmation, choose **Deactivate**.

To deactivate a self-managed license using the command line

- update-license-configuration (Amazon CLI)
- Update-LICMLicenseConfiguration (Amazon Tools for PowerShell)

Delete a self-managed license

Before you can delete a self-managed license, you must disassociate any resources. You can delete a self-managed license if you need to start over with new licensing rules. If the licensing terms from your software vendors change, you can disassociate existing resources, delete the self-managed license, create a new self-managed license to reflect the updated terms and associate it with the existing resources.

To delete a self-managed license using the console

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **Self-managed licenses**.
3. Choose the name of the self-managed license to open the license details page.
4. Select each resource (individually or in bulk) and choose **Disassociate resource**. Repeat until the list is empty.

5. Choose **Actions**, **Delete**. When prompted for confirmation, choose **Delete**.

To delete a self-managed license using the command line

- delete-license-configuration (Amazon CLI)
- Remove-LICMLicenseConfiguration (Amazon Tools for PowerShell)

License rules in License Manager

After self-managed license rules are in place, they can be attached to the relevant launch mechanisms, where they can directly prevent the deployment of new resources that are non-compliant. Users in your organization can seamlessly launch EC2 instances from designated AMIs, and administrators can track license inventory through the built-in License Manager dashboard. Launch controls and dashboard alerts allow easier compliance enforcement.

> **Important**
>
> Amazon does not participate in the audit process with software vendors. Customers are responsible for compliance and assume the responsibility of carefully understanding and capturing rules into License Manager based on their licensing agreements.

License tracking works from the time rules are attached to an instance until its termination. You define your usage limits and licensing rules, and License Manager tracks deployments while also alerting you to rule violations. If you have configured hard limits, License Manager can prevent resources from launching.

When a tracked server is stopped or terminated, its license is released and returned to the pool of available licenses.

Because organizations have differing approaches to operations and compliance, License Manager supports multiple launch mechanisms:

- **Manual association of self-managed licenses with AMIs** – For tracking licenses for operating system or other software, you can attach licensing rules to AMIs before publishing them for broader use in your organization. Any deployments from these AMIs are then automatically tracked with License Manager without requiring any additional actions by users. You can also

attach licensing rules to your current AMI building mechanisms such as Systems Manager Automation, VM Import/Export, and Packer.

- **Amazon EC2 launch templates and Amazon CloudFormation** – If attaching licensing rules to AMIs is not a preferred option, you can specify them as optional parameters in EC2 launch templates or Amazon CloudFormation templates. Deployments using these templates are tracked using License Manager. You can enforce rules on EC2 launch templates or Amazon CloudFormation templates by specifying one or more self-managed license IDs in the **self-managed licenses** field.

Amazon treats license-tracking data as sensitive customer data accessible only through the Amazon account that owns it. Amazon does not have access to your license-tracking data. You control your license-tracking data and you can delete it at any time.

Associating self-managed licenses and AMIs

The following procedure demonstrates how to associate self-managed licenses with AMIs using the License Manager console. The procedure assumes that you have at least one existing self-managed license. You can associate self-managed licenses with any AMI that you have access to, whether owned or shared. If an AMI was shared with you, you can associate it with the self-managed license in the current account. Otherwise, you can specify whether the AMI is associated with the self-managed license across all accounts or only in the current account.

If you associate an AMI with a self-managed license across all accounts, you can track instance launches from the AMI across accounts. When a hard limit is reached, License Manager blocks additional instance launches. When a soft limit is reached, License Manager notifies you of additional instance launches.

If you copy an AMI within the same Region, and that AMI has associated license configurations, those license configurations are automatically associated with the new AMI. When you launch an instance from the new AMI, License Manager tracks it. Similarly, if you create a new AMI from a running instance that has associated license configurations, those license configurations are automatically associated with the new AMI, and License Manager tracks the instances that you launch from the new AMI.

> **Warning**
>
> License Manager does not support cross-Region instance tracking. If you copy an AMI that has associated license configurations to a different Region, License Manager blocks all instance launches from the new AMI.

To associate a self-managed license and an AMI

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **Self-managed licenses**.
3. Choose the name of the self-managed license to open the license details page. To view the currently associated AMIs, choose **Associated AMIs**.
4. Choose **Associate AMI**.
5. For **Available AMIs**, select one or more AMIs and choose **Associate**.
   - If your account owns at least one of the AMIs, you are prompted to choose an AMI association scope for the AMIs that you own. Any AMIs that were shared with from another account are associated with only your account. Choose **Confirm**.
   - If the AMIs were shared with you from another account, they are associated with only your account.

   The newly associated AMIs now appear on the **Associated AMIs** tab on the license details page.

Disassociating self-managed licenses and AMIs

The following procedure demonstrates how to disassociate self-managed licenses from AMIs using the License Manager console. You cannot disassociate a deregistered AMI. License Manager checks for deregistered AMIs every 8 hours and automatically disassociates them.

To disassociate a self-managed license and an AMI

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **Self-managed licenses**.
3. Choose the name of the self-managed license to open the license details page.
4. Choose **Associated AMIs**.

5. Select the AMI and choose **Disassociate AMI**.

Usage reports in License Manager

Using Amazon License Manager you can track the history of your self-managed licenses by scheduling periodic snap shots of your license usage. By setting up usage reports License Manager will automatically upload reports of your self-managed licenses to an S3 bucket based on your specifications. Usage reports were formerly called report generators. You can set up multiple usage reports to effectively track configurations of different license types in your environment.

> **Note**
>
> Amazon License Manager does not store your reports. License Manager reports are published directly to your S3 bucket. Once you delete a usage report, reports are no longer published to your S3 bucket.

Creating a usage report

When you create a usage report you specify a self-managed license type for License Manager to track, a frequency interval that defines how often to generate reports, and a report type. All reports are generated in CSV format and published to an S3 bucket. A usage report can produce one or more of following report types.

Self-managed license summary report

This report type contains information on the number of consumed licenses and details about self-managed license. The tracked self-managed license type is listed with details such as the license count, license rules, and the distribution of licenses across different resource types.

Resource usage report

This report type gives you details about your tracked resources and their license consumption. Each tracked resource using the specified self-managed license type is listed with details such as the license ID, the status of the resource, and the Amazon account ID that owns the resource.

To create a usage report

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.

2. From the navigation panel choose **Usage reports**.
3. Choose **Create usage report**, then from the **Create usage report** pane define the parameters for the report:

   a. Enter a **Name** and optional **Description** for your usage report.

   b. Select a self-managed license type from the drop down list. This is the type of license that the usage report will be generating data on.

   c. Choose the report types to generate.

   d. Choose the frequency by which License Manager will publish the reports, you can choose **Once every 24 hours**, **Once every 7 days** or **Once every 30 days**.

   e. (Optional) Add **Tags** to track the usage report resource.
4. Select **Create usage report**.

A new usage report will begin publishing reports within 60 minutes or less.

If you do not already have an S3 bucket associated with your account, License Manager will create a new Amazon S3 bucket in your account when you create a usage report. If you have previously enabled **Cross-account inventory search** reports will be sent to the S3 bucket created by License Manager when **Cross-account inventory search** was enabled.

Reports are stored in your bucket with the following Amazon S3 URI pattern:

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

Editing your usage reports

You can view and make changes to your usage reports from the License Manager console at any time. The **usage reports** table lists all the usage reports created for your account, from the table you can get an overview of your different reports, pivot to the Amazon S3 bucket associated with your usage reports, and view the status of report generation.

To edit a usage report

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. From the navigation panel choose **Usage reports**.
3. Choose the usage report you want to edit from the table, then select **View details**.

4. Select **Edit** to make changes to the usage report.
5. Make the desired changes to your usage report then choose **Save changes**.

An updated usage report will generate a new report within an hour.

> **Note**
>
> Changing the name of your usage report will send future reports to a new folder in your License Manager S3 bucket reflecting the new name.

Deleting a usage report

Deleting a usage report stops the generation of new reports, however, your Amazon S3 bucket and all your previous reports are not affected.

> **Note**
>
> You will be unable to delete a self-managed license from your account if it has a usage report associated. You must first delete that usage report.

To edit a usage report

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. From the navigation panel choose **Usage reports**.
3. Choose the usage report you want to edit from the table, then select **View details**.
4. Select **Delete**. This action permanently deletes the usage report.

License type conversions in License Manager

With License Manager, you can change your license type between Amazon provided licensing and Bring Your Own License model (BYOL), or Bring your Own Subscription model (BYOS), as your business needs change. You can change your license type without redeploying your existing workloads.

You can optimize your license inventory for the following scenarios using license type conversion:

Migrate on-premises workloads to Amazon EC2

During your migration, you can deploy your workload to Amazon Elastic Compute Cloud (Amazon EC2) and use Amazon provided licenses. When the migration is complete, use License Manager license type conversion to change the license type of your instances. You can change to BYOL or BYOS so that you can use the licenses that were released during the migration.

Continue running workloads with expiring license agreements

You can use License Manager license type conversion to switch from BYOL or BYOS to Amazon provided licenses. This switch allows you to continue running your workloads with fully-compliant software licenses provided by Amazon with a flexible pay-as-you go licensing model. You might choose to do this if your license agreement with the operating system's software vendor, such as Microsoft or Canonical, is about to expire and you do not plan to renew it.

Optimize costs

For small or irregular workloads, Amazon provided licenses (license included) instances might be more cost effective. When you choose to use BYOL or BYOS, these options might require a longer term commitment. For this case, you can use License Manager license type conversion to switch your instances to license included to optimize licensing related costs. If your instances were launched from your own virtual machine (VM) image, you can switch back to BYOL or BYOS. You might choose to do this when the workload is more steady or predictable.

Extended maintenance

If your Ubuntu operating system has reached the end of standard support, you can add a paid subscription of Ubuntu Pro. Adding a subscription to Ubuntu pro provides security updates for an extended period of time. For more information, see Ubuntu Pro in the Canonical documentation.

Topics

Eligible license types for license type conversion

You can use License Manager license type conversion with supported versions and combinations of Windows Server and Microsoft SQL Server licenses. You can also use license type conversion with Ubuntu Linux subscriptions.

Contents

Eligible license types for Windows and SQL Server

> **Important**
>
> Instances that were originally launched from an Amazon provided Amazon Machine Image (AMI) are not eligible for license type conversion to BYOL.

Windows and SQL Server must meet certain requirements in order to be eligible for license type conversion.

Topics

SQL Server editions

License Manager supports the following SQL Server editions:

- SQL Server Standard edition
- SQL Server Enterprise edition
- SQL Server Web edition

SQL Server versions

License Manager supports the following SQL Server versions:

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

Usage operation values

A license type conversion changes the usage operation value associated with your instance. Usage operation values for each supported operating system are provided in the following table. For more information, see AMI billing information fields.

Operating system details	Usage operation
Windows Server as BYOL	RunInstances:0800
Windows Server as BYOL SQL Server (any edition) as BYOL	RunInstances:0800
Windows Server as license included	RunInstances:0002

Operating system details	Usage operation
Windows Server as license included SQL Server (any edition) as BYOL	RunInstances:0002
Windows Server as license included SQL Server Web as license included	RunInstances:0202
Windows Server as license included SQL Server Standard as license included	RunInstances:0006
Windows Server as license included SQL Server Enterprise as license included	RunInstances:0102

Media compatibility

The following table confirms which media can be used on which instance licensing models.

Source	Target	
	BYOL	License included
Amazon provided Windows Server image	No	Yes
Amazon provided SQL Server image	No	Yes
Your Windows Server media[1]	Yes	Yes
Your SQL Server media[2]	Yes	Yes

[1] Denotes that the instance was originally launched from your own imported virtual machine (VM). You can import your VM using a service such as VM Import/Export or Amazon Application Migration Service.

[2] Denotes that you have sourced your own SQL Server installation media (.iso, .exe).

Conversion paths

The following table confirms if the source license model can be converted to another between BYOL and license included. For more information, see Convert a license type.

> **Important**
>
> - Windows Server as BYOL with SQL Server as license included is an unsupported configuration.
> - Conversions that are specified as "Not needed" won't change the usage operation value.

Source	Target					
	Windows Server as BYOL	Windows Server as license included	Windows Server as BYOL SQL Server as BYOL	Windows Server as license included SQL Server as BYOL	Windows Server as BYOL SQL Server as license included	Windows Server as license included SQL Server as license included
Windows Server as BYOL (your media)	Not needed	Yes	Not needed	Yes[1]	Unsupported	Yes[1]
Windows Server as license included (your media)	Yes[2]	Not needed	Yes[1,2]	Not needed[3]	Unsupported	Yes[1]

Source	Target					
Windows Server as license included (Amazon provided image)	No✗	Not needed	No✗	Not needed[3]	Unsupported	Yes[1]
Windows Server as BYOL (your media) SQL Server as BYOL (your media)	Not needed[4]	Yes	Not needed	Yes	Unsupported	Yes
Windows Server as license included (your media) SQL Server as BYOL (your media)	Yes[2]	Not needed[4]	Yes[2]	Not needed	Unsupported	Yes

Source	Target					
Windows Server as license included (Amazon provided image) SQL Server as BYOL (your media)	No✗	Not needed[4]	No✗	Not needed	Unsupported	Yes
Windows Server as BYOL (your media) SQL Server as license included	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported

Source	Target					
Windows Server as license included (Amazon provided image or your media)	No✗	No✗	No✗	No✗	Unsupported	Not needed
SQL Server as license included (Amazon provided image)						
Windows Server as license included (your media)	Yes[2,5,6]	Yes[5]	Yes[2]	Yes	Unsupported	Not needed
SQL Server as license included (your media)						

Source	Target					
Windows Server as license included (Amazon provided image)	No✗	Yes[5]	No✗	Yes	Unsupported	Not needed
SQL Server as license included (your media)						

✗ You must deploy a new instance with an alternate configuration, as converting to the target license type(s) is not supported. For more information, see Media compatibility.

For other conversion scenarios, you might need to take the following steps to perform a license conversion:

[1] You must first **install** SQL Server before converting to BYOL for SQL Server.

[2] You must first modify your Windows configuration to use your own KMS server for license activation. For more information, see Convert Windows Server from license included to BYOL.

[3] You must first **install** SQL Server when you convert from a source without SQL Server to a target with SQL Server (regardless of the SQL Server license type).

[4] You must first **uninstall** SQL Server when you convert from a source with SQL Server to a target without SQL Server (regardless of the SQL Server license type).

[5] You must first **uninstall** SQL Server before converting to license-included SQL Server.

[6] You must first perform the steps for [2] and [5]. Once these steps are complete, you must convert the license type to Windows Server as license included, and then convert the license type once more to Windows Server as BYOL.

Eligible subscription types for Linux

License type conversion is available for supported versions of Ubuntu. The supported versions include updates such as Ubuntu 18.04.1 LTS. When you convert a subscription to Ubuntu Pro, security updates are provided for an additional five years. For more information, see Ubuntu Pro in the Canonical documentation.

You can use license type conversion with the following Ubuntu versions:

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

Operating system details	Usage operation
Linux/Unix	RunInstances
Ubuntu Pro	RunInstances:0g00

Conversion paths for Linux

You can convert any supported version of Ubuntu LTS to Ubuntu Pro. If you need to convert from Ubuntu Pro to Ubuntu LTS, you will need to raise a request to Amazon Web Services Support. For more information, see Creating a support case.

Conversion prerequisites

To convert license types with License Manager, there are general and operating system specific prerequisites.

Topics

- General
- Windows
- Linux

General

You must meet the following general prerequisites before performing a license type conversion:

- Your Amazon Web Services account must be onboarded to License Manager. See Getting started with Amazon License Manager.
- The target instance must be in the stopped state before you convert the license type. For more information, see Stop and start your instance in the *Amazon EC2 User Guide*.
- If stop protection is enabled on the target instance, the conversion process will fail. For more information, see Troubleshooting license type conversion.
- The target instance must be configured with Amazon Systems Manager Inventory. For more information, see Setting up Systems Manager for EC2 instances and Amazon Systems Manager Inventory in the *Amazon Systems Manager User Guide*.
- Your user or role must have the following permissions:
  - `ssm:GetInventory`
  - `ssm:StartAutomationExecution`
  - `ssm:GetAutomationExecution`
  - `ssm:SendCommand`
  - `ssm:GetCommandInvocation`
  - `ssm:DescribeInstanceInformation`
  - `ec2:DescribeImages`
  - `ec2:DescribeInstances`
  - `ec2:StartInstances`
  - `ec2:StopInstances`
  - `license-manager:CreateLicenseConversionTaskForResource`
  - `license-manager:GetLicenseConversionTask`
  - `license-manager:ListLicenseConversionTasks`
  - `license-manager:GetLicenseConfiguration`
  - `license-manager:ListUsageForLicenseConfiguration`
  - `license-manager:ListLicenseSpecificationsForResource`
  - `license-manager:ListAssociationsForLicenseConfiguration`
  - `license-manager:ListLicenseConfigurations`

For more information about Systems Manager Inventory, see Amazon Systems Manager Inventory.

Windows

Windows instances must meet the following prerequisites:

- Instances that were originally launched from an Amazon provided Amazon Machine Image (AMI) are not eligible for license type conversion to BYOL. The original Amazon EC2 instance must be launched from your own virtual machine (VM) image. For more information about converting a VM to Amazon EC2, see VM Import/Export.
- To change your SQL Server license to BYOL, SQL Server must have been installed using your own media.

Linux

Linux instances must meet the following prerequisites:

- Instances must be running Ubuntu LTS.
- The Ubuntu Pro Client must be installed in your Ubuntu operating system.
  - Run the following command to confirm if the Ubuntu Pro Client is installed:

    ```
    pro --version
    ```

  - If the command is not found, or the version needs to be updated, run the following command to install the Ubuntu Pro Client:

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

- Instances must be able to reach multiple endpoints to activate their Ubuntu Pro subscription and receive updates. You must allow outbound traffic from your instance over TCP port 443 to reach the following endpoints:
  - **contracts.canonical.com** – Used for Ubuntu Pro activation.
  - **esm.ubuntu.com** – Used for APT repository access for most services.
  - **api.snapcraft.io** – Used for installing and running snaps.
  - **dashboard.snapcraft.io** – Used for installing and running snaps.

- **login.ubuntu.com** – Used for installing and running snaps.
- **cloudfront.cdn.snapcraftcontent.com** – Used for downloading from content development networks (CDNs).
- **livepatch.canonical.com** – Used for downloading patches from the Livepatch server.

For more information, see Ubuntu Pro Client network requirements in the Ubuntu Pro Client documentation and Network requirements in the Canonical Snapcraft documentation.

Convert a license type

You can convert Windows licenses, Microsoft SQL Server licenses, and Ubuntu Linux subscriptions using the License Manager console or Amazon CLI. You might need to complete additional steps to convert the license or subscription in the operating system of the instance.

You can convert license types using the License Manager console or the Amazon CLI. When you create a license type conversion, License Manager validates the billing products on your instance. If these preliminary validations are successful, License Manager creates a license type conversion. You can check the status of a license type conversion by using the `list-license-conversion-tasks` and `get-license-conversion-task` Amazon CLI commands.

License Manager might update the resources associated with your self-managed licenses as part of a license type conversion. Specifically, for any self-managed license with automated discovery rules of type `License Included`, License Manager disassociates the resource in the license type conversion from the license if the `license included` automated discovery rule explicitly excludes the resource.

For example, if your self-managed license contains two automated discovery rules, and each rule excludes license-included Windows Server, then a license type conversion from BYOL to license included Windows Server results in disassociation of the instance from the self-managed license. However, if only one of the two automated discovery rules contains a `License Included` rule, then the instance is not disassociated.

You should not start or stop your instance while a license type conversion is in progress. When the license type conversion succeeds, its status changes from `IN_PROGRESS` to `SUCCEEDED`. If License Manager encounters issues during the workflow, it updates the status of the license type conversion to `FAILED`, and updates the status message with an error message.

> **Note**
>
> The billing product information on the AMI used to launch an instance does not change when you convert the license type. To retrieve accurate billing information, use the Amazon EC2 `DescribeInstances` API. Additionally, if you have existing workflows that search for billing information from AMIs, update those workflows to use `DescribeInstances`.

Contents

Convert a license type for Windows and SQL Server

You can use either the License Manager Console or the Amazon CLI to convert the license type of eligible Windows and SQL Server instances.

Topics

License type conversion limits

> **Important**
>
> The use of Microsoft software is subject to the licensing terms of Microsoft. You are responsible for complying with Microsoft licensing terms. This documentation is provided

for convenience, and you are not entitled to rely on its description. This documentation does not constitute legal advice. If you have questions about your licensing rights to Microsoft software, consult with your legal team, Microsoft, or your Microsoft reseller.

License Manager restricts the types of license conversions that you can create in accordance with the Microsoft Service Provider License Agreement (SPLA). Some of the restrictions that license type conversion is subject to are listed as follows. This is not a comprehensive list and is subject to change.

- The Amazon EC2 instance must be launched from your own virtual machine (VM) image.
- License-included SQL Server cannot be run on a Dedicated Host.
- A license-included SQL Server instance must have at least 4 vCPUs.

Convert a license type using the License Manager console

You can use the License Manager console to convert a license type.

Note

Only instances that are in a stopped state and have been associated by Amazon Systems Manager Inventory are displayed.

To start a license type conversion in the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/ .
2. From the left navigation pane, choose **License type conversion**, then choose **Create license type conversion**.
3. For **Source operating system**, choose the platform of the instance you want to convert:
    1. **Ubuntu LTS**
    2. **Windows BYOL**
    3. **Windows license included**
4. (Optional) Filter the available instances by specifying a value for **Instance ID** or **Usage operation value**.

5. Select the instances whose licenses you want to convert, and then choose **Next**.
6. Enter the **Usage operation value** for the license type, select the license that you are converting to, and choose **Next**.
7. Verify that you are satisfied with your license type conversion configuration and choose **Start conversion**.

You can view the status of your license type conversion from the license type conversion panel. The Conversion status column displays the status of the conversion as **In progress**, **Completed**, or **Failed**.

> **Important**
>
> If you convert Windows Server from license included to BYOL, you must activate Windows according to your Microsoft license agreement. See Convert Windows Server from license included to BYOL for more information.

Convert a license type using the Amazon CLI

To start a license type conversion in the Amazon CLI:

Determine the license type of your instance

1. Verify that you have installed and set up the Amazon CLI. For more information, see Installing, updating, and uninstalling the Amazon CLI and Configuring the Amazon CLI.

   > **Important**
   >
   > You might need to update the Amazon CLI to run certain commands and receive all required output in the following steps.

2. Verify that you have permissions to run the `create-license-conversion-task-for-resource` Amazon CLI command. For help with this, see Create IAM policies for License Manager.
3. To determine the license type currently associated with your instance, run the following Amazon CLI command. Replace the instance ID with the ID of the instance for which you want to determine the license type.

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

4. The following is an example response to the `describe-instances` command. Note that the `UsageOperation` value is the billing information code associated with the license. The `UsageOperationUpdateTime` is the time when the billing code was updated. For more information, see DescribeInstances in the *Amazon EC2 API reference*.

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

Note

The usage operation for Windows Server with SQL Server Enterprise BYOL is the same as the usage operation for Windows BYOL because they are identically billed.

Convert Windows Server from license included to BYOL

When you convert Windows Server from license included to BYOL, License Manager does not automatically activate Windows. You must switch the KMS server for your instance from the Amazon KMS server to your own KMS server.

Important

In order to convert from license included to BYOL, the original Amazon EC2 instance must be launched from your own virtual machine (VM) image. For more information about converting a VM to Amazon EC2, see VM Import/Export. Instances that were originally launched from an Amazon Machine Image (AMI) are not eligible for license conversion to BYOL.

Check your Microsoft license agreement to determine what methods you can use to activate Microsoft Windows Server. For example, if you are using a KMS server, you must obtain the address of your KMS server from the original BYOL configuration of the instance.

1. To convert the license type of your instance, run the following command, replacing the ARN with the ARN of the instance you want to convert:

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

2. To activate Windows after you convert your license, you must point the Windows Server KMS server for your operating system to your own KMS servers. Log in to the Windows instance and run the following command:

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

Convert Windows Server from BYOL to license included

When you convert Windows Server from BYOL to license included, License Manager automatically switches the KMS server for your instance to the Amazon KMS server.

To convert the license type of your instance from BYOL to license included, run the following command, replacing the ARN with the ARN of the instance you want to convert:

```
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
```

Convert both Windows Server and SQL Server from BYOL to license included

You can switch multiple products at the same time. For example, you can convert both Windows Server and SQL Server in one license type conversion.

To convert the license type of your Windows Server instance from BYOL to license included, and SQL Server Standard from BYOL to license included, run the following command, replacing the ARN with the ARN of the instance you want to convert:

```
aws license-manager create-license-conversion-task-for-resource \
    --resource-arn <instance_arn> \
    --source-license-context UsageOperation=RunInstances:0800 \
    --destination-license-context UsageOperation=RunInstances:0006
```

Convert a license type for Linux

You can use either the License Manager Console or the Amazon CLI to convert the license type of eligible Ubuntu LTS instances.

Topics

License type conversion considerations

Some of the considerations that license type conversion is subject to are listed as follows. This is not a comprehensive list and is subject to change.

- The instance must be running Ubuntu LTS in order to convert the license type to Ubuntu Pro.
- You can't use license type conversion for a Ubuntu Pro subscription. To remove a Ubuntu Pro subscription, see Remove a Ubuntu Pro subscription.
- Ubuntu Pro is not available as a Reserved Instance. For savings with On-Demand Instance pricing, we recommend that you use Ubuntu Pro with Savings Plans. For more information, see Reserved Instances in the *Amazon EC2 User Guide for Linux Instances* and What are Savings Plans? in the *Savings Plans User Guide*.

Convert a license type using the License Manager console

You can use the License Manager console to convert a license type.

> **Note**
>
> Only instances that are in a stopped state and have been associated by Amazon Systems Manager Inventory are displayed.

To start a license type conversion in the console

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/ .
2. From the left navigation pane, choose **License type conversion**, then choose **Create license type conversion**.
3. For **Source operating system**, choose the platform of the instance you want to convert:
    1. **Ubuntu LTS**
    2. **Windows BYOL**
    3. **Windows license included**
4. (Optional) Filter the available instances by specifying a value for **Instance ID** or **Usage operation value**.
5. Select the instances whose licenses you want to convert, and then choose **Next**.
6. Enter the **Usage operation value** for the license type, select the license that you are converting to, and choose **Next**.
7. Verify that you are satisfied with your license type conversion configuration and choose **Start conversion**.

You can view the status of your license type conversion from the license type conversion panel. The Conversion status column displays the status of the conversion as **In progress**, **Completed**, or **Failed**.

Convert a license type using the Amazon CLI

To start a license type conversion in the Amazon CLI, you should confirm the license type of your instance is eligible, and then perform a license type conversion to change to the required subscription. For more information on eligible subscription types, see Eligible subscription types for Linux.

Determine the license type of your instance

Verify that you have installed and set up the Amazon CLI. For more information, see Installing, updating, and uninstalling the Amazon CLI and Configuring the Amazon CLI.

> **Important**
>
> You might need to update the Amazon CLI to run certain commands and receive all required output in the following steps. Verify that you have permissions to run the

`create-license-conversion-task-for-resource` Amazon CLI command. For more information, see Create IAM policies for License Manager.

To determine the license type currently associated with your instance, run the following Amazon CLI command. Replace the instance ID with the ID of the instance for which you want to determine the license type:

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

The following is an example response to the `describe-instances` command. The **UsageOperation** value is the billing information code associated with the license. A usage operation value of `RunInstances` indicates that the instance is using Amazon provided licensing. The `UsageOperationUpdateTime` is the time when the billing code was updated. For more information, see DescribeInstances in the *Amazon EC2 API Reference*.

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

Convert to Ubuntu Pro

When you convert your instance from Ubuntu LTS to Ubuntu Pro, you must have outbound internet access from the instance to retrieve a license token from the Canonical servers and have the Ubuntu Pro Client installed. For more information, see Conversion prerequisites.

To convert Ubuntu LTS to Ubuntu Pro:

1. Run the following command from the Amazon CLI while specifying your instance's ARN:

```
aws license-manager create-license-conversion-task-for-resource \
    --resource-arn <instance_arn> \
    --source-license-context UsageOperation=RunInstances \
    --destination-license-context UsageOperation=RunInstances:0g00
```

2. Run the following command from within the instance to retrieve details about your Ubuntu Pro subscription status:

```
pro status
```

3. Confirm your output indicates that the instance has a valid Ubuntu Pro subscription:

```
ubuntu@ip-                    pro status
SERVICE                       STATUS    DESCRIPTION
cc-eal           yes          disabled  Common Criteria EAL2 Provisioning Packages
cis              yes          disabled  Security compliance and audit tools
esm-apps         yes          disabled  Expanded Security Maintenance for Applications
esm-infra        yes          enabled   Expanded Security Maintenance for Infrastructure
fips             yes          disabled  NIST-certified core packages
fips-updates     yes          disabled  NIST-certified core packages with priority security updates
livepatch        yes          enabled   Canonical Livepatch service

Enable services with: pro enable <service>

               Account:
          Subscription:
           Valid until: Fri Dec 31 00:00:00 9999 UTC
Technical support level: essential
```

Remove a Ubuntu Pro subscription

License type conversion can only be used to convert from Ubuntu LTS to Ubuntu Pro. If you need to convert from Ubuntu Pro to Ubuntu LTS, you will need to raise a request to Amazon Web Services Support. For more information, see Creating a support case.

Tenancy conversion

You can change the tenancy of your instance to best suit your use case. You can use the modify-instance-placement Amazon CLI command to switch among the following tenancies:

- Shared
- Dedicated Instance
- Dedicated Host
- Host resource groups

Your account must have a Dedicated Host with available capacity to start the instance in order to switch to the Dedicated Host tenancy type. For more information about working with dedicated hosts, see Work with Dedicated Hosts in the *Amazon Elastic Compute Cloud User Guide*.

To move to the host resource groups tenancy type, you must have at least one host resource group in your account. In order to launch an instance into a host resource group, the instance must have the same set of licenses that are associated with the host resource group. For more information, see Host resource groups in Amazon License Manager.

Tenancy conversion limits

The following limits apply to tenancy conversion:

- The Linux billing code is permitted on all tenancy types.
- The Windows BYOL billing code is not permitted on Shared tenancy.
- The Windows Server license included billing code is permitted on all tenancy types.
- All supported SQL Server editions, Red Hat (RHEL), and SUSE (SLES) license included billing codes are permitted on Shared tenancy and Dedicated Instances. However, these billing codes are not permitted on Dedicated Hosts and host resource groups.
- License included billing codes other than Windows Server are not permitted on Dedicated Hosts and host resource groups.

Change the tenancy of an instance using the Amazon CLI

An instance must be in the `stopped` state in order to change its tenancy.

To stop the instance, run the following command:

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

To change an instance from any tenancy to `default` or `dedicated` tenancy, run the following commands:

`default`

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

`dedicated`

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

To change an instance from any tenancy to `host` tenancy with auto-placement, run the following command:

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

To change an instance from any tenancy to `host` tenancy, targeting a specific Dedicated Host, run the following command:

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

To change an instance from any tenancy to `host` tenancy using a Host Resource Group, run the following command:

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

Troubleshooting license type conversion

Troubleshooting topics

- Windows activation
- Instance [instance] is launched from an Amazon owned AMI. Provide an instance launched originally from a BYOL AMI.
- Failed to validate that instance [instance] was launched from a BYOL AMI. Ensure that the SSM Agent is running on your instance.
- An error occurred (InvalidParameterValueException) when calling the CreateLicenseConversionTaskForResource operation: ResourceId - [instance] is in an invalid state for changing license type.
- EC2 instance [instance] failed to stop. Ensure that you have permissions for EC2 StopInstances.

Windows activation

A license type conversion contains multiple steps. In some cases, when you convert Windows Server instances from BYOL to license included, the billing products on an instance are successfully updated. However, the KMS server might not switch to the Amazon KMS server.

To remediate this issue, follow the steps in Why did Windows activation fail on my EC2 Windows instance? to activate Windows either with the Systems Manager AWSSupport-ActivateWindowsWithAmazonLicense Automation runbook, or log in to the instance and manually make the switch to the Amazon KMS server.

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

You must launch your Amazon EC2 Windows instance from an AMI that you have imported to perform a license type conversion to Bring Your Own License model (BYOL). Instances originally launched from an Amazon-owned AMI aren't eligible for license type conversion to BYOL. For more information, see Conversion prerequisites.

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

In order for the license type conversion to succeed, your instance must first have been online and managed by Systems Manager to have its inventory collected. The Amazon Systems Manager Agent (SSM Agent) will gather inventory from your instance, which includes details about the operating system. For more information, see Checking SSM Agent status and starting the agent and Troubleshooting SSM Agent in the *Amazon Systems Manager User Guide*.

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

To perform a license type conversion, the target instance must be in the stopped state. For more information, see Conversion prerequisites and Troubleshoot stopping your instance in the *Amazon Elastic Compute Cloud User Guide*.

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

You must have permissions to perform the `StopInstances` EC2 API action on the target instance. Also, If stop protection is enabled on the target instance, the conversion process will fail. For more information, see Disable stop protection for a running or stopped instance in the *Amazon Elastic Compute Cloud User Guide*.

Host resource groups in Amazon License Manager

Amazon EC2 Dedicated Hosts are physical servers with EC2 instance capacity fully dedicated to your use. A host resource group is a collection of Dedicated Hosts that you can manage as a single entity. As you launch instances, License Manager allocates the hosts and launches instances on them based on the settings that you configured. You can add existing Dedicated Hosts to a host resource group and take advantage of automated host management through License Manager. For more information, see Dedicated Hosts in the *Amazon EC2 User Guide*.

You can use host resource groups to separate hosts by purpose, for example, development test hosts versus production, organizational unit, or license constraint. After you add a Dedicated Host to a host resource group, you cannot launch instances directly on the Dedicated Host, you must launch them using the host resource group.

Settings

You can configure the following settings for a host resource group:

- **Allocate hosts automatically** – Indicates whether Amazon EC2 can allocate new hosts on your behalf if launching an instance in this host resource group would exceed its available capacity.
- **Release hosts automatically** – Indicates whether Amazon EC2 can release unused hosts on your behalf. An unused host has no running instances.
- **Recover hosts automatically** – Indicates whether Amazon EC2 can move instances from a host that has failed unexpectedly to a new host.
- **Associated self-managed licenses** – The self-managed licenses that can be used to launch instances in this host resource group.
- **(Optional) Instance families** – The types of instances that you can launch. By default, you can launch any instance types that are supported on a Dedicated Host. If you launch Nitro-based instances, then you can launch instances with different instance types in the same host resource group. Otherwise, you must launch only instances with the same instance type in the same host resource group.

Contents

- Launch an instance in a host resource group
- Modify a host resource group
- Removing Dedicated Hosts from a host resource group
- Delete a host resource group

Create a host resource group

Configure a host resource group to enable License Manager to manage your Dedicated Hosts. To best utilize your most expensive licenses, you can associate one or more core- or socket-based self-managed licenses with your host resource group. To best optimize host utilization, you can allow all core- or socket-based self-managed licenses with your host resource group.

To create a host resource group

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **Host resource groups**.
3. Choose **Create host resource group**.
4. For **Host resource group details**, specify a name and description for the host resource group.
5. For **EC2 Dedicated Host management settings**, enable or disable the following settings as needed:
   - **Allocate hosts automatically**
   - **Release hosts automatically**
   - **Recover hosts automatically**
6. (Optional) For **Additional settings**, select the instance families that you can launch in the host resource group.
7. For **self-managed licenses**, select one or more core- or socket-based self-managed licenses.
8. (Optional) For **Tags**, add one or more tags.
9. Choose **Create**.

Share a host resource group

You can use Amazon Resource Access Manager to shared your host resource groups through Amazon Organizations. After you share a host resource group and self-managed license, member

accounts can launch instances into the shared host resource group. The new hosts are allocated in the account that owns the host resource group. The member account owns the instances. For more information, see the Amazon RAM User Guide.

Adding Dedicated Hosts to a host resource group

You can add your existing hosts to a host resource group from the Amazon Web Services Management Console, Amazon CLI, or Amazon API. To add your hosts, you must be the Amazon account owner where you created the Dedicated Host and host resource groups. If your host resource group lists allowed self-managed licenses and instances types, the host you add must match these requirements.

> **Note**
>
> Suppose you stop the instances and want to restart them. You must perform the following two tasks:
>
> - Modify the instance to point to the host resource group.
> - Associate self-managed licenses to match the host resource group.

For more information about Resource Groups, see Amazon Resource Groups User Guide.

Use the following steps to add one or more Dedicated Hosts to a resource group:

1. Log into the License Manager console at https://console.amazonaws.cn/license-manager/.
2. Choose **Host resource groups**.
3. From the list of host resource group names, click on the name of the host resource group where you want to add the Dedicated Host.
4. Choose **Dedicated Hosts**.
5. Choose **Add**.
6. Choose one or more Dedicated Hosts to add to the host resource group.
7. Choose **Add**.

   Adding the host may take 1 - 2 minutes, and then it appears in the list of **Dedicated Hosts.**

Launch an instance in a host resource group

When you launch an instance, you can specify a host resource group. For example, you can use the following run-instances command. You must associate a core- or socket-based self-managed license with the AMI.

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

You can also use the Amazon EC2 console. For more information, see Launching Instances into a host resource group in the *Amazon EC2 User Guide*.

Modify a host resource group

You can modify the settings for a host resource group at any time. You cannot set the host limit lower than the number of existing hosts in the host resource group. You cannot remove an instance type if there's an instance of that type running in the host resource group.

To modify a host resource group

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **Host resource groups**.
3. Select the host resource group and choose **Actions**, **Edit**.
4. Modify the settings as needed.
5. Choose **Save changes**.

Removing Dedicated Hosts from a host resource group

When you remove a host from the host resource group, the instance running on the host remains on the host. The instances attached to the host resource group remain associated with the group, and instances directly attached to the host through affinity maintain the same property. If you share the host resource group with other Amazon accounts, License Manager automatically removes the shared host and consumers receive an eviction notice to move their instances from the host in 15 days. To work with a Dedicated Host that has been removed from a host resource group, see Work with Dedicated Hosts in the *Amazon EC2 User Guide*.

Use the following steps to remove a Dedicated Host to a host resource group:

1. Log into the License Manager console at https://console.amazonaws.cn/license-manager/.
2. Choose **Host resource groups**.
3. Click on the name of the host resource that you want to remove a Dedicated Host.
4. Choose **Dedicated Hosts**.
5. Choose the Dedicated Host to delete from the host resource group. Or, you can search for a Dedicated Host by host ID, host type, host state, or availability zone.
6. Choose **Remove**.
7. Choose **Remove** again to confirm.

Delete a host resource group

You can delete a host resource group if it has no hosts.

To delete a host resource group

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **Host resource groups**.
3. Select the host resource group and choose **Actions**, **Delete**.
4. When prompted for confirmation, choose **Delete**.

Inventory search in License Manager

License Manager allows you to discover on-premises applications using Systems Manager inventory, and then to attach licensing rules to them. After licensing rules are attached to these servers, you can track them along with your Amazon servers in the License Manager dashboard.

License Manager cannot, however, validate licensing rules for these servers at launch or termination time. To keep information about non-Amazon servers up-to-date, you must periodically refresh the inventory information using the **Inventory search** section of the License Manager console.

Systems Manager stores data in its Inventory data for 30 days. During this period, License Manager counts a managed instance as active even if it is not pingable. After inventory data has been

purged from Systems Manager, License Manager marks the instance as inactive and updates local inventory data. To keep managed instance counts accurate, we recommend manually deregistering instances in Systems Manager so that License Manager can run cleanup operations.

Querying Systems Manager inventory requires a Resource Data Sync to store inventory in an Amazon S3 bucket, Amazon Athena to aggregate inventory data from organizational accounts, and Amazon Glue to provide a fast query experience. For more information, see Using service-linked roles for Amazon License Manager.

Resource inventory tracking is also useful if your organization does not restrict Amazon users from creating AMI-derived instances or installing additional software on running instances. License Manager provides you with a mechanism to easily discover these instances and applications using inventory search. You can attach rules to these discovered resources and track and validate them the same as instances created from managed AMIs.

Contents

Working with inventory search

License Manager uses Systems Manager inventory to discover software usage on premises. After you associate a self-managed license with on-premises servers, License Manager periodically collects software inventory, updates licensing information, and refreshes its dashboards to report usage.

Tasks

Setting up for inventory search

Complete the following requirements before using resource inventory search:

- Enable cross-account inventory discovery by integrating License Manager with your Amazon Organizations account. For more information, see Settings in Amazon License Manager.
- Create self-managed licenses for the servers and applications to manage. For example, create a self-managed license that reflects the terms of your licensing agreement with Microsoft for SQL Server Enterprise.

Using inventory search

Complete the following steps to search your resource inventory. You can search for applications by name (for example, names that begin with "SQL Server") and the type of license included (for example, a license that is not for "SQL Server Web").

Search your resource inventory

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the navigation pane, choose **Inventory search**.
3. (Optional) You can specify filter options to streamline search results as follows.

   Amazon EC2 resources

Filter name	Description	Logical operators	Supported values
Resource ID	The ID of the resource.	`Equals`, `Not equals`	
Account ID	The ID of the Amazon account that owns the resource.	`Equals`, `Not equals`	
Platform name	The operating system platform for the resource.	`Equals`, `Not equals`, `Begins with`, `Contains`	
Application name	The name of the application.	`Equals`, `Begins with`	

Filter name	Description	Logical operators	Supported values
License included name	The type of license included.	`Equals`, `Not equals`	• `SQL Server Enterprise` • `SQL Server Standard` • `SQL Server Web` • `Windows Server Datacenter`
Tag	A metadata tag key and optional value that's assigned to the resource. Note, the `Not equals` logical operator is only available if cross-account discovery is enabled.	`Equals`, `Not equals`	

Amazon RDS resources

Filter name	Description	Logical operators	Supported values
Engine Edition	The database engine edition.	`Equals`	• `oracle-ee` • `oracle-se` • `oracle-se1` • `oracle-se2` • `db2-se` • `db2-ae`

Filter name	Description	Logical operators	Supported values
License Pack (Oracle only)	The management pack associated with an Amazon RDS for Oracle license.	`Equals`	• `Spatial and Graph` • `Active Data Guard` • `Label Security` • `Oracle On-Line Analytical Processing (OLAP)` • `Diagnosti c Pack and Tuning Pack`

For more information about Amazon RDS database product licenses, see RDS for Oracle licensing options, or RDS for Db2 licensing options in the *Amazon RDS User Guide*.

Adding automated discovery rules to a self-managed license

After you add product information to your self-managed license, License Manager can track license usage for the instances that have those products installed. For more information, see Automated discovery of inventory.

To add automated discovery rules to a self-managed license

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. Open the **Inventory search** page.
3. Select the resource and choose **Add automated discovery rules**.
4. For **Self-managed license**, select a self-managed license.

5. Specify the products to discover and track.
6. (Optional) Select **Stop tracking instances when software is uninstalled** to make the license available for reuse after License Manager detects that the software was uninstalled and any license affinity period has elapsed.
7. (Optional) To exclude resources from automated discovery select **Add exclusion rule**.

   > **Note**
   >
   > Exclusion rules do not apply to Amazon RDS products (such as RDS for Oracle and RDS for Db2).

   a. Choose a **Property** to filter on, currently **Account ID**, and **Tag** are supported.
   b. Enter the information to identify that property. For an **Account ID** specify the 12 digit Amazon Account ID as the value. For **Tags** enter a key/value pair.
   c. Repeat step 7 to add additional rules.
8. Choose **Add**.

Associating a self-managed license with inventory search

After you have identified the unmanaged resources that you need to manage, you can manually associate them with a self-managed license, instead of using automated discovery.

To associate a self-managed license with a resource

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. Open the **Inventory search** page.
3. Select the resource and choose **Associate self-managed license**.
4. For **self-managed license name**, select a self-managed license.
5. (Optional) Select **Share self-managed license with all my member accounts**.
6. Choose **Associate**.

Disassociating a self-managed license and a resource

If the licensing terms from your software vendors change, you can disassociate resources that were associated manually and then delete the self-managed license.

To disassociate a self-managed license and a resource

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **self-managed license**.
3. Choose the name of the self-managed license.
4. Choose **Resources**.
5. Select each of the resources to disassociate from the self-managed license and then choose **Disassociate resource**.

Automated discovery of inventory

License Manager uses Systems Manager inventory to discover software usage on Amazon EC2 instances and on-premises instances. You can add product information to your self-managed license, and License Manager will track the instances that have those products installed. Additionally, you can specify exclusion rules based on your licensing agreement to decide which instances to exclude. You can exclude instances belonging to Amazon account IDs or associated with resource tags from being considered for automated discovery

Automated discovery can be added to a new license set, to an existing self-managed license, or resources in your inventory. Rules for automated discovery can be edited at any time through the CLI using the UpdateLicenseConfiguration API command. To edit rules in the console, you must delete the existing self-managed license and create a new one.

To use automated discovery, you must add product information to your self-managed license. You can do so when you create the self-managed license using **Inventory search**.

You cannot manually disassociate instances tracked by automated discovery. By default, automated discovery does not disassociate tracked instances after the software is uninstalled. You can configure automated discovery to stop tracking instances when the software is uninstalled.

After you configure automated discovery, you can track license usage through the License Manager dashboard.

Prerequisites

- Enable cross-account inventory search by integrating License Manager with your Amazon Organizations account. For more information, see Settings in Amazon License Manager.

> **Note**
>
> Single accounts can set up automated discovery but cannot add exclusion rules.

- Install Systems Manager inventory on your instances.

To configure automated discovery when you create a self-managed license

You can configure automated discovery rules and exclusion rules when you create a self-managed license. For more information, see Create a self-managed license.

To add automated discovery rules to an existing self-managed license

Use the process below to add automated discovery rules to existing self-managed licenses through the console, you can also do this from the **Inventory search** pane by selecting an resource ID and selecting **Add automated discovery rules**.

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **Self-managed licenses**.
3. Choose the name of the self-managed license to open the license details page.
4. On the **Automated discovery rules** tab, choose **Add automated discovery rules**.
5. Specify the products to discover and track.
6. (Optional) Select **Stop tracking instances when software is uninstalled** to make the license available for reuse after License Manager detects that the software was uninstalled and any license affinity period has elapsed.
7. (Optional) To define resources to exclude from automated discovery select **Add exclusion rule**.

> **Note**
>
> - Exclusion rules do not apply to RDS database products (such as Amazon RDS for Oracle and Amazon RDS for Db2).

- Exclusion rules are only available if Cross-account resource discovery has been enabled.

a. Choose a **Property** to filter on, currently **Account ID**, and **Tag** are supported.

b. Enter the information to identify that property. For an **Account ID** specify the 12 digit Amazon account ID as the value. For **Tags** enter a key/value pair.

c. Repeat step 7 to add additional rules.

8. When you are finished choose **Add** to apply your automated discovery rule.

Granted licenses in License Manager

Granted licenses are licenses for products that your organization purchased from Amazon Web Services Marketplace, Amazon Data Exchange, or directly from a seller who integrated their software with managed entitlements. License administrators can use Amazon License Manager to govern the use of these licenses and to distribute rights of use, known as entitlements, to specific Amazon accounts.

Data licenses distributed to Amazon Data Exchange products are available to the Amazon account through Amazon Data Exchange. Before you can distribute licenses from Amazon Web Services Marketplace, you must enable subscription sharing. For more information, see Sharing subscriptions in an organization.

After a license administrator distributes an entitlement from an Amazon Web Services Marketplace license to an Amazon account, and the recipient accepts and activates the granted license, the subscription is available to the Amazon account through Amazon Web Services Marketplace. The account also has access to the product. For example, if a license administrator purchases an Amazon Machine Image (AMI) from Amazon Web Services Marketplace and distributes an entitlement to your Amazon account, you can launch Amazon EC2 instances from the AMI using Amazon Web Services Marketplace and Amazon EC2.

Topics

- License status
- Metrics for buyer accounts

View your granted licenses

License Manager displays tabs to view and manage your granted licenses based on the permissions you are authenticated with. The granted license page can display the following tabs:

My licenses

This tab is available for any user that has access to view the granted licenses in License Manager. The tab has a **My granted licenses** section which includes information about each license such as the **License ID** and **Product name**. From this page you can view additional information about each license.

License summary (for organization administrators)

This tab is available only for organization administrators. The tab has a **Totals** section which lists the total amount of products and granted licenses across all accounts in your organization. It also shows a **Products** section which includes a table detailing the properties of each product, such as the **Product name** and **Number of granted licenses**.

Aggregated licenses (for organization administrators)

This tab is available only for organization administrators. This tab has a section detailing **Granted licenses for my organization** which includes information about each license such as the **License ID** and **Product name**. From this page you can view additional information about each license.

Manage your granted licenses

Licenses that have been granted to you will appear in the License Manager console. Recipients must accept and activate granted licenses before they can use the product. How you accept and activate a license depends on whether the license is from Amazon Web Services Marketplace, if your account is member account in an organization for Amazon Organizations, and whether all features is enabled for your organization.

Granted licenses require cross-Region replication of license metadata. License Manager automatically replicates each granted license and its associated information to other Amazon Web

Services Regions. This enables you to have a centralized view across all Regions where licenses are granted to you.

Licenses from Amazon Web Services Marketplace and Amazon Data Exchange

- Licenses for subscriptions that you purchase are automatically accepted and activated.
- If the management account for an organization with all features enabled purchases a subscription and distributes licenses to member accounts, the licenses are automatically accepted in the member accounts. Either the management account or the member accounts can later activate the license.
- If the management account for an organization with only consolidated billing features enabled purchases a subscription and distributes licenses to member accounts, each member account must accept and activate the license.

Licenses from a seller

- You must accept and activate licenses for products that use License Manager to distribute licenses.
- If the management account for an organization with all features enabled purchases a product and distributes licenses to member accounts, the licenses are automatically accepted in the member accounts. Either the management account or the member accounts can later activate the license.
- If the management account for an organization with only consolidated billing features enabled purchases a product and distributes licenses to member accounts, each member account must accept and activate the license.

Console (My licenses)

You can view and manage granted licenses for a single Amazon Web Services account.

To manage granted licenses in your account

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the navigation pane, choose **Granted licenses**.
3. Choose the **My licenses** tab if it is not the current selection.
4. (Optional) Use the filter options, such as the following, to scope the list of licenses that are displayed.

- Product SKU – The product identifier for this license, as defined by the license issuer when creating the license. The same product SKU might exist across multiple ISVs.
- Recipient – The ARN of the license recipient.
- Status – The status of the license. For example, **Available**.

5. To view additional information about the license, choose the license ID to open the **License overview** page.
6. If the license issuer is an entity other than Amazon Web Services Marketplace, the initial grant status is **Pending acceptance**. Do one of the following:
   - Choose **Accept & activate license**. The resulting grant status is **Active**.
   - Choose **Accept license**. The resulting grant status is **Disabled**. When you are ready to use the license, choose **Activate license**.
   - Choose **Reject license**. The resulting grant status is **Rejected**. After you reject a license, you cannot activate it.

If you don't want to continue using a license that was activated, you can return to the **License overview** page and choose **Deactivate license**. If you want to continue using a license that was deactivated, return to the **License overview** page and choose **Activate license**.

Console (Aggregated licenses)

You can view your granted licenses that have been aggregated from all accounts in your organization.

> **Important**
>
> In order to use the organization wide view for your granted licenses, you must first link Amazon Organizations using the Amazon License Manager console settings. For more information, see Settings in Amazon License Manager.

To manage granted licenses across your accounts in Amazon Organizations

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the navigation pane, choose **Granted licenses**.
3. Choose the **Aggregated licenses** tab if it is not the current selection.

4. (Optional) Use the filter options, such as the following, to scope the list of licenses that are displayed.

   - Product SKU – The product identifier for this license, as defined by the license issuer when creating the license. The same product SKU might exist across multiple ISVs.
   - Beneficiary – The account in your organization that the license is granted to.

5. To view additional information about the license, choose the license ID to open the license detail page.
6. If the license issuer is an entity other than Amazon Web Services Marketplace, do one of the following:

   - Choose **Activate license**. The resulting grant status is **Active**.
   - Choose **Deactivate license**. The resulting grant status is **Deactivated**.

If you don't want to continue using a license that was activated, you can return to the **License overview** page and choose **Deactivate license**. If you want to continue using a license that was deactivated, return to the **License overview** page and choose **Activate license**.

Amazon CLI

You can use the Amazon CLI to work with your granted licenses.

To manage your granted licenses using the Amazon CLI:

- accept-grant
- create-grant-version
- get-grant
- list-licenses
- list-received-grants
- list-received-grants-for-organization
- list-received-licenses
- list-received-licenses-for-organization
- reject-grant

Distribute entitlements

If you are a license administrator operating in the management account of your organization with all features enabled, you can distribute entitlements to your organization from your granted licenses by creating a grant. For more information about Amazon Organizations, see Amazon Organizations terminology and concepts.

You can specify the recipient of the grant as one of the following:

- An Amazon Web Services account, which includes only the specified account.
- An organization root, which will include all accounts across your organization.
- An organizational unit (OU) (that is not nested), which includes all accounts in the specified OU and in nested OUs under the specified OU.

> **Note**
>
> You can create up to 2,000 grants per license.

You can use either the Amazon License Manager console or the Amazon CLI to distribute your entitlements. You can specify the organization ID or the organization ARN when creating a grant in the console, but the ARN format must be used with the Amazon CLI. For example, the ARNs will resemble the following:

Organization ID ARN

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

Organization OU ARN

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

Console

To create a grant (Console)

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.

2. In the navigation pane, choose **Granted licenses**.
3. Choose a license ID to open the **License overview** page.
4. From the **Grants** section, choose **Create grant**.
5. On the **Grant details** panel, do the following:

    a. Enter a name for the grant to help you identify the purpose or recipient of the grant.

    b. Enter the Amazon Web Services account ID, Amazon Organizations OU ID or ARN, or Amazon Organizations ID or ARN of the grant recipient.

    c. Choose **Create grant**.
6. On the **License overview** page, you'll see an entry for the grant in the **Grants** panel. The initial status of the grant is **Pending acceptance**. The status changes to **Active** when the recipient accepts the grant or **Rejected** when the recipient rejects the grant.

Amazon CLI

You can use the Amazon CLI to distribute an entitlement. You must use specify an organization ID or OU in ARN format when using the Amazon License Manager API.

To create and list your grants using the Amazon CLI:

- create-grant
- list-distributed-grants

The grant details page displays the list of accounts that you have granted access to the entitlement. After distributing a license to your organization, you can deactivate or activate the licenses individually on each account.

Grant acceptance and activation

When a grant is created for a granted license, it is distributed to the recipient. A granted license must be accepted and activated before it can be used by the grant recipient. The grant activation process can include additional options for granted licenses sourced from the Amazon Web Services Marketplace.

By default, the **Grant overview** page for a granted license has a status of `Pending Acceptance`. You can choose to `Accept`, `Accept and Activate`, or `Reject` the grant. Grants that are

accepted but not yet activated have a status of `Disabled`. Accepted and activated grants have a status of `Active`.

A granted license must be accepted and activated before it can be used by the grant recipient. By default, the grant details page for a granted license has a status of **Pending acceptance**. You can choose to **Accept**, **Accept and Activate**, or **Reject** the license. Grants that are accepted but not yet activated have a status of **Disabled**. Accepted and activated grants have a status of **Active**.

> **Tip**
>
> You can automatically accept grants that come from the management account of your organization. To enable grant auto-acceptance, link your organization accounts on the settings page in the Amazon License Manager console from the management account.

You can't activate two licenses for the same product from Amazon Web Services Marketplace at the same time. If you have two subscriptions (for example, the public offer for a product and a private offer, or a subscribed license for a product and a granted license for the same product), you can take one of the following actions:

1. Disable the existing grant for the same product and then activate the new grant.
2. Activate the new grant and specify that you want to disable and replace the existing active grant with the new grant. You can use the License Manager console or the Amazon CLI:
   a. Using the License Manager console, activate the new grant while selecting **Yes** that you want to replace active grants.
   b. Using the `CreateGrantVersion` API, activate the new grant by specifying `ALL_GRANTS_PERMITTED_BY_ISSUER` for the `ActivationOverrideBehavior` with a `Status` of `Active`.

Console

You can use the License Manager console to activate a grant. When you activate a grant sourced from the Amazon Web Services Marketplace, you might be presented with the option whether to replace active grants:

- As a license administrator, you must specify if you want to replace active grants when activating a grant.

- As a grantor, you can optionally specify if you want to replace active grants when you activate a grant for another account in your organization.

- As a grantee, if the grantor creating the distributed grant didn't specify whether to replace active grants, you must make a selection when activating the grant.

To activate a grant (Console)

1. Open the License Manager console at https://console.aws.amazon.com/license-manager/.
2. In the navigation pane, choose **Granted licenses**.
3. Choose a license ID to open the **License overview** page.
4. Choose a grant name to open the **Grant overview** page.
5. If presented, select an activation option for whether you want to replace active grants:
   a. **No** – This option will activate the grant without replacing any existing active grants for the recipient (grantee).
   b. **Yes** – This option will disable grants for the same product and activate a new grant for the defined recipient (grantee):
      i. A specified Amazon Web Services account.
      ii. Member accounts of the specified organization OU.
      iii. All member accounts of the organization.
6. (Optional) Provide a reason for activating the grant.
7. Enter **`activate`** into the input box, and choose **Activate**.

Amazon CLI

You can use the Amazon CLI to work with your granted licenses.

To work with distributed grants using the Amazon CLI:

- accept-grant
- create-grant-version
- list-received-grants
- list-received-grants-for-organization
- reject-grant

License status

Licenses have two statuses: The **License status**, which shows the overall availability and sharability of the license, and the **Grant status**, which shows the ability to use the license.

The follow table shows the various statuses for a granted license:

Status	Description
AVAILABLE	The license is available to use and share.
PENDING_AVAILABLE	The license is not available to use as it is still processing.
DEACTIVATED	The license is not available to use because it has been deactivated by the license issuer.
SUSPENDED	The license is not available to use as it is suspended.
EXPIRED	The license is not available to use because it has reached the end of term.
PENDING_DELETE	The license is not available to use as it is in the process of being deleted.
DELETED	The license is not available to use because the license agreement has been canceled.

The following table shows the various statuses for a grant:

Status	Description
PENDING_WORKFLOW	The grant is in the process of being distribut ed.
PENDING_ACCEPT	The grant has been created and the grant recipient has not yet accepted it.

Status	Description
REJECTED	The grant has been rejected by the grant recipient.
ACTIVE	The grant has been accepted and activated for use by the grant recipient. The licensed resource can be used.
FAILED_WORKFLOW	The grant failed to distribute.
DELETED	The grant has been deleted by the grantor.
PENDING_DELETE	The grant that was distributed is in the process of being deleted.
DISABLED	The grant has been accepted by the grant recipient, but has not been activated for use.
WORKFLOW_COMPLETE	The grant to an organization has been distributed or recalled. The grant details show the status of sub-grants to each account in the organization.

Metrics for buyer accounts

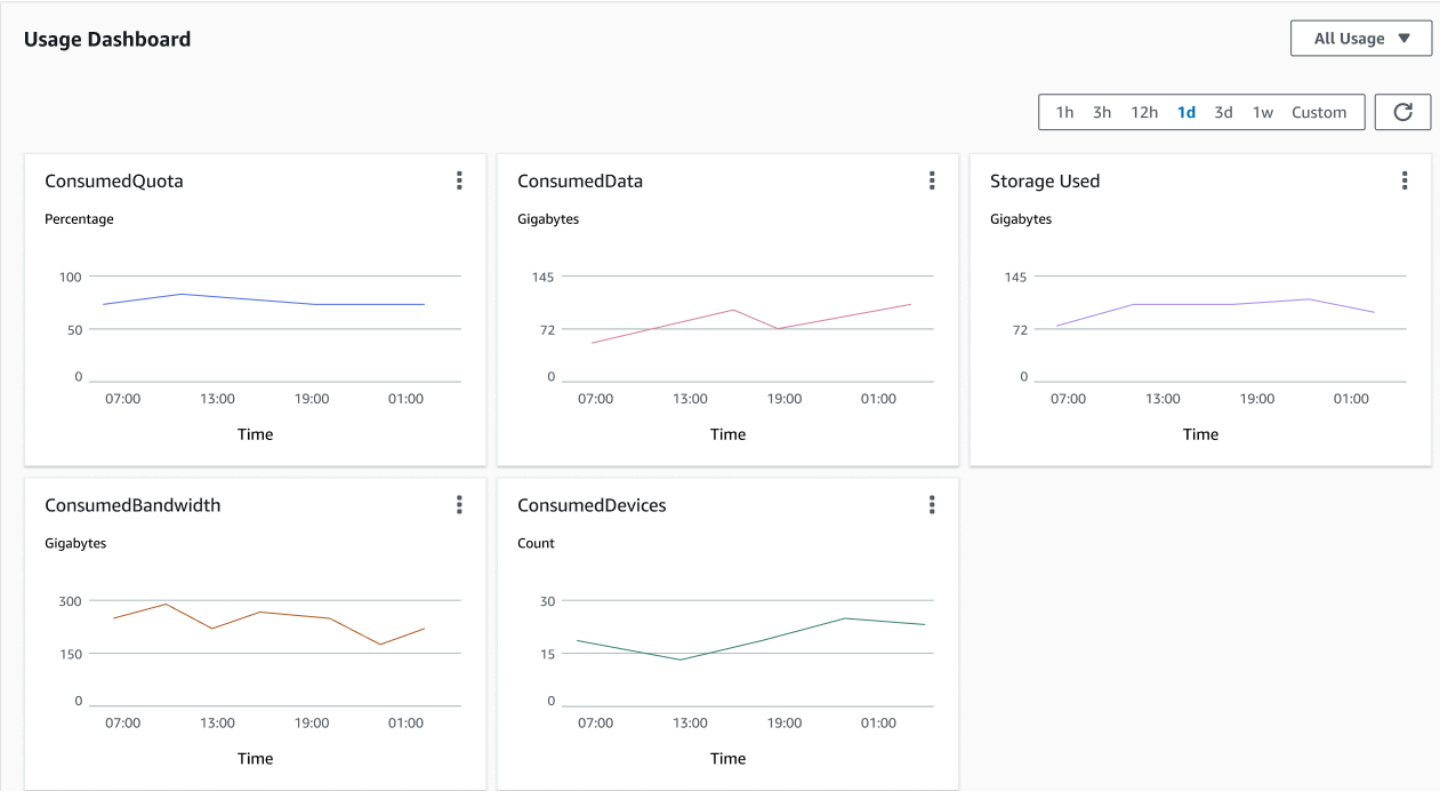
When a grant for a seller issued license is configured with **allow submission of usage records** selected, License Manager emits a CloudWatch metric to the seller account, root buyer account, and the account against which the usage is being recorded. Buyer accounts are the Amazon Web Services accounts who have purchased or been granted a seller issued license. For more information, see Granting licenses to customers.

Usage dashboard

When a seller or independent software vendor (ISV) application records usage against a license for a buyer account, the account in which usage is being recorded and the root buyer account see a CloudWatch widget with usage records on the **Usage dashboard** page in the License Manager console. Buyers can also see metrics for accounts that they have distributed licenses to in Amazon

Organizations. The graphs on the **Usage dashboard** page are available for every license for which usage records have been sent.

The following image is an example of the usage dashboard:



Seller issued licenses in License Manager

Independent software vendors (ISVs) can use Amazon License Manager to manage and distribute software licenses to end-users. As an issuer, you can track the usage of your seller issued licenses centrally using the License Manager dashboard.

License Manager uses open, secure, industry standards for representing licenses and allows customers to cryptographically verify their authenticity. License Manager associates each license with an asymmetric key. As the ISV, you own the asymmetric Amazon KMS keys and store them in your account.

Seller issued licenses require cross-Region replication of license metadata. License Manager automatically replicates each seller issued license and its associated information to other Regions.

License Manager supports a variety of different licensing models including the following:

- **Perpetual** – Lifetime licenses with no expiration date that authorize users to use the software indefinitely.
- **Floating** – Shareable licenses with multiple instances of the application. Licenses can be prepaid and a fixed set of entitlements added to them.
- **Subscription** – Licenses with expiration dates that can be automatically renewed unless specifically deactivated.
- **Usage-based** – Licenses with specific terms based on usage, such as the number of API requests, transactions, or storage capabilities.

You can create licenses in License Manager and distribute them to customers using an Amazon IAM identity or through bearer tokens generated by License Manager. Customers with an Amazon account can re-distribute the license entitlements to Amazon identities in their respective organizations. Customers with distributed entitlements can check out and check in the required entitlements from that license through your software integration with License Manager.

Entitlements

License Manager captures license capabilities as *entitlements* in the license. Entitlements can be characterized with a limited or unlimited quantity. An example of a limited entitlement is '40 GB of data transfer'. An example of an unlimited quantity entitlement is 'Platinum Tier'.

A license captures all the granted entitlements, the activation and expiration dates, and the issuer details. A license is a versioned entity and each version is immutable. License versions are updated whenever the license is changed.

To check out or check in limited entitlements, ISV applications must specify the amount of each limited capacity. For unlimited entitlements, ISV applications can simply specify the relevant entitlement to check out or check in again. Finally, limited capabilities also support an "overage" flag, which indicates if end-users can exceed their usage of the initial entitlements. License Manager tracks and reports usage, along with any overages, to the ISV.

License usage

License Manager allows you to centrally track licenses across multiple Regions, by maintaining a count of all the checked out entitlements. License Manager also tracks the identity of the user and the underlying resource identifier, if available, associated with each check out, along with when it was checked out. You can track this time-series data through CloudWatch Events.

Licenses may be in one of the following states:

- **Created** – The license is created.
- **Updated** – The license is updated.
- **Deactivated** – The license is deactivated.
- **Deleted** – The license is deleted.

Requirements

To get started with this feature, you need permission to call the following License Manager API actions.

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

If you will integrate with License Manager so customers without an Amazon account can consume licenses sold outside of Amazon Web Services Marketplace, you must create a role that enables your software application to call the License Manager API. For example, you can use the Amazon CLI. First, use the create-role command to create a role named **AWSLicenseManagerConsumptionRole**.

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

The following is `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"
            }
        }
    }
}
```

Next, use the attach-role-policy command to add the **AWSLicenseManagerConsumptionPolicy** Amazon managed policy to the **AWSLicenseManagerConsumptionRole** role.

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

Creating seller issued licenses

Use the following procedure to create a block of licenses to grant to customers using the Amazon Web Services Management Console. Alternatively, you can create the license using the CreateLicense API action.

To create a license using the console

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. Choose **Seller Issued Licenses** from the left menu.
3. Choose **Create license**.
4. For **License metadata**, provide the following information:
   - **License name** – The name, up to 150 characters, to display to buyers.
   - **License description** – An optional description, up to 400 characters, that differentiates this license from other licenses.
   - **Product SKU** – The product SKU.
   - **Recipient** – The recipient's name (company or individual).
   - **Home Region** – The Amazon Region for the license. Although licenses can be consumed globally, you can only change the license in the home region. You cannot change the home region for a license after you create it.
   - **License start date** – The date of activation.
   - **License end date** – The end date of the license, if applicable.
5. For **Consumption configuration**, provide the following information:
   - **Renewal frequency** – Whether to renew weekly, monthly, or not at all.
   - **Consumption configuration** – Choose **Provisional Consumption Configuration Options** if the license is to be used for continuous connectivity or **Borrow** if the license is to be used offline. Enter **Max time to live (minutes)** to set the length of availability of the license.
6. For **Issuer**, provide the following information:
   - **Enter an Amazon KMS key** – License Manager uses this key to sign and verify the issuer. For more information, see Cryptographic Signing of Licenses.
   - **Issuer name** – The business name for the seller.
   - **Seller of record** – An optional business name.

- **Agreement URL** – The URL to the license agreement.

7. For **Entitlement**, provide the following information about the capabilities that the license grants to recipients:

   - **Name** – The name of the recipient.
   - **Unit type** – Select the unit type, then provide the maximum count.
   - Check **Allow check in** if recipients must check in licenses before renewal.
   - Check **Overages allowed** if recipients can use the resource beyond the maximum count. This option might incur additional charges for the recipient.

8. Choose **Create license**.

Granting licenses to customers

After you add the new license, you can grant the license to a customer with an Amazon account using the Amazon Web Services Management Console. The recipient must accept the grant before using the license. For more information, see Granted licenses in License Manager.

Alternatively, if the customer does not have an Amazon account, you can use the License Manager API to enable customers to consume licenses.

To grant a license to a customer using the console

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. Choose **Seller Issued Licenses** from the left menu.
3. Choose the ID of the license to open its details page.
4. For **Grants**, choose **Create grant**.
5. For **Grant details**, provide the following information:

   - **Grant name** – The grant name. This is used to enable search capabilities.
   - **Amazon account ID** – The Amazon account number of the license recipient.
   - **License rights**
     - Select **Consumption** if the recipient can consume granted entitlements.
     - Select **Distribution** if the recipient can distribute granted entitlements to other Amazon accounts.

- Select **Allow on-premise token generation** to authenticate shared licenses without using Amazon identities or credentials.
- Select **Allow submission of usage records** to permit license recipients to emit usage records for usage types.

- **Home Region** – The Amazon Web Services Region for the license.

6. Choose **Create grant**.

Getting temporary credentials for customers without an Amazon account

For customers without an Amazon account, you can use entitlements in the same manner that you do for your customers with an Amazon account. Use the following procedure to get temporary Amazon credentials for your customers without an Amazon account. The API calls must be made in the home Region.

To get temporary credentials to use in calling the License Manager API

1. Call the CreateToken API action to get a refresh token encoded as a JWT token.
2. Call the GetAccessToken API action, specifying the refresh token that you received from `CreateToken` in the previous step, to receive a temporary access token.
3. Call the AssumeRoleWithWebIdentity API action, specifying the access token that you received from `GetAccessToken` in the previous step, and the **AWSLicenseManagerConsumptionRole** role that you created, to get temporary Amazon credentials.

To create a token from the Amazon License Manager console

1. From the License Manager console, navigate to the License details page for the specific license entitlement you want to use without an Amazon account.
2. Choose **Create token** to generate a temporary access token.

> **Note**
>
> The first time you generate a temporary access token, you will be asked to create a service role so that License Manager can access services on your behalf. The following service role is created: `AWSLicenseManagerConsumptionRole`.

3. Download the `token.csv` file, or copy the token string when it is generated.

> **Important**
>
> This is the only time you can view or download this token. We recommend that you download the token and store the file in a secure location. You can create new tokens at any time, up to the service limit.

Consuming licenses

License Manager allows multiple users to concurrently consume entitlements, with limited capabilities, from a single license. Call the CheckoutLicense API action. The following is a description of the parameters.

- **Key fingerprint** – Trusted license issuer.

  Example: aws:123456789012:issuer:issuer-fingerprint

- **Product SKU** – Product identifier for this license, as defined by the license issuer when creating the license. The same product SKU might exist across multiple ISVs. Therefore, trusted key fingerprints play an important role.

  Example: 1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0daEXAMPLE

- **Entitlements** – Capabilities to check out. If you specify an unlimited capability, the quantity is zero. Example:

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

- **Beneficiary** – Software as a Service (SaaS) ISVs can check out licenses on behalf of a customer by including the customer identifier. License Manager limits the call to the repository of licenses created in the SaaS ISV account.

  Example: user@domain.com
- **Node ID** – An identifier used to node-lock the license to a single instance of the application.

  Example: 10.0.21.57

Deleting seller issued licenses

After you delete a license, you can recreate it. The license and its data are retained and available to the license issuer and license grantees in read-only mode for six months.

Use the following procedure to delete a license that you have created using the Amazon Web Services Management Console. Alternatively, you can delete the license using the DeleteLicense API action.

To delete a license using the console

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. Choose **Seller issued licenses** from the left menu.
3. Choose the radio button next to the license to select it for deletion.
4. Choose **Delete**. When prompted for confirmation, enter **`delete`** and choose **Delete**.

Linux subscriptions in License Manager

Amazon License Manager provides you with the capability to view and manage commercial Linux subscriptions which you own and run on Amazon. License utilization can be tracked across Amazon Web Services Regions and accounts in Amazon Organizations. Once data is discovered and aggregated, you will have insight to all your instances using commercial Linux subscriptions. In addition, your discovered subscription data will be displayed in the License Manager console as Amazon CloudWatch dashboards. If your accounts are in Organizations, you can register a member account as the delegated administrator for administrative tasks. For more information, see Delegated administrators.

You track utilization across multiple subscriptions such as:

- Red Hat Enterprise Linux (RHEL) subscription-included
- RHEL Bring Your Own Subscription model (BYOS) with the Red Hat Cloud Access Program
- SUSE Linux Enterprise Server
- Ubuntu Pro

Linux subscriptions uses the eventual consistency model. A consistency model determines the manner and timing in which data is loaded and presented in your Linux subscriptions view. With this model, License Manager ensures that your Linux subscription data will be updated periodically from your resources. In the event that some data is not ingested during these intervals, the information will be delivered at the next metric emission. This behavior can delay resources, such as newly launched EC2 commercial Linux instances, from displaying in the Linux subscriptions dashboard.

> **Note**
>
> It can take up to 36 hours for the initial resource discovery to complete, and up to 12 hours for newly launched instances to be discovered and reported. Once your resources are discovered, Amazon CloudWatch metrics are emitted hourly for Linux subscriptions data.

Contents

Managing discovery of Linux subscriptions

You can manage the discovery of Linux subscriptions using the License Manager console. When you enable discovery of Linux subscriptions for the Amazon Web Services Regions you specify, you can optionally extend this discovery to your accounts in Amazon Organizations. If you no longer want to track subscription utilization, you can also disable discovery.

> **Note**
>
> You can discover and display up to 5,000 resources per account per Amazon Web Services Region by default. To request an increase to these limits, use the limit increase form.

Topics

Enabling discovery of Linux subscriptions

To enable the discovery of Linux subscriptions, you need to configure the required settings in License Manager. From the settings page, you can create the service-linked role, specify which Amazon Web Services Regions to enable discovery in, and whether to discover resources across your accounts in Amazon Organizations.

To enable discovery for Linux subscriptions

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **Settings**.
3. On the **Settings** page, choose the **Linux subscriptions** tab and choose **Configure**.
4. For **Source Amazon Web Services Regions**, choose the Regions for which you want to discover Linux subscriptions.
5. If you want to aggregate subscription data across your accounts in Amazon Organizations, select **Link Amazon Organizations**.
6. Review and acknowledge the option which grants Amazon License Manager permission to create a service-linked role for Linux subscriptions.

7. Choose **Save configuration**.

Resource discovery status reasons

Amazon License Manager will display a status and a corresponding status reason for each Amazon Web Services Region you choose to enable discovery for Linux subscriptions. The status reason will vary if you have linked Linux subscriptions with Amazon Organizations:

- In progress
- Successful
- Failed

The status reason that displays for each Region you choose will show up to two status reasons at a time. The following table provides more detail:

Status reason action	Description
Account-onboard	Onboarding a single account.
Account-offboard	Offboarding a single account.
Org-onboard	Onboarding an entire organization.
Org-offboard	Offboarding an entire organization.

You can call the `UpdateServiceSettings` API and subsequently call the `GetServiceSettings` API to monitor the progress of enabling Linux subscriptions. Each status and status reason can apply to multiple Regions at once. The follow table provides more detail on the status and status reason:

Status	Status reason	Description
In Progress	`"Region": "Account-Onboard: Pending"`	Enabling Linux subscriptions for a single account is in progress.

Status	Status reason	Description
	`"Region": "Org-Onboard: Pending"`	Enabling Linux subscriptions for an organization is in progress.
	`"Region": "Account-Offboard: Pending`	Disabling Linux subscriptions for a single account is in progress.
	`"Region": "Org-Offboard: Pending`	Disabling Linux subscriptions for an organization is in progress.
Successful	`"Region": "Account-Onboard: Successful"`	Enabling Linux subscriptions for a single account was successful.
	`"Region": "Org-Onboard: Successful"`	Enabling Linux subscriptions for an organization was successful.
	`"Region": "Account-Offboard: Successful`	Disabling Linux subscriptions for a single account was successful.
	`"Region": "Org-Offboard: Successful`	Disabling Linux subscriptions for an organization was successful.
Failed	`"Region": "Account-Onboard: Failed - Service-linked role not present"`	Enabling Linux subscriptions for a single account has failed due to the required service-linked role not being created. Create the required role, and try again.
	`"Region": "Account-Onboard: Failed - An internal error occurred"`	Enabling Linux subscriptions for a single account has failed due to an internal error.

Status	Status reason	Description
	`"Region": "Org-Onboard: Failed - Account isn't the management account"`	Enabling Linux subscriptions for an organization has failed due to the account performing the operation not being the organization's management account. Log in to the management account, and try again.
	`"Region": "Org-Onboard: Failed - Account isn't part of an organization"`	Enabling Linux subscriptions for an organization has failed due to the account performing the operation not being in an organization. Try the operation from an account in the organization, or add this account to the organization, and try again.
	`"Region": "Org-Onboard: Failed - Linux subscriptions can't access the organization"`	Enabling Linux subscriptions for an organization has failed due to License Manager not having permissions to access the organization. Create the service-linked role for Linux subscriptions, and try again.

Disabling discovery of Linux subscriptions

You can disable discovery of Linux subscriptions from the Amazon License Manager settings page.

> **Warning**
>
> If you disable discovery, all of your data previously discovered for Linux subscriptions will be removed from Amazon License Manager.

To disable discovery for Linux subscriptions

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **Settings**.
3. On the **Settings** page, choose the **Linux subscriptions** tab and choose **Disable Linux subscription discovery**.
4. Enter **`Disable`** and then choose **Disable** to confirm deactivation.
5. (Optional) Remove the service-linked role used for Linux subscriptions. For more information, see Delete a service-linked role for License Manager.
6. (Optional) Disable trusted access between License Manager and your organization. For more information, see Amazon License Manager and Amazon Organizations.

Viewing discovered instance data

Once the initial resource discovery has completed, you will be able to view your Linux subscriptions discovered in the Amazon Web Services Regions you selected. If you chose to link Amazon Organizations, data from accounts across your organization will be aggregated as well. You can navigate to the **Instances** section of the Amazon License Manager console to view a table of the data. You can navigate to the **Instances** section of the Amazon License Manager console to view a table of the data.

Data for each instance includes the following:

- **Instance ID** – The ID of the instance.
- **Instance type** – The type of instance.
- **Account ID** – The ID of the account which owns the instance.
- **Status** – The status of the instance.
- **Region** – The Amazon Web Services Region in which the instance resides.
- **Usage operation** – The operation of the instance and the billing code that is associated with the AMI. For more information, see Usage operation values.
- **Product code** – The product code associated with the AMI used to launch the instance. For more information, see AMI product codes.
- **AMI ID** – The ID of the AMI used to launch the instance.

Topics

Viewing data for all instances

You can view data for all instances has been aggregated across accounts in your organization within the chosen Regions.

To view discovered data for all of your instances

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, under Linux subscriptions, choose **Instances**.
3. Review the data as needed in the console. You can filter the data by:
   - Instance ID
   - Account
   - Region
   - AMI ID
   - Usage operation
   - Product code
4. (Optional) Choose **Export view to CSV** to export data for all of your instances as a comma-separated values file (CSV).

Viewing data for instances per subscription

You can view data for all instances has have been aggregated across accounts in your organization within the chosen Regions.

To view discovered data for instances with a specific subscription

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, under Linux subscriptions, choose **Subscriptions**.
3. Under the **Subscription name** column, choose the subscription you would like to view data for.
4. Choose the **Instances** tab and review the data as needed in the console. You can filter the data by:

- Instance ID
- Account
- Region
- AMI ID
- Usage operation
- Product code

5. (Optional) Choose **Export view to CSV** to export data for your instances with this subscription as a comma-separated values file (CSV).

Billing information for Linux subscriptions

Each commercial Linux subscription running on Amazon EC2 will have billing information associated with the Amazon Machine Image (AMI). Commercial Linux subscriptions will have Amazon EC2 usage operation, Amazon Web Services Marketplace product code, or a combination of both. For more information, see AMI billing information fields in the *Amazon Elastic Compute Cloud User Guide for Linux Instances* and AMI product codes in the *Amazon Web Services Marketplace Seller Guide*.

Subscription name	Amazon EC2 usage operation	Amazon Web Services Marketplace product code	Subscription type
Red Hat Enterprise Linux Server BYOS	RunInstances:00g0	✗	Bring Your Own Subscription model (BYOS)
Red Hat Enterprise Linux Server	RunInstances:0010	✗	EC2 subscription-included
Red Hat Enterpris e Linux with High Availability Add-on	RunInstances:1010	✗	EC2 subscription-included
Red Hat Enterpris e Linux with SQL	RunInstances:1014	✗	EC2 subscription-included

Subscription name	Amazon EC2 usage operation	Amazon Web Services Marketplace product code	Subscription type
Server Standard and High Availability			
Red Hat Enterprise Linux with SQL Server Enterprise and High Availability	RunInstances:1110	✗	EC2 subscription-included
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014	✗	EC2 subscription-included
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210	✗	EC2 subscription-included
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110	✗	EC2 subscription-included
SUSE Linux Enterprise Server	RunInstances:000g	✗	EC2 subscription-included
Red Hat Enterprise Linux for SAP with High Availability and Update Services	RunInstances:0010	✓	Amazon Web Services Marketplace subscription [1]
SUSE Linux Enterprise Server with SAP	✗	✓	Amazon Web Services Marketplace subscription
Ubuntu Pro	RunInstances:0g00	✓	Amazon Web Services Marketplace subscription

Subscription name	Amazon EC2 usage operation	Amazon Web Services Marketplace product code	Subscription type
Red Hat Enterprise Linux Workstation	✗	✓	Amazon Web Services Marketplace subscription

[1] This subscription has both an Amazon EC2 usage operation and Amazon Web Services Marketplace product code.

Usage metrics and Amazon CloudWatch alarms for Linux subscriptions

The **Subscriptions** section of the Amazon License Manager console lists the discovered commercial Linux subscriptions you have purchased on Amazon or have brought in using the Bring Your Own Subscription model (BYOS). All commercial Linux subscriptions are on a per instance basis for licensing.

The following details are available per discovered Linux subscription:

- Subscription name
- Subscription type
- Number of running instance per subscription
- Configured Amazon CloudWatch alarms

When you choose a Linux subscription from the summary page, the **Usage metrics and alarms** tab will display data for that subscription. In this tab, Amazon CloudWatch dashboards display for the chosen subscription within the License Manager console. You can adjust the dashboard to encompass a certain time frame, or *evaluation range,* in hours, days, or a week from a selected date.

In the **Usage metrics and alarms** tab, each subscription has an **Alarms** section which details the following:

- **Alarm name** – The name of the alarm.
- **State** – The state of the alarm.

- **Dimension** – The dimensions of the alarm. The dimension will include the Amazon Web Services Region and instance type that was defined.
- **Condition** – The condition of the alarm. The condition will include the comparison operator and alarm threshold value that was defined.

You can create CloudWatch alarms using the dimensions and conditions you define to track and alert based on your current subscription utilization. The Linux subscriptions console displays a summary of the subscription names in use, the subscription types, amount of running instances for each, and the alarm status.

The following are possible CloudWatch alarm states:

- **OK** – The metric or expression is within the defined threshold.
- **ALARM** – The metric or expression is outside of the defined threshold.
- **INSUFFICIENT_DATA** – The alarm has just started, the metric is not available, or not enough data is available for the metric to determine the alarm state.

Topics

Usage metrics for Linux subscriptions

The following metrics and dimensions are available for Linux subscriptions:

Metric	Description
RunningInstancesCount	The total number of instances running in the current account that are grouped by the subscription name, or by subscription name and Region. Units: Count Dimensions:

Metric	Description
	`SubscriptionName` : The name of the subscription. `Region`: The Region where the resource using a commercial Linux subscription was discovered.

Creating an alarm for Linux subscriptions

You can create alarms for each commercial Linux subscription that you have discovered on your running EC2 instances. If necessary, you can create multiple alarms with different dimensions and conditions for each subscription.

To create a CloudWatch alarm for Linux subscriptions using the console

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, under Linux subscriptions, choose **Subscriptions**.
3. Under the **Subscription name** column, choose the subscription to create an alarm for, then choose **Create alarm**.
4. Specify the following for the alarm:
   - **Alarm name** – specify a name which resembles `AWS-LM-LS-`*`AlarmName`*.
   - Instance type – choose an instance type that will be using the subscription that was selected.
   - Usage Region – choose the Regions to create the alarms for.
   - Comparison operator – the comparison operator for the alarm threshold.
   - Alarm threshold value – the value for the alarm threshold.
5. Choose **Create** to create the alarm.

Modifying an alarm for Linux subscriptions

You can modify existing alarms to adapt to changing requirements from the License Manager console.

To modify a CloudWatch alarm for Linux subscriptions using the console

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, under Linux subscriptions, choose **Subscriptions**.

3. Under the **Subscription name** column, choose the subscription to modify, then choose **Edit**.
4. Modify the defined values as required.
5. Choose **Edit** to modify the alarm.

Deleting an alarm for Linux subscriptions

You can delete existing alarms to adapt to changing requirements from the License Manager console.

To delete a CloudWatch alarm for Linux subscriptions using the console

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, under Linux subscriptions, choose **Subscriptions**.
3. Under the **Subscription name** column, choose the subscription to modify, then choose **Delete**.

Settings in Amazon License Manager

The **Settings** section of the Amazon License Manager console displays settings for the current account. You must configure settings to enable certain functionality such as distribution of managed entitlements and self-managed licenses to your organization, as well as for performing cross-account resource discovery.

To edit License Manager settings

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the left navigation pane, choose **Settings**.
3. Choose the tab containing the settings you wish to configure or modify. For example, choose **Managed licenses** to configure **Account details**.
4. Choose the relevant action for the setting you wish to configure or modify. For example, you might choose **Edit** or **Turn on**.

Settings topics

- Managed licenses
  - Account details
  - Cross-account resource discovery

- Simple Notification Service (SNS)
- Linux subscriptions
- User-based subscriptions
  - Amazon Managed Microsoft AD
  - Virtual private cloud
- Delegated administrators
  - Regions supported for delegated administrators
  - Register a delegated administrator
  - Deregister a delegated administrator

Managed licenses

The following settings are available for managed licenses.

Account details

You can review your account details to see information such as the account type, whether accounts in Amazon Organizations are linked, the account's License Manager S3 bucket ARN, and the Amazon Resource Access Manager share ARN. This section also enables you to link your Amazon Organizations accounts.

To distribute managed entitlements or self-managed licenses within your organization, choose **Link Amazon Organizations accounts**. The distributed grants for managed entitlements are auto-accepted by all of your member accounts. When you select this option, we add a service-linked role to the management and member accounts.

> **Note**
>
> To enable this option, you must be signed in to your management account and all features must be enabled in Amazon Organizations. For more information, see Enabling all features in your organization in the *Amazon Organizations User Guide*.
> This selection also creates an Amazon Resource Access Manager resource share in your management account, which allows you to seamlessly share self-managed licenses. For more information, see the Amazon Resource Access Manager User Guide.

To disable this option, call the UpdateServiceSettings API.

Cross-account resource discovery

You can turn on cross-account resource discovery in order to manage license usage across all of your accounts in Amazon Organizations.

To enable cross-account resource discovery in your organization, choose **Turn on** for cross-account resource discovery. When you turn on the cross-account resource discovery, Amazon Organizations will automatically be linked to perform resource discovery across all of your accounts.

License Manager uses Systems Manager inventory to discover software usage. Verify that you have configured Systems Manager inventory on all of your resources. Querying Systems Manager inventory requires the following:

- Resource data sync to store inventory in an Amazon S3 bucket.
- Amazon Athena to aggregate inventory data from your accounts in Amazon Organizations.
- Amazon Glue to provide a fast query experience.

> **Note**
>
> The following Amazon Web Services Regions don't require Amazon Athena or Amazon Glue to query or aggregate inventory data for Systems Manager inventory to discover software usage:
>
> - Asia Pacific (Jakarta)
> - Israel (Tel Aviv)

Simple Notification Service (SNS)

You can configure an Amazon SNS to receive notifications and alerts from License Manager.

To configure an Amazon SNS topic

1. Choose **Edit** next to **Simple Notification Service (SNS)**.
2. Specify an SNS topic ARN in the following format:

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

3. Choose **Save changes**.

Linux subscriptions

You can configure settings for Linux subscriptions to control how the discovery and aggregation of your subscriptions are performed. You can choose the Regions for which you want to discover Linux subscriptions for, and whether you want to aggregate subscription data across your accounts in Amazon Organizations. For more information, see Linux subscriptions in License Manager.

User-based subscriptions

The following settings are available depending on which products you require for user-based subscriptions.

Amazon Managed Microsoft AD

License Manager requires Amazon Managed Microsoft AD to be configured before you can work with user-based subscriptions. For more information, see ???.

Virtual private cloud

License Manager requires your VPC to be configured, in addition to your Amazon Managed Microsoft AD, when you use user-based subscriptions with Microsoft Office. For more information, see ???.

Delegated administrators

You can register a delegated administrator to perform administrative tasks for managed licenses and Linux subscriptions in License Manager. To simplify administration, we recommend using the License Manager console to register a single delegated administrator for each feature of License Manager. Using this approach, you will have a single delegated administrator in your organization for License Manager.

Using the Amazon CLI or SDKs, you can register different member accounts in your organization as the delegated administrator for each supported feature of License Manager. This results in

different member accounts in your organization being able to perform administrative tasks for managed licenses and Linux subscriptions.

> **Important**
>
> To use the delegated administration features in the License Manager console, you must have the same member account registered as the delegated administrator for each feature of License Manager. If you registered more than one member account as the delegated administrator, you first have to deregister the existing member accounts, and then register the same account for each feature of License Manager.

Before you register a delegated administrator, you must enable trusted access with Organizations. For more information, see Inviting an Amazon account to join your organization and Enable trusted access with Amazon Organizations.

The following are the features for which you can register a delegated administrator:

Managed licenses

You can perform administrative tasks, such as sharing self-managed licenses with other member accounts, performing cross-account resource discovery, and distributing managed entitlements to other member accounts.

Linux subscriptions

You can perform administrative tasks, such as viewing and managing commercial Linux subscriptions you own and run across Amazon Web Services Regions and your accounts in Amazon Organizations. You can also create and manage Amazon CloudWatch alarms for your Linux subscriptions. The data must first be discovered and aggregated before it is visible in the License Manager console and any alarms can function if they are configured.

> **Important**
>
> Once registered, the delegated administrator has visibility into EC2 instances owned by accounts in your organization.

You can register and deregister delegated administrators using the Amazon License Manager console, Amazon CLI, or Amazon SDKs.

Regions supported for delegated administrators

The following Regions support License Manager delegated administrators:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Asia Pacific (Hong Kong)
- Middle East (Bahrain)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- Europe (Milan)
- Africa (Cape Town)
- South America (São Paulo)

Register a delegated administrator

You can register a delegated administrator using the Amazon CLI or Amazon Web Services Management Console.

Console

To register a delegated administrator using the Amazon License Manager console, perform the following steps:

1. Sign in to Amazon as the administrator of the management account.
2. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
3. Choose **Settings** from the left navigation pane.
4. Choose the **Delegated administration** tab.
5. Choose **Register delegated administrator**.
6. Enter the member account ID to register as the delegated administrator, confirm that you want to grant License Manager the required permissions, and then choose **Register**.
7. A message indicates if the specified account has been successfully registered as the delegated administrator License Manager.

Amazon CLI

To register a delegated administrator for managed licenses using the Amazon CLI, perform the following steps:

1. From the command line, run the following Amazon CLI command:

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

2. Run the following command to verify that the specified account is successfully registered as the delegated administrator:

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

To register a delegated administrator for Linux subscriptions using the Amazon CLI, perform the following steps:

1. From the command line, run the following Amazon CLI command:

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

2. Run the following command to verify that the specified account is successfully registered as the delegated administrator:

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

Deregister a delegated administrator

You can deregister a delegated administrator using the Amazon CLI or Amazon Web Services Management Console.

Console

To deregister a delegated administrator using the Amazon License Manager console, perform the following steps:

1. Sign in to Amazon as the administrator of the management account.
2. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
3. Choose **Settings** from the left navigation pane.
4. Choose the **Delegated administration** tab.
5. Choose **Remove**.
6. Enter the text **`remove`** to confirm you would like to remove the delegated administrator for License Manager and choose **Remove**.
7. A message indicates if the specified account has been successfully removed the delegated administrator for License Manager.

Amazon CLI

To deregister a delegated administrator for managed licenses using the Amazon CLI, perform the following steps:

1. From the command line, run the following Amazon CLI command:

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

2. Run the following command to verify that the specified account is successfully deregistered as the delegated administrator:

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

To deregister a delegated administrator for Linux subscriptions using the Amazon CLI, perform the following steps:

1. From the command line, run the following Amazon CLI command:

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

2. Run the following command to verify that the specified account is successfully deregistered as the delegated administrator:

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

You can register a deregistered account again at any time.

Dashboard in Amazon License Manager

The **Dashboard** section of the License Manager console provides usage details to track the license consumption associated with each self-managed license, granted license entitlements, subscribed users of user-based subscriptions, and running instances. The dashboard also displays alerts resulting from license rule violations.

Overview

The overview section provides the following details about your licenses.

Granted licenses

The total amount of granted licenses in this account in this Region.

Self-managed licenses

The total amount of self-managed licenses in this account in this Region.

Seller-issued licenses

The total amount of seller-issued licenses in this account in this Region.

Products

The products section provides the following details for user-based subscriptions.

Product name

The name product of the user-based subscription.

Subscribed users

The amount of subscribed users for the product.

Granted license entitlements

The granted license entitlements section provides the following details.

Product name

The product name of the granted license.

Entitlement

The name of the entitlement.

Usage

The utilization of the entitlement.

Self-managed licenses

The self-managed licenses provides following details.

License name

The name of the self-managed license.

Entitlement

The name of the entitlement.

Usage

The utilization of the entitlement.

Instance usage

The instance usage section provides the following details.

Running instance count

The total amount of running instances in this account in this Region.

Aggregate running instance count

The total amount of running instances aggregated across all of your accounts in Amazon Organizations in this Region. This graph is only visible from the management account and delegated administrator account.

Monitoring Amazon License Manager

You can monitor the usage of licenses and subscriptions tracked in Amazon License Manager using Amazon CloudWatch. CloudWatch collects raw data and processes it into readable, near real-time metrics. You can set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see Monitoring license usage with Amazon CloudWatch.

You can capture API calls and related events made by or on behalf of your Amazon Web Services account using Amazon CloudTrail. Events are captured as log files and delivered to an Amazon S3 bucket that you specify. You can identify which users and accounts called Amazon, the source IP address from which the calls were made, and when the calls occurred. For more information, see Logging Amazon License Manager API calls using Amazon CloudTrail.

Contents

Monitoring license usage with Amazon CloudWatch

You can monitor metric statistics for License Manager using Amazon CloudWatch. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your web application or service is performing. You can set alarms that watch for certain thresholds and send notifications or take actions when those thresholds are met. For example, you can watch for the percentage of licenses using the `LicenseConfigurationUsagePercentage` metric, and take action before limits are exceeded. For more information, see the Amazon CloudWatch User Guide.

License Manager emits the following metrics hourly in the `AWSLicenseManager/licenseUsage` namespace:

Metric	Description
RunningInstancesCount	The total number of instances running in the current account that are grouped by the subscription name. Units: Count Dimensions: `SubscriptionName` : The name of the subscription.
AggregateRunningInstancesCount	The aggregated total number of instances that are running across all of your accounts in Amazon Organizations in the current Amazon Web Services Region. Units: Count Dimensions: `SubscriptionName` : The name of the subscription.
TotalLicenseConfigurationUsageCount	The total number of a license configuration that could be available. Units: Count Dimensions: • `LicenseConfigurationArn` : The license configuration Amazon Resource Name (ARN). • `LicenseConfigurationType` : The license configuration type.
LicenseConfigurationUsageCount	The total number of used licenses of this configuration. Units: Count Dimensions: • `LicenseConfigurationArn` : The license configuration ARN. • `LicenseConfigurationType` : The license configuration type.

Metric	Description
LicenseConfigurationUsagePercentage	The used licenses of this license configuration expressed as a percentage. Units: Percent Dimensions: • `LicenseConfigurationArn` : The license configuration ARN. • `LicenseConfigurationType` : The license configuration type.

Creating alarms to monitor License Manager metrics

You can create a CloudWatch alarm that sends an Amazon Simple Notification Service (Amazon SNS) message when the value of the metric changes and causes the alarm to change state. An alarm watches a metric over a time period you specify, and performs actions based on the value of the metric relative to a given threshold over a number of time periods. Alarms invoke actions for sustained state changes only. CloudWatch alarms do not invoke actions simply because they are in a particular state; the state must have changed and been maintained for a specified number of periods. For more information, see Using CloudWatch alarms.

Logging Amazon License Manager API calls using Amazon CloudTrail

Amazon License Manager is integrated with Amazon CloudTrail, a service that provides a record of actions taken by a user, role, or an Amazon service in License Manager. CloudTrail captures all API calls for License Manager as events. The calls captured include calls from the License Manager console and code calls to the License Manager API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for License Manager. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to License Manager, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the Amazon CloudTrail User Guide.

License Manager information in CloudTrail

CloudTrail is enabled on your Amazon account when you create the account. When activity occurs in License Manager, that activity is recorded in a CloudTrail event along with other Amazon service events in **Event history**. You can view, search, and download recent events in your Amazon account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your Amazon account, including events for License Manager, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all Amazon Regions. The trail logs events from all Regions in the Amazon partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other Amazon services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All License Manager actions are logged by CloudTrail and are documented in the License Manager API Reference. For example, calls to the `CreateLicenseConfiguration`, `ListResourceInventory` and `DeleteLicenseConfiguration` actions generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or Amazon Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another Amazon service.

For more information, see the CloudTrail userIdentity Element.

Understanding License Manager log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `DeleteLicenseConfiguration` action.


```
{
   "eventVersion":"1.05",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"AIDAIF2U5EXAMPLEH5AP6",
      "arn":"arn:aws:iam::123456789012:user/Administrator",
      "accountId":"012345678901",
      "accessKeyId":"AKIDEXAMPLE",
      "userName":"Administrator"
   },
   "eventTime":"2019-02-15T06:48:37Z",
   "eventSource":"license-manager.amazonaws.com",
   "eventName":"DeleteLicenseConfiguration",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.83",
   "userAgent":"aws-cli/2.4.6 Python/3.8.8 Linux",
   "requestParameters":{
      "licenseConfigurationArn":"arn:aws:license-manager:us-
east-1:123456789012:license-configuration:lic-9ab477f4bEXAMPLE55f3ec08a5423f77"
   },
   "responseElements":null,
   "requestID":"3366df5f-4166-415f-9437-c38EXAMPLE48",
   "eventID":"6c2c949b-1a81-406a-a0d7-52EXAMPLE5bd",
   "eventType":"AwsApiCall",
   "recipientAccountId":"012345678901"
}
```

Security in Amazon License Manager

Cloud security at Amazon is the highest priority. As an Amazon customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between Amazon and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – Amazon is responsible for protecting the infrastructure that runs Amazon services in the Amazon Cloud. Amazon also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the Amazon Compliance Programs. To learn about the compliance programs that apply to License Manager, see Amazon Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the Amazon service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations

This documentation helps you understand how to apply the shared responsibility model when using License Manager. It shows you how to configure License Manager to meet your security and compliance objectives. You also learn how to use other Amazon services that help you to monitor and secure your License Manager resources.

Contents

Data protection in Amazon License Manager

The Amazon shared responsibility model applies to data protection in Amazon License Manager. As described in this model, Amazon is responsible for protecting the global infrastructure that runs all of the Amazon Web Services Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the Amazon Web Services that you use. For more information about data privacy, see the Data Privacy FAQ.

For data protection purposes, we recommend that you protect Amazon Web Services account credentials and set up individual users with Amazon IAM Identity Center or Amazon Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with Amazon resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with Amazon CloudTrail.
- Use Amazon encryption solutions, along with all default security controls within Amazon Web Services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing Amazon through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with License Manager or other Amazon Web Services using the console, API, Amazon CLI, or Amazon SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Encryption at rest

License Manager stores data in an Amazon S3 bucket in the management account. The bucket is configured using Amazon S3 managed encryption keys (SSE-S3).

Identity and access management for Amazon License Manager

Amazon Identity and Access Management (IAM) is an Amazon service that helps an administrator securely control access to Amazon resources. IAM administrators control who can be authenticated (signed in) and authorized (have permissions) to use Amazon resources. With IAM you can create users and groups under your Amazon account. You control the permissions that users have to perform tasks using Amazon resources. You can use IAM for no additional charge.

By default, users don't have permissions for License Manager resources and operations. To allow users to manage License Manager resources, you must create an IAM policy that explicitly grants them permissions.

When you attach a policy to a user or group of users, it allows or denies the users permission to perform the specified tasks on the specified resources. For more information, see Policies and Permissions in the *IAM User Guide* guide.

Create users, groups, and roles

You can create users and groups for your Amazon Web Services account and then assign them the permissions they require. As a best practice, users should acquire the permissions by assuming IAM roles. For more information on how to set up users and groups for your Amazon Web Services account, see Getting started with Amazon License Manager.

An IAM role is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user in that it is an Amazon identity with permissions policies that determine what the identity can and cannot do in Amazon. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session.

IAM policy structure

An IAM policy is a JSON document that consists of one or more statements. Each statement is structured as follows.

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

Various elements make up a statement:

- **Effect:** The *effect* can be `Allow` or `Deny`. By default, users don't have permission to use resources and API operations, so all requests are denied. An explicit *allow* overrides the default. An explicit *deny* overrides any allows.
- **Action**: The *action* is the specific API operation for which you are granting or denying permission.
- **Resource**: The resource is affected by the action. Some License Manager API operations allow you to include specific resources in your policy that can be created or modified by the operation. To specify a resource in the statement, you need to use its Amazon Resource Name (ARN). For more information, see Actions Defined by Amazon License Manager.
- **Condition**: Conditions are optional. They can be used to control when your policy is in effect. For more information, see Condition Keys for Amazon License Manager.

Create IAM policies for License Manager

In an IAM policy statement, you can specify any API operation from any service that supports IAM. License Manager, uses the following prefixes with the name of the API operation:

- `license-manager:`

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

For example:

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

For more information on the available License Manager APIs, see the following API references:

- Amazon License Manager API Reference
- Amazon License Manager User Subscriptions API Reference
- Amazon License Manager Linux Subscriptions API Reference

To specify multiple operations in a single statement, separate them with commas as follows:

```
"Action": ["license-manager:action1", "license-manager:action2"]
```

You can also specify multiple operations using wildcards. For example, you can specify all License Manager API operations whose name begins with the word *List* as follows:

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

To specify all License Manager API operations, use the * wildcard as follows:

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

Example policy for an ISV using License Manager

ISVs that distribute licenses through License Manager require the following permissions:

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

Grant permissions to users, groups, and roles

Once you have created the IAM policies you require, you must grant these permissions to your users, groups, and roles.

To provide access, add permissions to your users, groups, or roles:

- Users managed in IAM through an identity provider:

  Create a role for identity federation. Follow the instructions in Creating a role for a third-party identity provider (federation) in the *IAM User Guide*.
- IAM users:
  - Create a role that your user can assume. Follow the instructions in Creating a role for an IAM user in the *IAM User Guide*.
  - (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in Adding permissions to a user (console) in the *IAM User Guide*.

Using service-linked roles for Amazon License Manager

Amazon License Manager uses Amazon Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to License Manager. Service-

linked roles are predefined by License Manager and include all the permissions that the service requires to call other Amazon services on your behalf.

A service-linked role makes setting up License Manager easier because you don't have to manually add the necessary permissions. License Manager defines the permissions of its service-linked roles, and unless defined otherwise, only License Manager can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting the related resources. This protects your License Manager resources because you can't inadvertently remove permissions to access the resources.

License Manager actions depend on three service-linked roles, as described in the following sections.

Service-linked roles

- License Manager – Core role
- License Manager – Management account role
- License Manager – Member account role

License Manager – Core role

License Manager requires a service-linked role to manage licenses on your behalf.

Permissions for the core role

The service-linked role named `AWSServiceRoleForAWSLicenseManagerRole` allows License Manager access to Amazon resources to manage licenses on your behalf.

The `AWSServiceRoleForAWSLicenseManagerRole` service-linked role trusts the `license-manager.amazonaws.com` service to assume the role.

To review permissions for the **AWSLicenseManagerServiceRolePolicy**, see Amazon managed policy: AWSLicenseManagerServiceRolePolicy. To learn more about configuring permissions for a service-linked role, see Service-Linked Role Permissions in the *IAM User Guide*.

Create a service-linked role for License Manager

You don't need to manually create a service-linked role. When you complete the License Manager first-run experience form the first time that you visit the License Manager console, the service-linked role is automatically created for you.

You can also use the IAM console, Amazon CLI, or IAM API to create a service-linked role manually. For more information, see Creating a Service-Linked Role in the *IAM User Guide*.

> **Important**
>
> This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. If you were using License Manager before January 1, 2017, when it began supporting service-linked roles, then License Manager created the `AWSServiceRoleForAWSLicenseManagerRole` role in your account. For more information, see A New Role Appeared in My IAM Account.

You can use the License Manager console to create a service-linked role.

To create the service-linked role

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. Choose **Start using License Manager**.
3. In the **IAM Permissions (one-time-setup)** form, select **I grant Amazon License Manager the required permissions**, then choose **Continue**.

You can also use the IAM console to create a service-linked role with the **License Manager** use case. Alternatively, in the Amazon CLI or the Amazon API, use IAM to create a service-linked role with the `license-manager.amazonaws.com` service name. For more information, see Creating a Service-Linked Role in the *IAM User Guide*.

If you delete this service-linked role, you can use the same IAM process to create the role again.

Edit a service-linked role for License Manager

License Manager doesn't allow you to edit the `AWSServiceRoleForAWSLicenseManagerRole` service-linked role. After you create a service-linked role, you cannot change the name of the role

because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Delete a service-linked role for License Manager

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way, you only have entities that are actively monitored or maintained. However, you must clean up your service-linked role before you can manually delete it.

Clean up a service-linked role

Before you can use IAM to delete a service-linked role, you must first delete all resources used by the role. This means disassociating any self-managed licenses from associated instances and AMIs, and then deleting the self-managed licenses.

> **Note**
>
> If License Manager is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the action again.

To delete License Manager resources used by the core role

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. In the navigation pane, choose **Self-managed licenses**.
3. Choose a self-managed license for which you are the owner and disassociate all entries within the **Associated AMIs** and **Resources** tabs. Repeat this process for each license configuration.
4. While still on the self-managed license's page, choose **Actions**, then choose **Delete**.
5. Repeat the previous steps until all self-managed licenses have been deleted.

Manually delete the service-linked role

Use the IAM console, the Amazon CLI, or the Amazon API to delete the `AWSServiceRoleForAWSLicenseManagerRole` service-linked role. If you are also using AWSServiceRoleForAWSLicenseManagerMasterAccountRole and AWSLicenseManagerMemberAccountRole, delete those roles first. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

License Manager – Management account role

License Manager requires a service-linked role to perform license management.

Permissions for the management account role

The service-linked role named `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` allows License Manager access to Amazon resources to manage license management actions for a central management account on your behalf.

The `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` service-linked role trusts the `license-manager.master-account.amazonaws.com` service to assume the role.

To review permissions for the **AWSLicenseManagerMasterAccountRolePolicy**, see Amazon managed policy: AWSLicenseManagerMasterAccountRolePolicy. To learn more about configuring permissions for a service-linked role, see Service-Linked Role Permissions in the *IAM User Guide*.

Create a management account service-linked role

You don't need to manually create this service-linked role. When you configure cross-account license management in the Amazon Web Services Management Console, License Manager creates the service-linked role for you.

> **Note**
>
> To make use of cross-account support in License Manager, you must be using Amazon Organizations.

If you delete this service-linked role and then need to create it again, you can use the same process to recreate the role in your account.

You can also use the IAM console, Amazon CLI, or IAM API to create a service-linked role manually. For more information, see Creating a Service-Linked Role in the *IAM User Guide*.

> **Important**
>
> This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. If you were using License Manager before January 1, 2017, when it began supporting service-linked roles, then License

Manager created `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` in your account. For more information, see A New Role Appeared in My IAM Account.

You can use the License Manager console to create this service-linked role.

To create the service-linked role

1. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
2. Choose **Settings**, **Edit**.
3. Choose **Link Amazon Organizations accounts**.
4. Choose **Apply**.

You can also use the IAM console to create a service-linked role with the License Manager–Management account use case. Alternatively, in the Amazon CLI or the Amazon API, use IAM to create a service-linked role with the `license-manager.master-account.amazonaws.com` service name. For more information, see Creating a Service-Linked Role in the *IAM User Guide*.

If you delete this service-linked role, you can use the same IAM process to create the role again.

Edit a service-linked role for License Manager

License Manager does not allow you to edit the `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Delete a service-linked role for License Manager

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way, you only have entities that are actively monitored or maintained. However, you must clean up your service-linked role before you can manually delete it.

Manually delete the service-linked role

Use the IAM console, Amazon CLI, or Amazon API to delete the `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

License Manager – Member account role

License Manager requires a service-linked role that allows the management account to manage licenses.

Permissions for the member account role

The service-linked role named `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` allows License Manager to access Amazon resources for license management actions from a configured management account on your behalf.

The `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` service-linked role trusts the `license-manager.member-account.amazonaws.com` service to assume the role.

To review permissions for the **AWSLicenseManagerMemberAccountRolePolicy**, see Amazon managed policy: AWSLicenseManagerMemberAccountRolePolicy. To learn more about configuring permissions for a service-linked role, see Service-Linked Role Permissions in the *IAM User Guide*.

Create the service-linked role for License Manager

You don't need to manually create the service-linked role. You can enable integration with Amazon Organizations from the management account in the License Manager console on the **Settings** page. You can also do this using the Amazon CLI (run `update-service-settings`) or the Amazon API (call `UpdateServiceSettings`). When you do, License Manager creates the service-linked role for you in the Organizations member accounts.

If you delete this service-linked role and then need to create it again, you can use the same process to recreate the role in your account.

You can also use the IAM console, Amazon CLI, or the Amazon API to create a service-linked role manually. For more information, see Creating a Service-Linked Role in the *IAM User Guide*.

> **Important**
>
> This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. If you were using the License Manager service before January 1, 2017, when it began supporting service-linked roles, then License Manager created the `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` role in your account. For more information, see A New Role Appeared in My IAM Account.

You can use the License Manager console to create a service-linked role.

To create the service-linked role

1. Log in to your Amazon Organizations management account.
2. Open the License Manager console at https://console.amazonaws.cn/license-manager/.
3. In the left navigation pane, choose **Settings**, and then choose **Edit**.
4. Choose **Link Amazon Organizations accounts**.
5. Choose **Apply**. This creates the roles AWSServiceRoleForAWSLicenseManagerRole and AWSServiceRoleForAWSLicenseManagerMemberAccountRole in all child accounts.

You can also use the IAM console to create a service-linked role with the `License Manager - Member account` use case. Alternatively, in the Amazon CLI or Amazon API, create a service-linked role with the `license-manager.member-account.amazonaws.com` service name. For more information, see Creating a Service-Linked Role in the *IAM User Guide*.

If you delete this service-linked role, you can use the same IAM process to create the role again.

Edit a service-linked role for License Manager

License Manager does not allow you to edit the `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Delete a service-linked role for License Manager

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way, you only have entities that are actively monitored or maintained. However, you must clean up your service-linked role before you can manually delete it.

Manually delete the service-linked role

Use the IAM console, Amazon CLI, or Amazon API to delete the `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Amazon managed policies for Amazon License Manager

To add permissions to users, groups, and roles, it is easier to use Amazon managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our Amazon managed policies. These policies cover common use cases and are available in your Amazon account. For more information about Amazon managed policies, see Amazon managed policies in the *IAM User Guide*.

Amazon services maintain and update Amazon managed policies. You can't change the permissions in Amazon managed policies. Services occasionally add additional permissions to an Amazon managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an Amazon managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an Amazon managed policy, so policy updates won't break your existing permissions.

Additionally, Amazon supports managed policies for job functions that span multiple services. For example, the `ReadOnlyAccess` Amazon managed policy provides read-only access to all Amazon services and resources. When a service launches a new feature, Amazon adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see Amazon managed policies for job functions in the *IAM User Guide*.

Amazon managed policy: AWSLicenseManagerServiceRolePolicy

This policy is attached to the service-linked role named `AWSServiceRoleForAWSLicenseManagerRole` to allow License Manager to call API actions to manage licenses on your behalf. For more information about the service-linked role, see Permissions for the core role.

The role permissions policy allows License Manager to complete the following actions on the specified resources.

Action	Resource ARN
`iam:CreateServiceLinkedRole`	`arn:aws-cn:iam::*:role/aws-service-role/license-management.mark`

Action	Resource ARN
	etplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement
iam:CreateServiceLinkedRole	arn:aws-cn:iam::*:role/aws-service-role/license-manager.member-account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole
s3:GetBucketLocation	arn:aws-cn:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws-cn:s3:::aws-license-manager-service-*
s3:ListAllMyBuckets	*
s3:PutObject	arn:aws-cn:s3:::aws-license-manager-service-*
sns:Publish	arn:aws-cn::sns:*:*:aws-license-manager-service-*
sns:ListTopics	*
ec2:DescribeInstances	*
ec2:DescribeImages	*
ec2:DescribeHosts	*

Action	Resource ARN
ssm:ListInventoryEntries	*
ssm:GetInventory	*
ssm:CreateAssociation	*
organizations:ListAWSServiceAccessForOrganization	*
organizations:DescribeOrganization	*
organizations:ListDelegatedAdministrators	*
license-manager:GetServiceSettings	*
license-manager:GetLicense*	*
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:List*	*

To view the permissions for this policy in the Amazon Web Services Management Console, see AWSLicenseManagerServiceRolePolicy.

Amazon managed policy: AWSLicenseManagerMasterAccountRolePolicy

This policy is attached to the service-linked role named AWSServiceRoleForAWSLicenseManagerMasterAccountRole to allow License Manager to call API actions that perform license management for a central management account on your behalf. For more information about the service-linked role, see License Manager – Management account role.

The role permissions policy allows License Manager to complete the following actions on the specified resources.

Action	Resource ARN
s3:GetBucketLocation	arn:aws-cn:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws-cn:s3:::aws-license-manager-service-*
s3:GetLifecycleConfiguration	arn:aws-cn:s3:::aws-license-manager-service-*
s3:PutLifecycleConfiguration	arn:aws-cn:s3:::aws-license-manager-service-*
s3:GetBucketPolicy	arn:aws-cn:s3:::aws-license-manager-service-*
s3:PutBucketPolicy	arn:aws-cn:s3:::aws-license-manager-service-*
s3:AbortMultipartUpload	arn:aws-cn:s3:::aws-license-manager-service-*
s3:PutObject	arn:aws-cn:s3:::aws-license-manager-service-*
s3:GetObject	arn:aws-cn:s3:::aws-license-manager-service-*

Action	Resource ARN
s3:ListBucketMultipartUploads	arn:aws-cn:s3:::aws-license-manager-service-*
s3:ListMultipartUploadParts	arn:aws-cn:s3:::aws-license-manager-service-*
s3:DeleteObject	arn:aws-cn:s3:::aws-license-manager-service-*/resource-sync/*
athena:GetQueryExecution	*
athena:GetQueryResults	*
athena:StartQueryExecution	*
glue:GetTable	*
glue:GetPartition	*
glue:GetPartitions	*
glue:CreateTable	See footnote [1]
glue:UpdateTable	See footnote [1]
glue:DeleteTable	See footnote [1]
glue:UpdateJob	See footnote [1]
glue:UpdateCrawler	See footnote [1]
organizations:DescribeOrganization	*
organizations:ListAccounts	*
organizations:DescribeAccount	*

Action	Resource ARN
organizations:ListChildren	*
organizations:ListParents	*
organizations:ListAccountsForParent	*
organizations:ListRoots	*
organizations:ListAWSServiceAccessForOrganization	*
ram:GetResourceShares	*
ram:GetResourceShareAssociations	*
ram:TagResource	*
ram:CreateResourceShare	*
ram:AssociateResourceShare	*
ram:DisassociateResourceShare	*
ram:UpdateResourceShare	*
ram:DeleteResourceShare	*
resource-groups:PutGroupPolicy	*
iam:GetRole	*
iam:PassRole	arn:aws-cn:iam::*:role/LicenseManagerServiceResourceDataSyncRole*

Action	Resource ARN
cloudformation:UpdateStack	arn:aws-cn:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:CreateStack	arn:aws-cn:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:DeleteStack	arn:aws-cn:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:DescribeStacks	arn:aws-cn:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*

[1] The following are the resources defined for the Amazon Glue actions:

- 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

To view the permissions for this policy in the Amazon Web Services Management Console, see AWSLicenseManagerMasterAccountRolePolicy.

Amazon managed policy: AWSLicenseManagerMemberAccountRolePolicy

This policy is attached to the service-linked role named `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` to allow License Manager to call API actions for license management from a configured management account on your behalf. For more information, see License Manager – Member account role.

The role permissions policy allows License Manager to complete the following actions on the specified resources.

Action	Resource ARN
`license-manager:UpdateLicenseSpecificationsForResource`	*
`license-manager:GetLicenseConfiguration`	*
`ssm:ListInventoryEntries`	*
`ssm:GetInventory`	*
`ssm:CreateAssociation`	*
`ssm:CreateResourceDataSync`	*
`ssm:DeleteResourceDataSync`	*
`ssm:ListResourceDataSync`	*
`ssm:ListAssociations`	*
`ram:AcceptResourceShareInvitation`	*
`ram:GetResourceShareInvitations`	*

To view the permissions for this policy in the Amazon Web Services Management Console, see AWSLicenseManagerMemberAccountRolePolicy.

Amazon managed policy: AWSLicenseManagerConsumptionPolicy

You can attach the `AWSLicenseManagerConsumptionPolicy` policy to your IAM identities. This policy grants permissions that allow access to the License Manager API actions required to consume licenses. For more information, see License usage.

To view the permissions for this policy, see AWSLicenseManagerConsumptionPolicy in the Amazon Web Services Management Console.

License Manager updates to Amazon managed policies

View details about updates to Amazon managed policies for License Manager since this service began tracking these changes.

Change	Description	Date
AWSLicenseManagerMasterAccountRolePolicy – Update to an existing policy	License Manager added the `resource-groups:PutGroupPolicy` permission for resource groups managed by Amazon Resource Access Manager.	June 27, 2022
AWSLicenseManagerMasterAccountRolePolicy – Update to an existing policy	License Manager changed the Amazon managed policy `AWSLicenseManagerMasterAccountRolePolicy` condition key for Amazon Resource Access Manager from using `ram:ResourceTag` to `aws:ResourceTag`.	November 16, 2021

Change	Description	Date
AWSLicenseManagerConsumptionPolicy – New policy	License Manager added a new policy that grants permissions to consume licenses.	August 11, 2021
AWSLicenseManagerServiceRolePolicy – Update to an existing policy	License Manager added a permission to list delegated administrators and a permission to create the service-linked role named `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` .	June 16, 2021
AWSLicenseManagerServiceRolePolicy – Update to an existing policy	License Manager added a permission to list all License Manager resources, such as license configurations, licenses, and grants.	June 15, 2021
AWSLicenseManagerServiceRolePolicy – Update to an existing policy	License Manager added a permission to create the service-linked role named `AWSServiceRoleForMarketplaceLicenseManagement` . This role provides Amazon Web Services Marketplace with permissions to create and manage licenses in License Manager. For more information, see Service-linked roles for Amazon Web Services Marketplace in the *Amazon Web Services Marketplace Buyer Guide*.	March 9, 2021

Change	Description	Date
License Manager started tracking changes	License Manager started tracking changes to its Amazon managed policies.	March 9, 2021

Cryptographic Signing of Licenses

License Manager can cryptographically sign licenses issued by an ISV or through Amazon Web Services Marketplace on behalf of an ISV. Signing permits vendors to validate the integrity and origin of a license within the application itself, even in an offline environment.

To sign licenses, License Manager uses an asymmetric Amazon KMS key belonging to an ISV and protected in Amazon Key Management Service (Amazon KMS). This customer managed CMK consists of a mathematically related public key and private key pair. When a user requests a license, License Manager generates a JSON object listing the license entitlements, and signs this object with the private key. The signature and the plaintext JSON object are returned to the user. Any party presented with these objects can use the public key to validate that the text of the license has not been altered and that the license was signed by the owner of the private key. The private part of the key pair never leaves Amazon KMS. For more information about asymmetric cryptography in Amazon KMS, see Using symmetric and asymmetric keys.

> **Note**
>
> License Manager calls the Amazon KMS `Sign` and `Verify` API operations when signing and verifying licenses. The CMK must have a key usage value of SIGN_VERIFY for it to be used by these operations. This variety of CMK cannot be used for encryption and decryption.

The following workflow describes the issuance of cryptographically signed licenses:

1. In the Amazon KMS console, API, or SDK, the license administrator creates an asymmetric customer managed CMK. The CMK must have a key usage of sign and verify, and support the RSASSA-PSS SHA-256 signing algorithm. For more information, see Creating asymmetric CMKs and How to choose your CMK configuration.

2. In License Manager, the license administrator creates a consumption configuration that includes an Amazon KMS ARN or ID. The configuration may specify either or both the **Borrow** and **Provisional** options. For more information, see Creating a block of seller issued licenses.
3. An end-user obtains the license using the `CheckoutLicense` or `CheckoutBorrowLicense` API operation. The `CheckoutBorrowLicense` operation is allowed only on licenses with **Borrow** configured. It returns a digital signature as part of its response along with the JSON object listing entitlements. The plaintext JSON resembles the following:

```
{
   "entitlementsAllowed":[
      {
         "name":"EntitlementCount",
         "unit":"Count",
         "value":"1"
      }
   ],
   "expiration":"2020-12-01T00:47:35",
   "issuedAt":"2020-11-30T23:47:35",
   "licenseArn":"arn:aws:license-
manager::123456789012:license:l-6585590917ad46858328ff02dEXAMPLE",
   "licenseConsumptionToken":"306eb19afd354ba79c3687b9bEXAMPLE",
   "nodeId":"100.20.15.10",
   "checkoutMetadata":{
      "Mac":"ABCDEFGHI"
   }
}
```

Compliance validation for Amazon License Manager

To learn whether an Amazon Web Service is within the scope of specific compliance programs, see Amazon Web Services in Scope by Compliance Program and choose the compliance program that you are interested in. For general information, see Amazon Web Services Compliance Programs.

You can download third-party audit reports using Amazon Artifact. For more information, see Downloading Reports in Amazon Artifact.

Your compliance responsibility when using Amazon Web Services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. Amazon provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on Amazon that are security and compliance focused.
- Amazon Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *Amazon Config Developer Guide* – The Amazon Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- Amazon Security Hub – This Amazon Web Service provides a comprehensive view of your security state within Amazon. Security Hub uses security controls to evaluate your Amazon resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see Security Hub controls reference.

Resilience in Amazon License Manager

The Amazon global infrastructure is built around Amazon Regions and Availability Zones. Regions provide multiple physically separated and isolated Availability Zones, which are connected through low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about Amazon Regions and Availability Zones, see Amazon Global Infrastructure.

Infrastructure security in Amazon License Manager

As a managed service, Amazon License Manager is protected by Amazon global network security. For information about Amazon security services and how Amazon protects infrastructure, see Amazon Cloud Security. To design your Amazon environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar Amazon Well-Architected Framework*.

You use Amazon published API calls to access License Manager through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.

- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the Amazon Security Token Service (Amazon STS) to generate temporary security credentials to sign requests.

Amazon License Manager and interface VPC endpoints (Amazon PrivateLink)

You can establish a private connection between your virtual private cloud (VPC) and Amazon License Manager by creating an interface VPC endpoint. Interface endpoints are powered by Amazon PrivateLink, a technology that you can use to privately access the License Manager API without an internet gateway, NAT device, VPN connection, or Amazon Direct Connect connection. Instances in your VPC don't need public IP addresses to communicate with License Manager. Traffic between your VPC and License Manager does not leave the Amazon network.

Each interface endpoint is represented by one or more Elastic Network Interfaces in your subnets.

For more information, see Interface VPC endpoints (Amazon PrivateLink) in the *Amazon VPC User Guide*.

Create an interface VPC endpoint for License Manager

Create an interface endpoint for License Manager using one of the following service names:

- **com.amazonaws.*region*.license-manager**
- **com.amazonaws.*region*.license-manager-fips**

If you enable private DNS for the endpoint, you can make API requests to License Manager using its default DNS name for the Region. For example, `license-manager.*region*.amazonaws.com`.

For more information, see Creating an Interface Endpoint in the *Amazon VPC User Guide*.

Create a VPC endpoint policy for License Manager

You can attach a policy to your VPC endpoint to control access to License Manager. The policy specifies the following information:

- The principal that can perform actions
- The actions that can be performed
- The resource on which the actions can be performed

The following is an example of an endpoint policy for License Manager. When attached to an endpoint, this policy grants access to the specified License Manager actions for all principals on all resources.

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

For more information, see Controlling access to services using VPC endpoints in the *Amazon VPC User Guide*.

Troubleshooting Amazon License Manager

The following information can help you troubleshoot issues when using Amazon License Manager. Before you start, confirm that your License Manager setup meets the requirements stated in Settings in Amazon License Manager.

Cross-account discovery error

While setting up cross-account discovery, you may encounter the following error message on the **Inventory search** page:

Athena Exception: Athena Query failed because - Insufficient permissions to execute the query. Please migrate your Catalog to enable access to this database.

This can occur if your Athena service uses the Athena-managed data catalog rather than the Amazon Glue Data Catalog. For upgrade instructions, see Upgrading to the Amazon Glue Data Catalog Step-by-Step.

Management account cannot disassociate resources from a self-managed license

If a member account of an Organization deletes the `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` Service Linked Role (SLR) in its account, and there are member-owned resources associated with a self-managed license, the management account is prevented from disassociating licenses from those member-account resources. This means that the member account resources will continue to consume licenses from the management account pool. To allow the management account to disassociate resources, restore the SLR.

This behavior accounts for cases when a customer prefers not to allow the management account to perform some actions affecting member-account resources.

Systems Manager Inventory is out of date

Systems Manager stores data in its Inventory data for 30 days. During this period, License Manager counts a managed instance as active even if it is not pingable. After inventory data has been purged from Systems Manager, License Manager marks the instance as inactive and updates local

inventory data. To keep managed instance counts accurate, we recommend manually deregistering instances in Systems Manager so that License Manager can run cleanup operations.

Apparent persistence of a de-registered AMI

License Manager purges stale associations between resources and self-managed licenses once every few hours. If an AMI associated with a self-managed license is deregistered through Amazon EC2, The AMI may briefly continue to appear in the License Manager resource inventory before being purged.

New child account instances are slow to appear in resource inventory

When cross-account support is enabled, License Manager updates customer accounts at 1 PM daily by default. Instances added later in the day show up in the management account resource inventory on the following day. You can change the frequency at which the update script runs by editing the `LicenseManagerResourceSynDataProcessJobTrigger` in the Amazon Glue console for the management account.

After enabling cross-account mode, child account instances are slow to appear

When you enable cross-account mode in License Manager, instances in child accounts may take anywhere from a few minutes to a few hours to appear in the resource inventory. The time depends on the number of child accounts and the number of instances in each child account.

Cross-account discovery cannot be disabled

After an account is configured for cross-account discovery, it is impossible to revert to single-account discovery.

Child account user cannot associate shared self-managed license with an instance

When this occurs and cross-account discovery has been enabled, check for the following:

- The child account has been removed from the organization.
- The child account has been removed from the resource share created in the management account.
- The self-managed license has been removed from the resource share.

Linking Amazon Organizations accounts fails

If the **Settings** page reports this error, it means that an account is not a member of an organization for the following reasons:

- A child account was removed from the organization.
- A customer turned off access to License Manager from organization console of the management account.

Document history for Amazon License Manager

The following table describes the releases of Amazon License Manager.

Change	Description	Date
Added support for Amazon RDS for Db2 vCPU-based BYOL licenses	License Manager added support for Amazon RDS for Db2 vCPU-based BYOL licenses.	March 20, 2024
Added Windows Server 2019 support for Microsoft Office user-based subscriptions	Amazon added support for Windows Server 2019 in the Amazon Machine Images (AMIs) with Amazon-provided licenses for Microsoft Office LTSC Professional Plus 2021 on Amazon EC2.	December 4, 2023
Self-managed (on-premises) domain users can utilize user-based subscriptions	License Manager added support for users in self-managed active directory domain to utilize user-based subscriptions when a trust with your Amazon Managed Microsoft AD directory has been created.	September 6, 2023
License type conversions for Ubuntu LTS subscriptions	License Manager added support for Ubuntu LTS instances to use license type conversion to add a Ubuntu Pro subscription.	April 20, 2023
Replace active grants	License Manager added functionality to optionally replace active grants for a	March 31, 2023

Change	Description	Date
	granted license during grant activation.	
Delegated administration for Linux subscriptions	License Manager added support for delegated administrators for Linux subscriptions.	March 3, 2023
Linux subscriptions	License Manager added tracking for commercial Linux subscriptions.	December 21, 2022
Amazon CloudWatch metrics	License Manager now emits CloudWatch metrics for license configuration usage and subscriptions.	December 21, 2022
Microsoft Office for user-based subscriptions	License Manager added Microsoft Office as supported software for user-based subscriptions.	November 28, 2022
Distribute entitlements to organizational units	Distribute entitlements to specific a specific OU in your organization.	November 17, 2022
Organization wide view (console)	Manage granted licenses across your accounts in Amazon Organizations using the License Manager console.	November 11, 2022
Record and submit license usage data (console)	Record and submit license usage data using the License Manager console.	March 28, 2022

Change	Description	Date
License type conversion (console)	Change your license type between Amazon-provided licensing and Bring Your Own License model (BYOL) using the License Manager console without redeploying your existing workloads.	November 9, 2021
License type conversion (CLI)	Change your license type between Amazon-provided licensing and Bring Your Own License model (BYOL) using the Amazon CLI without redeploying your existing workloads.	September 22, 2021
Sharing entitlements	Share managed license entitlements with your entire organization with one request.	July 16, 2021
Usage reports	Track the history of your license type configurations with License Manager usage reports. Usage reports were formerly called report generators and license reports.	May 18, 2021
Automated discovery exclusion rules	Exclude instances from License Manager automated discovery based on Amazon account IDs and tags.	March 5, 2021

Change	Description	Date
Managed entitlements	Track and distribute license entitlements for products purchased from Amazon Web Services Marketpla ce and sellers who use License Manager to distribute licenses.	December 3, 2020
Automated accounting for uninstalled software	Configure automated discovery to stop tracking instances when software is uninstalled.	December 3, 2020
Tag-based filtering	Search your resource inventory using tags.	December 3, 2020
AMI association scope	Associate your self-managed licenses and the AMIs shared with your Amazon account.	November 23, 2020
License affinity to host	Enforce license assignment to dedicated hardware for a specific number of days.	August 12, 2020
Track Oracle deployments on Amazon RDS	Track license usage for Oracle database engine editions and licensing packs on Amazon RDS.	March 23, 2020
Host resource groups	Configure a host resource group to enable License Manager to manage your Dedicated Hosts.	December 1, 2019

Change	Description	Date
Automated software discovery	Configure License Manager to search for newly installed operating systems or applications and attach the corresponding self-managed licenses to the instances.	December 1, 2019
Differentiate between license included and bring your own license	Filter your search results based on whether you are using licenses provided by Amazon or your own licenses.	November 8, 2019
Attach licenses to on-premises resources	After you attach licenses to an on-premises instance, License Manager periodically collects software inventory, updates licensing information, and reports usage.	March 8, 2019
Amazon License Manager initial release	Initial service launch	November 28, 2018