Guía del usuario

AWS License Manager

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS License Manager: Guía del usuario

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS License Manager? ... 1
Derechos administrados ... 2
Casos de uso de License Manager ... 2
Servicios relacionados ... 3
Cómo funciona License Manager ... 5
Introducción ... 8
Uso de License Manager ... 9
Licencias autoadministradas ... 10
Parámetros y reglas ... 11
Creación de reglas de a partir de las licencias de los proveedores ... 13
Cree una licencia autoadministrada ... 15
Comparta una licencia autoadministrada ... 17
Edite una licencia autoadministrada ... 21
Desactive una licencia autoadministrada ... 22
Elimine una licencia autoadministrada ... 23
Reglas de asignación de licencias ... 23
Asociar licencias autogestionadas y AMIs ... 25
Desasociar las licencias autogestionadas y AMIs ... 26
Informes de uso ... 26
Cree un informe de uso ... 27
Editar un informe de uso ... 28
Eliminar un informe de uso ... 29
Conversiones de tipos de licencia ... 29
Tipos de licencia aptos ... 31
Requisitos previos ... 43
Conversión de un tipo de licencia ... 45
Conversión de tenencias ... 55
Solución de problemas ... 57
Grupos de recursos de host ... 59
Cree un grupo de recursos de host ... 60
Comparta un grupo de recursos de host ... 61
Agregue hosts dedicados a un grupo de recursos de hosts ... 61
Lance una instancia en un grupo de recursos de host ... 62
Modifique un grupo de recursos de host ... 62

Elimine los hosts dedicados de un grupo de recursos de hosts 63
Elimine un grupo de recursos de host 64
Búsqueda en el inventario 64
Trabaje con la búsqueda de inventario 65
Detección automatizada en el inventario 71
Licencias concedidas 73
Visualización de las licencias concedidas 74
Administre las licencias concedidas 75
Distribuya los derechos 78
Aceptación y activación de concesiones 80
Estado de las licencias 82
Métricas para las cuentas de compradores 84
Licencias emitidas por el vendedor 85
Concesiones de derechos 86
Uso de licencias 86
Permisos necesarios 87
Cree licencias emitidas por el vendedor 89
Otorgue licencias emitidas por el vendedor 90
Credenciales temporales para clientes de ISV 91
Consulta las licencias emitidas por el vendedor 92
Eliminar las licencias emitidas por el vendedor 93
Suscripciones basadas en usuarios 94
Consideraciones 95
Cargos de suscripción en License Manager 96
Requisitos previos de una suscripción basada en el usuario 101
Suscripciones de software compatibles 110
Active Directory 112
Software adicional 112
Introducción 113
Configure el GPO para más sesiones 123
Lance una instancia a partir de una licencia incluida (AMI) 124
Conexión a una instancia 125
Modificar la configuración del firewall de Microsoft Office 126
Administre los usuarios de suscripciones 127
Anule el registro de Active Directory 129
Solución de problemas 130

Administre las suscripciones de Linux 133
Configure la detección 135
Ver los datos de la instancia 142
Información de facturación 144
Gestione CloudWatch las alarmas 147
Configuración 149
Editar la configuración de License Manager 151
Configuración de licencias gestionadas 151
Configuración de suscripción a Linux 153
Configuración de suscripción basada en el usuario 156
Configuración de administrador delegado 157
Panel de control 161
Monitoreo de License Manager 164
Monitorización con CloudWatch 164
Creación de CloudWatch alarmas 166
CloudTrail registros 166
Información sobre License Manager en CloudTrail 167
Descripción de las entradas del archivo de registros de License Manager 168
Seguridad 170
Protección de los datos 171
Cifrado en reposo 172
Identity and Access Management 172
Creación de usuarios, grupos y roles 172
Estructura de la política de IAM 173
Cree políticas de IAM para License Manager 174
Concesión de permisos a usuarios, grupos y roles 175
Roles vinculados a servicios 176
Rol principal 177
Rol de cuenta de administración 179
Rol de cuenta miembro 182
Rol de suscripción basada en usuarios 184
Rol de suscripciones de Linux 186
AWS políticas gestionadas 187
AWSLicenseManagerServiceRolePolicy 188
AWSLicenseManagerMasterAccountRolePolicy 190
AWSLicenseManagerMemberAccountRolePolicy 194

AWSLicenseManagerConsumptionPolicy 195
AWSLicenseManagerUserSubscriptionsServiceRolePolicy 196
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 197
Actualizaciones de políticas 199
Firma de licencias 203
Validación de conformidad 205
Resiliencia 206
Seguridad de la infraestructura 206
Terminales de VPC con AWS PrivateLink 207
Creación de un punto de conexión de VPC de interfaz para License Manager 207
Cree una política de punto de conexión de VPC para License Manager 208
Solución de problemas 209
Error de detección entre cuentas 209
La cuenta de administración no puede desasociar los recursos de una licencia autogestionada 209
Systems Manager Inventory no está actualizado 209
Persistencia aparente de una AMI con registro anulado 210
Las nuevas instancias de cuentas secundarias tardan en aparecer en el inventario de recursos 210
Después de habilitar el modo entre cuentas, las instancias de las cuentas secundarias tardan en aparecer 210
La detección entre cuentas no se puede deshabilitar 210
El usuario de la cuenta secundaria no puede asociar la licencia autoadministrada compartida con una instancia 211
Se produce un error al vincular AWS Organizations cuentas 211
Error en la configuración del producto de suscripción de usuario 211
Las instancias de suscripción de usuario no se lanzan 212
La unión perfecta de dominios para EC2 instancias con productos de suscripción de usuario no funciona 213
No se puede eliminar Active Directory 213
El punto final de VPC se creó en mi cuenta 213
Elimine todos los recursos de puntos finales de VPC creados por License Manager 213
No se pudo eliminar el rol vinculado al AWSService RoleFor AWSLicense ManagerUserSubscriptionsService servicio (SLR) 214
Error de suscripción no presente para el producto SAL de RDS 214
Solución de problemas de confianza 214

Problemas de facturación de las suscripciones de los usuarios 215
Los productos de suscripción de usuario muestran el estado de suscripción de Marketplace como Inactivo 216
Cambie un nombre de usuario en Managed Active Directory 216
Disocia a los usuarios de una instancia finalizada 216
Límites de usuarios por instancia 216
Instalar software adicional en las instancias de suscripción de los usuarios 217
Paquetes de idioma japonés en las instancias de suscripción de usuario 217
Usuario administrador local en instancias de suscripción de usuario 217
Instancias en mal estado 217
Número de usuarios que pueden acceder mediante RDP a una instancia de suscripciones de usuario 218
Sistemas operativos Windows compatibles 218
Versiones compatibles de Office y Visual Studio 218
Uso de la suscripción de usuario con versiones anteriores de Windows Server 218
Uso de las suscripciones de usuario de License Manager en todas las cuentas o regiones 219
Gestión del token CAL durante la migración a RDS SAL 219
Usuarios en mi AD autogestionado con productos de suscripción de usuario 219
Consejos para contactar con AWS Support 220
Historial de documentos 221
..... ccxxviii

¿Qué es AWS License Manager?

AWS License Manager es un servicio que le facilita la gestión centralizada de las licencias de software de los proveedores de software (por ejemplo, Microsoft, SAP, Oracle e IBM) en AWS todos sus entornos locales. Esto proporciona control y visibilidad del uso de sus licencias, lo que le permite limitar los excedentes de licencias y reducir el riesgo de que se produzcan problemas de incumplimiento y de informes erróneos.

A medida que vaya desarrollando su infraestructura de nube AWS, podrá ahorrar costes gracias a las oportunidades que ofrece el modelo Bring Your Own License (BYOL). Es decir, puede reutilizar su inventario de licencias existente para sus recursos en la nube.

License Manager reduce el riesgo de excedentes de licencias y penalizaciones con el seguimiento del inventario que está directamente vinculado a AWS los servicios. Con controles basados en reglas en el consumo de licencias, los administradores pueden establecer límites fijos o flexibles en las implementaciones nuevas o existentes en la nube. En función de estos límites, License Manager ayuda a impedir el uso no conforme de servidores antes de que se produzca.

Los paneles integrados de License Manager proporcionan una visibilidad continua del uso de las licencias y ayudan con las auditorías de los proveedores.

License Manager permite el seguimiento de cualquier software que tenga licencia en función de los núcleos virtuales (vCPUs), los núcleos físicos, los sockets o la cantidad de máquinas. Esto incluye diversos productos de software de Microsoft, IBM, SAP, Oracle y otros proveedores.

Con él AWS License Manager, puede realizar un seguimiento centralizado de las licencias y hacer cumplir los límites en varias regiones, mediante el mantenimiento de un recuento de todos los derechos retirados. License Manager también hace un seguimiento de la identidad del usuario y el identificador de recursos subyacente, si está disponible, asociado a cada retirada, además de la fecha en que se retiró. El ISV puede hacer un seguimiento de estos datos de series temporales mediante CloudWatch métricas y eventos. ISVs puede usar estos datos para análisis, auditorías y otros fines similares.

AWS License Manager está integrado con AWS MarketplaceAWSData Exchange y con los siguientes AWS servicios: AWS Identity and Access Management (IAM) AWS Organizations, Service Quotas AWS CloudFormation, etiquetado de AWS recursos y. AWS X-Ray

Derechos administrados

Con License Manager, un administrador de licencias puede distribuir, activar y realizar un seguimiento de las licencias de software en todas las cuentas y en toda la organización.

Los proveedores de software independientes (ISVs) pueden utilizarlo AWS License Manager para gestionar y distribuir licencias de software y datos a los usuarios finales mediante derechos gestionados. Como emisor, puede realizar un seguimiento centralizado del uso de las licencias emitidas por el vendedor mediante el panel de control de License Manager. ISVs Las ventas se AWS Marketplace benefician de la creación y distribución automáticas de licencias como parte del flujo de trabajo de las transacciones. ISVs también puede usar License Manager para crear claves de licencia y activar licencias para clientes sin una AWS cuenta.

License Manager utiliza estándares del sector abiertos y seguros para representar las licencias y permite a los clientes verificar criptográficamente su autenticidad. License Manager admite varios modelos de licencias diferentes, incluidas licencias perpetuas, licencias flotantes, licencias de suscripción y licencias basadas en el uso. Si tiene licencias que deban estar estrictamente vinculadas a un nodo concreto, License Manager proporciona mecanismos para consumir sus licencias de esa manera.

Puede crear licencias AWS License Manager y distribuirlas a los usuarios finales mediante una identidad de IAM o mediante fichas firmadas digitalmente generadas por. AWS License Manager Los usuarios finales que lo utilicen AWS pueden redistribuir aún más los derechos de licencia entre las identidades de sus respectivas organizaciones. AWS Los usuarios finales con concesiones de derechos distribuidos pueden retirar y registrar las concesiones de derechos necesarias de esa licencia mediante la integración del software con AWS License Manager. En cada retirada de licencias se especifican los derechos, la cantidad asociada y el periodo de tiempo de la retirada; por ejemplo, si se retiran 10 licencias **`admin-users`** durante una hora. Esta verificación se puede realizar en función de la identidad de IAM subyacente de la licencia distribuida o en función de los tokens de larga duración generados a través del servicio. AWS License Manager AWS License Manager

Casos de uso de License Manager

Los siguientes son ejemplos de las funciones que ofrece License Manager para varios casos de uso:

- Licencias autoadministradas en License Manager— Se utiliza para definir las reglas de licencia en función de los términos de sus acuerdos empresariales, que determinan cómo se procesan AWS los comandos que consumen estas licencias.
- Licencias emitidas por el vendedor en License Manager: se utiliza para administrar y distribuir licencias de software a los usuarios finales.
- Licencias concedidas en License Manager— Se utiliza para regular el uso de las licencias adquiridas de AWS Marketplace AWS Data Exchange, o directamente de, un vendedor que integró su software con los derechos gestionados.
- Conversiones de tipos de licencia en License Manager— Se utiliza para cambiar el tipo de licencia entre la licencia AWS proporcionada y el modelo Bring Your Own License (BYOL) sin tener que volver a distribuir las cargas de trabajo.
- Búsqueda en el inventario en License Manager— Se utiliza para detectar y realizar un seguimiento de las aplicaciones locales mediante AWS Systems Manager las normas de inventario y licencias.
- Utilice las suscripciones basadas en usuarios de License Manager para los productos de software compatibles: se utiliza para adquirir licencias de software compatible proporcionadas por Amazon, plenamente conformes, con una cuota de suscripción por usuario.
- Gestione las suscripciones de Linux en License Manager: se utiliza para ver y administrar suscripciones comerciales de Linux que posea y ejecute en AWS.

Servicios relacionados

License Manager está integrado con Amazon EC2, Amazon RDS, AWS Marketplace AWS Systems Manager, y AWS Organizations.

La EC2 integración de Amazon le permite realizar un seguimiento de las licencias de los siguientes recursos y hacer cumplir las normas de licencia a lo largo del ciclo de vida de los recursos:

- EC2Instancias de Amazon
- Instancias dedicadas
- Hosts dedicados
- Instancias de spot y flotas de spot
- Nodos administrados

Si utiliza License Manager junto con él AWS Systems Manager, puede administrar las licencias en servidores físicos o virtuales alojados fuera de él AWS. Puede usar License Manager AWS Organizations para administrar todas las cuentas de su organización de forma centralizada.

Además, puede controlar el uso de las licencias adquiridas a AWS Marketplace AWS Data Exchange, o directamente a, un vendedor que haya integrado su software AWS License Manager. Puede utilizarlos AWS License Manager para distribuir los derechos de uso, conocidos como derechos, a personas específicas. Cuentas de AWS

License Manager se integra con Amazon RDS for Oracle y Amazon RDS para licencias BYOL basadas en vCPU de Db2. Con esta integración, obtiene visibilidad del uso de vCPU para sus instancias de base de datos de RDS para Oracle y RDS para Db2. Puede utilizar estos datos para calcular la cantidad de licencias consumidas en función de sus condiciones de licencia con los proveedores de sistemas de administración de bases de datos. Para obtener más información, consulte los siguientes enlaces asociados en la Guía del usuario de Amazon RDS.

- Opciones de licencia de RDS para Oracle
- Opciones de licencia de RDS para Db2

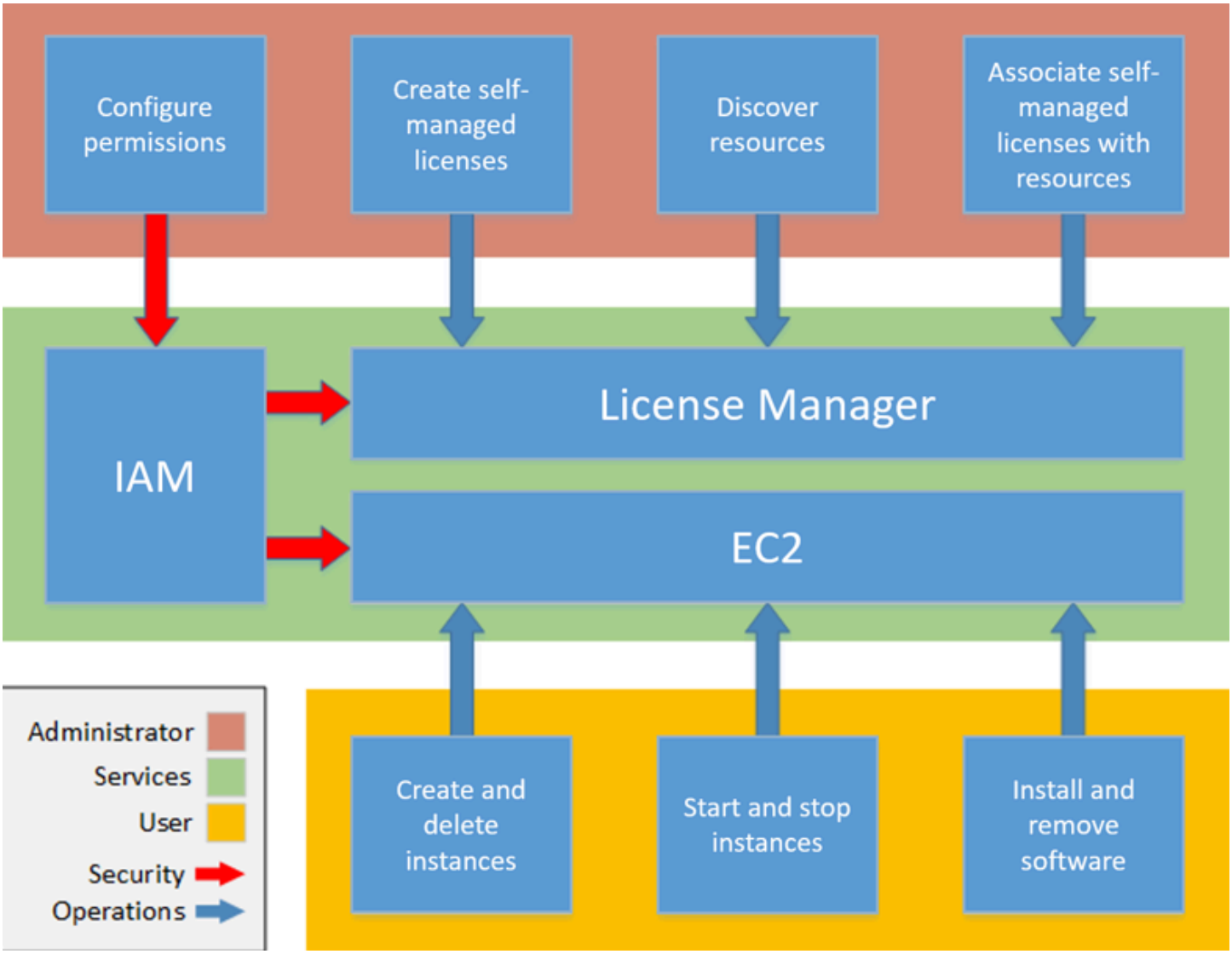
Cómo funciona License Manager

Una administración efectiva de licencias de software se basa en lo siguiente:

- Un conocimiento experto del lenguaje empleado en los contratos de licencias empresariales
- Una restricción adecuada del acceso a las operaciones que consumen licencias
- Un seguimiento exacto del inventario de licencias

Es posible que las empresas tengan personas o equipos dedicados a cada uno de estos dominios. Esto puede suponer un problema de comunicación efectiva, especialmente entre los expertos en licencias y los administradores de sistemas. License Manager proporciona una forma de agrupar los conocimientos de varios dominios. Lo que es más importante, también se integra de forma nativa con los AWS servicios, por ejemplo, con el plano de EC2 control de Amazon, donde se crean y eliminan las instancias. Esto significa que las reglas y los límites de License Manager capturan conocimientos empresariales y operativos y también se traducen en controles automatizados para la creación de instancias y la implementación de aplicaciones.

El siguiente diagrama ilustra las funciones distintas pero coordinadas de los administradores de licencias, que administran los permisos y configuran License Manager, y de los usuarios, que crean, administran y eliminan recursos a través de la EC2 consola de Amazon.



Si usted es responsable de la administración de licencias en su organización, puede utilizar License Manager para configurar reglas de asignación de licencias, asociarlas a los lanzamientos y realizar un seguimiento del uso. Esto permite que los usuarios de su organización puedan añadir y eliminar recursos que utilizan licencias sin esfuerzo adicional.

Un experto en licencias administra las licencias de toda la organización, lo que conlleva determinar las necesidades del inventario de recursos, supervisar la adquisición de licencias y controlar el uso conforme de las licencias. En una empresa que utilice License Manager, este trabajo se consolida a través de la consola License Manager. Como se muestra en el diagrama, esto implica la configuración de permisos de servicio, la creación de licencias autoadministradas, la realización del inventario de recursos informáticos tanto en las instalaciones como en la nube y la asociación de las licencias autoadministradas a los recursos detectados. En la práctica, esto podría implicar asociar una licencia autogestionada a una imagen de máquina de Amazon (AMI) aprobada que el

departamento de TI utilice como plantilla para todas las implementaciones de EC2 instancias de Amazon.

License Manager ahorra los costos que, de no utilizarlo, se dedicarían a pagar por las infracciones de licencias. Las auditorías internas detectan las infracciones después de que se han producido, cuando es demasiado tarde para evitar sanciones por incumplimiento, pero License Manager impide que se produzcan esos costosos incidentes. License Manager simplifica la generación de informes con paneles integrados que muestran el uso de licencias y los recursos que se controlan.

Comience a utilizar License Manager

Para usarlo AWS License Manager, primero debe completar los pasos de incorporación. El siguiente procedimiento le guiará por los pasos de incorporación del. AWS Management Console

Comience a utilizar License Manager

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Se le pedirá que configure los permisos para License Manager y sus servicios compatibles. Siga las instrucciones para configurar los permisos requeridos.
3. Una vez completada la configuración inicial, puede continuar con el uso de License Manager para el Casos de uso de License Manager deseado.

Para obtener más información sobre cómo administrar los permisos de los usuarios, grupos y roles para utilizar License Manager siguiendo las prácticas AWS recomendadas, consulteGestión de identidad y acceso para License Manager. Para obtener más información sobre cómo configurar EC2 los recursos de Amazon que se integran con License Manager, consulte Configurar para usar Amazon EC2 en la Guía del usuario de Amazon Elastic Compute Cloud.

Uso de License Manager

License Manager se puede aplicar a escenarios estándar para empresas con una infraestructura mixta de recursos de AWS y recursos en las instalaciones. Puede crear licencias autoadministradas, hacer un inventario de los recursos que utilizan licencias, asociar licencias autoadministradas a los recursos y realizar un seguimiento del inventario y la conformidad.

Licencias de AWS Marketplace productos

Con License Manager, ahora puede asociar reglas de licencia a los productos AMI de AWS Marketplace BYOL mediante plantillas de EC2 lanzamiento, AWS CloudFormation plantillas o productos de Service Catalog de Amazon. En cada caso, podrá beneficiarse del seguimiento de licencias centralizado y se asegurará del cumplimiento.

> **Note**
>
> License Manager no cambia la forma en que obtiene y activa su BYOL AMIs desde Marketplace. Después del lanzamiento, debe proporcionar una clave de licencia que se obtiene directamente del vendedor para activar cualquier software de terceros.

Seguimiento de licencias para los recursos de los centros de datos en las instalaciones

Con License Manager, puede detectar aplicaciones que se estén ejecutando fuera del AWS inventario de Systems Manager y, a continuación, adjuntarles reglas de licencia. Después de asociar las reglas de asignación de licencias, puede realizar un seguimiento de los servidores en las instalaciones junto con los recursos de AWS en la consola License Manager.

Diferenciación entre el modelo con licencia incluida y el modelo BYOL

Con License Manager, puede identificar qué recursos tienen una licencia que se incluye con el producto y cuáles utilizan una licencia de su propiedad. Esto le permite informar con precisión del uso que hace de las licencias BYOL. Este filtro requiere la versión 2.3.722.0 de SSM o posterior.

License Manager en todas sus AWS cuentas

License Manager le permite administrar las licencias en todas sus AWS cuentas. Puede crear configuraciones de licencia una vez en su cuenta AWS Organizations de administración y

compartirlas entre sus cuentas utilizando AWS Resource Access Manager o vinculando AWS Organizations cuentas mediante la configuración del License Manager. Esto también le permite realizar búsquedas entre cuentas para buscar en el inventario de sus AWS cuentas.

Contenido

- Licencias autoadministradas en License Manager
- Reglas de asignación de licencias en License Manager
- Informes de uso en License Manager
- Conversiones de tipos de licencia en License Manager
- Aloje grupos de recursos en License Manager
- Búsqueda en el inventario en License Manager
- Licencias concedidas en License Manager
- Licencias emitidas por el vendedor en License Manager
- Utilice las suscripciones basadas en usuarios de License Manager para los productos de software compatibles
- Gestione las suscripciones de Linux en License Manager
- Configuración en License Manager
- Panel de control en License Manager

Licencias autoadministradas en License Manager

Las licencias autogestionadas (anteriormente denominadas configuraciones de licencia) son el núcleo de License Manager. Las licencias autoadministradas contienen reglas de asignación de licencias que se basan en las condiciones de los acuerdos de su empresa. Las reglas que cree determinan cómo AWS procesa los comandos que consumen licencias. Cuando cree licencias autoadministradas, trabaje en estrecha colaboración con el equipo de conformidad de su organización para revisar los acuerdos de su empresa.

Servicios de AWS como License Manager, tienen cuotas de servicio que definen la cantidad máxima de recursos u operaciones por región que están disponibles Cuenta de AWS para ese servicio. Por ejemplo, con License Manager, puede tener un máximo de licencias `10` autogestionadas por recurso, con un total de licencias `25` autogestionadas como máximo. Región de AWS Para obtener más información sobre las cuotas de License Manager, consulte Cuotas de AWS License Manager servicio en Referencia general de AWS.

> **Note**
>
> Las instancias administradas por Systems Manager deben estar asociadas a licencias autoadministradas tipo vCPU e instancia.

Contenido

- Parámetros y reglas de licencia autogestionados en License Manager
- Cree reglas de License Manager a partir de licencias de los proveedores
- Cree una licencia autogestionada en License Manager
- Compartir una licencia autogestionada en License Manager
- Edición de una licencia autogestionada en License Manager
- Desactivar una licencia autogestionada en License Manager
- Eliminar una licencia autogestionada en License Manager

Parámetros y reglas de licencia autogestionados en License Manager

Una licencia autoadministrada consta de parámetros básicos y reglas que varían según los valores del parámetro. También puede agregar etiquetas a las licencias autoadministradas. Tras crear una licencia autoadministrada, un administrador puede modificar la cantidad de licencias y el límite de uso para adaptarse a los cambios en las necesidades de los recursos.

Los parámetros y reglas disponibles incluyen:

- Nombre de licencia autoadministrada: nombre de la licencia autoadministrada.
- (Opcional) Descripción: descripción de la licencia autoadministrada.
- Tipo de licencia: la métrica utilizada para contar las licencias. Los valores admitidos son v CPUs, núcleos, sockets e instancias.
- (Opcional) Número de <option>: el número de licencias que utiliza un recurso.
- Estado: indica si la configuración está activa.
- Información del producto: los nombres y las versiones de los productos para su detección automatizada. Los productos compatibles son Windows Server, SQL Server, Amazon RDS for Oracle y Amazon RDS for Db2.
- (Opcional) Reglas: se incluyen las siguientes. Las reglas disponibles varían según el tipo de recuento.

- Afinidad de licencia con el alojamiento (en días): restringe el uso de la licencia al host durante el número de días especificado. El rango va de 1 a 180. El tipo de recuento debe ser de núcleos o sockets. Una vez transcurrido el período de afinidad, la licencia estará disponible para su reutilización en 24 horas.
- Cantidad máxima de núcleos: número máximo de núcleos para un recurso.
- Cantidad máxima de sockets: número máximo de sockets para un recurso.
- v máximo CPUs: recuento máximo de v CPUs para un recurso.
- Cantidad mínima de núcleos: número mínimo de núcleos para un recurso.
- Cantidad mínima de sockets: número mínimo de sockets para un recurso.
- Mínimo v CPUs: recuento mínimo v CPUs para un recurso.
- Arrendamiento: restringe el uso de la licencia al arrendamiento especificado EC2. Si el tipo de recuento es de núcleos o sockets, se requieren hosts dedicados. Se admiten el arrendamiento compartido, los hosts dedicados y las instancias dedicadas si el tipo de recuento es Instancias o v. CPUs Los nombres de la consola (y la API) son los siguientes:
  - Compartido (`EC2-Default`)
  - Instancia dedicada (`EC2-DedicatedInstance`)
  - Host dedicado (`EC2-DedicatedHost`)
  - Optimización de vCPU: License Manager se integra con el soporte de optimización de CPU de Amazon EC2, lo que le permite personalizar el número de v CPUs en una instancia. Si esta regla se establece en True, License Manager cuenta v en CPUs función del recuento personalizado de núcleos y subprocesos. De lo contrario, License Manager cuenta el número predeterminado de v CPUs para el tipo de instancia.

En la siguiente tabla se describen las reglas de licencias disponibles para cada tipo de recuento.

Nombre de la consola	Nombre de API	Núcleos	instancias	Sockets	v CPUs
Afinidad de licencia con el alojamiento (en días)	`licenseAffinityToHost`	✓		✓	
Cantidad máxima de núcleos	`maximumCores`	✓	✓		

Nombre de la consola	Nombre de API	Núcleos	instancias	Sockets	v CPUs
Cantidad máxima de sockets	`maximumSockets`		✓	✓	
Máximo v CPUs	`maximumVcpus`		✓		✓
Cantidad mínima de núcleos	`minimumCores`	✓	✓		
Cantidad mínima de sockets	`minimumSockets`		✓	✓	
Mínimo v CPUs	`minimumVcpus`		✓		✓
Propiedad	`allowedTenancy`	✓	✓	✓	✓
Optimización de vCPU	`honorVcpu Optimization`				✓

Cree reglas de License Manager a partir de licencias de los proveedores

Puede crear conjuntos de reglas de License Manager en función de las condiciones empleadas en las licencias de los proveedores de software. Los ejemplos que aparecen a continuación no están pensados para utilizarlos como esquemas para casos de uso reales. En cualquier aplicación real de un acuerdo de licencia, puede elegir entre opciones contrapuestas que dependen de la arquitectura y el historial de licencias de su propio entorno de servidores en las instalaciones. Sus opciones también dependen de los detalles de su planificación de la migración de recursos a AWS.

En la medida de lo posible, estos ejemplos pretenden ser neutrales con respecto a los proveedores y se centran en cuestiones de asignación de hardware y software que pueden aplicarse de forma general. Las disposiciones sobre licencias de los proveedores también interactúan con AWS los requisitos y límites. El número de licencias necesario para una aplicación varía en función del tipo de instancia elegido y de otros factores.

> **Important**
>
> AWS no participa en el proceso de auditoría con los proveedores de software. Los clientes son responsables de la conformidad y asumen la responsabilidad de interpretar y capturar cuidadosamente las reglas en License Manager en función de sus acuerdos de licencia.

Ejemplo: Implementación de una licencia de sistema operativo

Este ejemplo es para una licencia para un sistema operativo de servidor. Los términos de la licencia imponen restricciones en cuanto al tipo de núcleo de CPU, la tenencia y el número mínimo de licencias por servidor.

En este ejemplo, las condiciones de la licencia incluyen las estipulaciones siguientes:

- El número de núcleos de procesador físicos determina el número de licencias.
- El número de licencias debe coincidir con el número de núcleos.
- Un servidor debe tener un mínimo de ocho núcleos.
- El sistema operativo debe ejecutarse en un host no virtualizado.

Además, el cliente ha tomado las siguientes decisiones:

- Se han adquirido licencias para 96 núcleos.
- Se impone un límite máximo para restringir el consumo de licencias a la cantidad adquirida.
- Cada servidor necesita un máximo de 16 núcleos.

En la tabla siguiente, se asocian los parámetros de creación de reglas de License Manager con los requisitos de asignación de licencias del proveedor que capturan y automatizan. Los valores de ejemplo son únicamente ilustrativos; debe especificar los valores que necesita en sus propias licencias autoadministradas.

Regla de License Manager	Configuración
Tipo de recuento de licencias	El tipo de licencia se define como **`Cores`**.
Número de licencias	

Regla de License Manager	Configuración
	El número de núcleos se establece en **96**.
V mínimo CPUs o máximo de 5 núcleos	La cantidad mínima de núcleos se establece en **8**. La cantidad máxima de núcleos se establece en **16**.
Límite máximo en cuanto al número de licencias	Se ha seleccionado Implementar límite de licencia.
Tenencia permitida	La tenencia se ha definido como **`Dedicated Host`**.

Cree una licencia autogestionada en License Manager

Una licencia autoadministrada representa los términos de licencia del acuerdo con su proveedor de software. Su licencia autogestionada especifica cómo deben contarse sus licencias (por ejemplo, por v CPUs o número de instancias). También especifica los límites de uso, de modo que puede evitar que el uso supere el número de licencias asignadas. Además, también puede especificar otras restricciones en sus licencias, como el tipo de tenencia.

Consideraciones sobre las bases de datos Amazon RDS for Oracle y Amazon RDS para Db2

Al añadir información de producto para configurar la detección automática de bases de datos de Amazon RDS for Oracle o Amazon RDS for Db2, se aplican los siguientes requisitos:

- El tipo de recuento de licencias admitido es `vCPU`.
- No se admiten reglas.
- No se admiten límites máximos fijos para las licencias.
- Puede realizar el seguimiento de una versión del producto por cada licencia autoadministrada.
- No puede realizar un seguimiento de las bases de datos de Amazon RDS y otros productos con la misma licencia autogestionada.

Procedimiento para crear una política autoadministrada con la consola

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Licencias autoadministradas.
3. Seleccione Crear licencia autoadministrada.
4. En el panel Detalles de configuración, introduzca la siguiente información:
   - Nombre de licencia autoadministrada: nombre para la licencia autoadministrada.
   - Descripción: descripción opcional de la licencia autoadministrada.
   - Tipo de licencia: el modelo de recuento de esta licencia (v CPUs, núcleos, sockets o instancias).
   - Número de <option>: la opción depende del tipo de licencia. Cuando el límite de la licencia se supera, License Manager le notifica (límite flexible) o impide que se implemente un recurso (límite máximo fijo).
   - Implementar límite de licencia: si se selecciona, el límite de licencia es un límite máximo fijo.
   - Reglas: una o más reglas. Para cada regla, seleccione un tipo de regla, introduzca un valor de regla y elija Agregar regla. Los tipos de regla que se muestran dependen del tipo de licencia. Por ejemplo, los valores mínimos, los valores máximos y la tenencia. Si no especifica un tipo de tenencia, se aceptan todos.
5. (Opcional) En el panel Reglas de detección automatizada, haga lo siguiente:
   a. Elija el nombre del producto, el tipo de producto y el tipo de recurso para cada producto que desee detectar y del que desee hacer un seguimiento mediante la detección automatizada.
   b. Seleccione Detener el seguimiento de instancias cuando el software se desinstale para que la licencia pueda volver a utilizarse una vez que License Manager detecte que el software se ha desinstalado y ha transcurrido cualquier período de afinidad de licencia.
   c. (Opcional) Si su cuenta es una cuenta de administración de License Manager para una organización, tiene la opción de definir recursos para su exclusión de la detección automatizada. Para ello, seleccione Añadir regla de exclusión, elija la propiedad por la que desee filtrar, ya que se admiten etiquetas de AWS cuentas IDs y recursos y, a continuación, introduzca la información para identificar esa propiedad.
6. (Opcional) Expanda el panel Etiquetas para añadir una o más etiquetas a la licencia autoadministrada. Las etiquetas son pares clave/valor. Proporcione la siguiente información para cada etiqueta:

- Clave: el nombre de la clave que se puede buscar.
- Valor: el valor de la clave.

7. Seleccione Enviar.

Procedimiento para crear una licencia autoadministrada con la línea de comandos

- create-license-configuration (AWS CLI)
- Nueva LICMLicense configuración (Herramientas de AWS para PowerShell)

Compartir una licencia autogestionada en License Manager

Puede utilizarla AWS Resource Access Manager para compartir sus licencias autogestionadas con cualquier AWS cuenta o a través de. AWS Organizations Para obtener más información, consulte Compartir sus AWS recursos en la Guía del AWS RAM usuario.

Comparta una licencia autogestionada con su organización AWS

Requisitos previos

Para completar este procedimiento, debe vincular su AWS organización con License Manager. Para obtener más información, consulte Configuración de licencias gestionadas en License Manager.

Comparta su licencia

Para compartir una licencia autogestionada con su AWS organización, siga estos pasos:

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Licencias autoadministradas.
3. Seleccione la licencia autoadministrada.
4. Seleccione Compartir con las cuentas de la AWS organización en el menú Acciones.

Cuota de cuentas admitidas

Si habilitó el uso compartido de licencias AWS License Manager antes del 14 de octubre de 2023, su cuota para el número máximo de cuentas que License Manager admite en su organización será inferior al nuevo máximo predeterminado. Puede aumentar esta cuota mediante las operaciones de API AWS RAM que se indican en la siguiente sección. Para obtener más información sobre las

cuotas predeterminadas en License Manager, consulte Cuotas para trabajar con licencias en la Guía de Referencia general de AWS .

Requisitos previos

Para completar el siguiente procedimiento, debe iniciar sesión como entidad principal en la cuenta de administración de la organización que tenga los siguientes permisos:

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

Cómo aumentar la cuota de cuentas admitidas

El siguiente procedimiento aumentará su cuota actual para `Number of accounts per organization for License Manager` hasta el máximo predeterminado actual.

Procedimiento para aumentar la cuota de cuentas admitidas para License Manager

1. Utilizar describe-organization AWS CLI comando para determinar el ARN de su organización mediante la operación:

```
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. Utilizar get-resource-shares AWS CLI comando para determinar el ARN de su organización mediante la operación:

```
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. Utilizar enable-sharing-with-aws-organization AWS CLI comando para habilitar el intercambio de recursos con AWS RAM:

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

{
 "returnValue": true
}
```

Puede utilizar el list-aws-service-access-for-organization AWS CLI comando para comprobar que los principales de servicio de Organizations lists están habilitados para License Manager y AWS RAM:

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

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

> **Important**
>
> La organización puede tardar hasta seis horas en finalizar esta operación. AWS RAM Este proceso debe completarse antes de poder continuar.

4. Utilizar associate-resource-share AWS CLI comando para asociar su recurso compartido de recursos de License Manager a su organización:

```
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
  }
 ]
}
```

Puede utilizar el get-resource-share-associations AWS CLI comando para validar que la asociación de recursos compartidos `status` es`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
  }
 ]
}
```

Edición de una licencia autogestionada en License Manager

Puede editar los valores de los campos siguientes en una licencia autoadministrada:

- Nombre de licencia autoadministrada
- Descripción
- Número de <option>
- Aplicación del límite de tipos de licencia

Procedimiento para editar una licencia autoadministrada

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Licencias autoadministradas.
3. Seleccione la licencia autoadministrada.
4. Seleccione Acciones, Editar.
5. Actualice los detalles según sea necesario y, a continuación, seleccione Actualizar.

Procedimiento para editar una licencia autoadministrada con la línea de comandos

- update-license-configuration (AWS CLI)
- Actualización: LICMLicense configuración (Herramientas de AWS para PowerShell)

Desactivar una licencia autogestionada en License Manager

Al desactivar una licencia autogestionada, los recursos existentes que utilizan la licencia no se ven afectados y se pueden seguir AMIs utilizando la licencia. Sin embargo, deja de realizarse el seguimiento del consumo de licencias.

Cuando se desactiva una licencia autoadministrada, no se debe asociar a ninguna instancia en ejecución. Después de la desactivación, no se pueden llevar a cabo lanzamientos con la configuración de licencia.

Procedimiento para desactivar una licencia autoadministrada

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Licencias autoadministradas.
3. Seleccione la licencia autoadministrada.
4. Seleccione Acciones, Desactivar. Cuando se le pida confirmación, seleccione Desactivar.

Procedimiento para desactivar una licencia autoadministrada con la línea de comandos

- update-license-configuration (AWS CLI)
- Actualización: LICMLicense configuración (Herramientas de AWS para PowerShell)

Eliminar una licencia autogestionada en License Manager

Para poder eliminar una licencia autoadministrada, debe desasociar todos los recursos. Puede eliminar una licencia autoadministrada si necesita empezar de cero con nuevas reglas de asignación de licencias. Si las condiciones de las licencias de sus proveedores de software cambian, puede desasociar los recursos existentes, eliminar la licencia autoadministrada, crear una nueva licencia autoadministrada que refleje las condiciones actualizadas y asociarla a los recursos existentes.

Procedimiento para eliminar una política autoadministrada con la consola

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Licencias autoadministradas.
3. Elija el nombre de la licencia autoadministrada para abrir la página de detalles de la licencia.
4. Seleccione cada uno de los recursos (uno por uno o en bloque) y Desasociar recurso. Repita la operación hasta la lista esté vacía.
5. Seleccione Acciones, Eliminar. Cuando se le pida confirmación, elija Eliminar.

Procedimiento para eliminar una política autoadministrada con la línea de comandos

- delete-license-configuration (AWS CLI)
- Eliminar- LICMLicense Configuración (Herramientas de AWS para PowerShell)

Reglas de asignación de licencias en License Manager

Una vez definidas las reglas de asignación de licencias autoadministradas, es posible asociarlas a los mecanismos de lanzamiento pertinentes, donde pueden evitar directamente la implementación de recursos nuevos que no sean conformes. Los usuarios de su organización pueden lanzar EC2 instancias sin problemas desde las instancias designadas AMIs, y los administradores pueden realizar un seguimiento del inventario de licencias a través del panel de control integrado de License Manager. Los controles de lanzamiento y las alertas del panel permiten aplicar el cumplimiento de una forma más sencilla.

> **Important**
>
> AWS no participa en el proceso de auditoría con los proveedores de software. Los clientes son responsables de la conformidad y asumen la responsabilidad de interpretar y capturar cuidadosamente las reglas en License Manager en función de sus acuerdos de licencia.

El seguimiento de licencias funciona desde el momento en que las reglas se asocian a una instancia hasta su terminación. Usted define los límites de uso y las reglas de asignación de licencias, y License Manager hace un seguimiento de las implementaciones al tiempo que le avisa cuando se producen infracciones de las reglas. Si ha configurado límites máximos fijos, License Manager puede evitar que se lancen los recursos.

Cuando se detiene o se termina un servidor que se está controlando, su licencia se libera y se devuelve al grupo de licencias disponibles.

Dado que las organizaciones tienen diferentes enfoques para las operaciones y la conformidad, License Manager admite varios mecanismos de lanzamiento:

- Asociación manual de licencias autogestionadas con AMIs: para realizar un seguimiento de las licencias de sistemas operativos u otro software, puede adjuntar reglas de licencia AMIs antes de publicarlas para un uso más amplio en su organización. A continuación, AMIs se realiza un seguimiento automático de todas las implementaciones realizadas a partir de ellas con License Manager sin que los usuarios deban realizar ninguna acción adicional. También puede asociar reglas de asignación de licencias a sus mecanismos actuales de creación de AMI, como Systems Manager Automation, VM Import/Export y Packer.
- Plantillas de EC2 lanzamiento de Amazon y AWS CloudFormation: si adjuntar reglas de licencia a no AMIs es una opción preferida, puede especificarlas como parámetros opcionales en las plantillas o AWS CloudFormation plantillas de EC2 lanzamiento. Las implementaciones con estas plantillas se controlan mediante License Manager. Puede hacer cumplir las normas sobre las plantillas o AWS CloudFormation plantillas de EC2 lanzamiento especificando una o más licencias autogestionadas IDs en el campo de licencias autogestionadas.

AWS trata los datos de seguimiento de las licencias como datos confidenciales de los clientes, a los que solo se puede acceder a través de la AWS cuenta propietaria. AWS no tiene acceso a los datos de seguimiento de sus licencias. Usted controla sus datos de seguimiento de licencias y puede eliminarlos en cualquier momento.

Asociar licencias autogestionadas y AMIs

El siguiente procedimiento muestra cómo asociar las licencias autogestionadas con el AMIs uso de la consola License Manager. El procedimiento presupone que ya tiene al menos una licencia autoadministrada. Puede asociar licencias autoadministradas a cualquier AMI a la que tenga acceso, ya sea de su propiedad o compartida. Si alguien compartió una AMI con usted, puede asociarla a la licencia autoadministrada de la cuenta corriente. De lo contrario, puede especificar si la AMI está asociada a la licencia autoadministrada en todas las cuentas o solo en la cuenta corriente.

Si asocia una AMI a una licencia autoadministrada en todas las cuentas, puede realizar un seguimiento de los lanzamientos de instancias desde la AMI en todas las cuentas. Cuando se alcanza un límite máximo fijo, License Manager bloquea los lanzamientos de instancias adicionales. Cuando se alcanza un límite flexible, License Manager notifica los lanzamientos de instancias adicionales.

Si copia una AMI dentro de la misma región y esa AMI tiene configuraciones de licencia asociadas, esas configuraciones de licencia se asocian automáticamente a la nueva AMI. Cuando lanza una instancia desde la nueva AMI, License Manager la rastrea. Del mismo modo, si crea una nueva AMI a partir de una instancia en ejecución que tiene configuraciones de licencia asociadas, esas configuraciones de licencia se asocian automáticamente a la nueva AMI y License Manager realiza un seguimiento de las instancias que lanza desde la nueva AMI.

> **Warning**
>
> License Manager no admite el seguimiento de instancias entre regiones. Si copia una AMI que tiene configuraciones de licencia asociadas a una región diferente, License Manager bloquea todos los lanzamientos de instancias desde la nueva AMI.

Procedimiento para asociar una licencia autoadministrada y una AMI

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Licencias autoadministradas.
3. Elija el nombre de la licencia autoadministrada para abrir la página de detalles de la licencia. Para ver lo que está asociado actualmente AMIs, seleccione Asociado AMIs.
4. Seleccione AMI asociadas.
5. AMIsEn Disponible, seleccione uno o más AMIs y elija Asociar.

- Si su cuenta es propietaria de al menos una de las AMIs, se le solicitará que elija un ámbito de asociación de AMI para la AMIs que sea de su propiedad. Todas AMIs las que se hayan compartido desde otra cuenta están asociadas únicamente a su cuenta. Elija Confirmar.
- Si AMIs se compartieron contigo desde otra cuenta, se asocian únicamente a tu cuenta.

Las recién asociadas aparecen AMIs ahora en la AMIs pestaña Asociadas de la página de detalles de la licencia.

Desasociar las licencias autogestionadas y AMIs

El siguiente procedimiento muestra cómo desasociar las licencias autogestionadas del AMIs uso de la consola License Manager. No se puede desasociar una AMI que se haya dado de baja. License Manager comprueba si las personas se han dado de baja AMIs cada 8 horas y las desvincula automáticamente.

Procedimiento para desasociar una licencia autoadministrada y una AMI

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Licencias autoadministradas.
3. Elija el nombre de la licencia autoadministrada para abrir la página de detalles de la licencia.
4. Seleccione Asociado AMIs.
5. Seleccione la AMI y elija Desasociar AMI.

Informes de uso en License Manager

Con AWS License Manager él, puede realizar un seguimiento del historial de sus licencias autogestionadas programando instantáneas periódicas del uso de las licencias. Al configurar los informes de uso, License Manager cargará automáticamente los informes de sus licencias autoadministradas a un bucket de S3 en función de sus especificaciones. Los informes de uso se denominaban antes generadores de informes. Puede configurar varios informes de uso para realizar un seguimiento eficaz de las configuraciones de los distintos tipos de licencias de su entorno.

> **Note**
>
> AWS License Manager no almacena sus informes. Los informes de License Manager se publican directamente en el bucket de S3. Una vez que elimina un informe de uso, los informes dejan de publicarse en el bucket de S3.

Crear un informe de uso en License Manager

Cuando cree un informe de uso, debe especificar un tipo de licencia autoadministrada para el seguimiento por parte de License Manager, un intervalo de frecuencia que defina cada cuanto se generan los informes y un tipo de informe. Todos los informes se generan en formato CSV y se publican en un bucket de S3. Un informe de uso puede generar uno o más de los siguientes tipos de informes.

Informe resumido de licencias autoadministradas

Este tipo de informe contiene información sobre el número de licencias consumidas y datos sobre las licencias autoadministradas. El tipo de licencia autoadministrada de la que se está haciendo el seguimiento aparece con detalles como el número de licencias, las reglas de asignación de licencias y la distribución de las licencias entre los distintos tipos de recursos.

Informe de uso de recursos

Este tipo de informe proporciona detalles sobre los recursos a los que se ha hecho el seguimiento y el consumo de licencias correspondiente. Cada recurso rastreado que utiliza el tipo de licencia autogestionada especificado aparece con detalles como el identificador de licencia, el estado del recurso y el identificador de AWS cuenta propietario del recurso.

Procedimiento para crear un informe de uso

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación, seleccione Informes de uso.
3. Seleccione Crear informe de uso y, a continuación, en el panel Crear informe de uso, defina los parámetros del informe:
   a. Introduzca un nombre y una descripción opcional para el informe de uso.
   b. Seleccione un tipo de licencia autoadministrada de la lista desplegable. Será el tipo de licencia sobre el que se generarán datos en el informe de uso.

c. Elija los tipos de informes que desee generar.

d. Seleccione la frecuencia con la que License Manager publicará los informes: una vez cada 24 horas, una vez cada 7 días o una vez cada 30 días.

e. (Opcional) Agregue etiquetas para realizar un seguimiento del recurso de informes de uso.

4. Seleccione Crear informe de uso.

Un nuevo informe de uso empezará a publicar los informes en 60 minutos o menos.

Si aún no dispone de un bucket de S3 asociado a su cuenta, License Manager creará un nuevo bucket de Amazon S3 en su cuenta cuando cree un informe de uso. Si ha habilitado previamente la búsqueda en inventario entre cuentas, los informes se enviarán al bucket de S3 creado por License Manager cuando la Búsqueda en inventario entre cuentas se encuentre habilitada.

Los informes se almacenan en el bucket con el siguiente patrón de URI de Amazon S3:

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

Editar un informe de uso en License Manager

Puede ver los informes de uso y realizar cambios en ellos desde la consola License Manager en cualquier momento. La tabla de informes de uso muestra todos los informes de uso creados para su cuenta. En la tabla, puede obtener una visión general de los distintos informes, ir al bucket de Amazon S3 asociado a sus informes de uso y ver el estado de la generación de los informes.

Procedimiento para eliminar un informe de uso

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación, seleccione Informes de uso.
3. Seleccione el informe de uso que desee editar de la tabla y, a continuación, seleccione Ver detalles.
4. Seleccione Editar para realizar cambios en el informe de uso.
5. Realice los cambios que desee en el informe de uso y, a continuación, seleccione Guardar cambios.

Un informe de uso actualizado generará un nuevo informe en menos de una hora.

> **Note**
>
> Al cambiar el nombre de un informe de uso, los informes futuros se enviarán a una nueva carpeta del bucket de S3 de License Manager que reflejará el nuevo nombre.

Eliminar un informe de uso en License Manager

Al eliminar un informe de uso, se detiene la generación de nuevos informes; sin embargo, el bucket de Amazon S3 y todos los informes anteriores no se ven afectados.

> **Note**
>
> No podrá eliminar una licencia autoadministrada de su cuenta si tiene un informe de uso asociado. Primero debe eliminar ese informe de uso.

Procedimiento para eliminar un informe de uso

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación, seleccione Informes de uso.
3. Seleccione el informe de uso que desee editar de la tabla y, a continuación, seleccione Ver detalles.
4. Seleccione Eliminar. Esta acción elimina permanentemente el informe de uso.

Conversiones de tipos de licencia en License Manager

Con License Manager, puede cambiar el tipo de licencia entre la licencia AWS proporcionada y el modelo Bring Your Own License (BYOL) o Bring your Own Subscription (BYOS), a medida que cambien las necesidades de su empresa. El tipo de licencia puede cambiarse sin tener que volver a implementar las cargas de trabajo existentes.

El inventario de licencias puede optimizarse para los siguientes escenarios mediante la conversión de tipos de licencia:

Migre las cargas de trabajo locales a Amazon EC2

Durante la migración, puede implementar su carga de trabajo en Amazon Elastic Compute Cloud (Amazon EC2) y utilizar las licencias AWS proporcionadas. Cuando se complete la migración, utilice la conversión de tipos de licencia de License Manager para cambiar el tipo de licencia de las instancias. Puede cambiar a los modelos BYOL o BYOS para poder usar las licencias que se publicaron durante la migración.

Uso de acuerdos de licencias vencidos para cargas de trabajo en ejecución

Puede utilizar la conversión de tipos de licencia de License Manager para cambiar de BYOL o BYOS a las licencias AWS proporcionadas. Este cambio le permite seguir ejecutando sus cargas de trabajo con licencias de software totalmente compatibles AWS con un modelo de licencia flexible y flexible pay-as-you. Esta sería una buena opción si su acuerdo de licencia con el proveedor de software del sistema operativo, como Microsoft o Canonical, está a punto de vencer y no tiene previsto renovarlo.

Optimización de costos

En el caso de cargas de trabajo pequeñas o irregulares, las instancias AWS provistas de licencias (licencia incluida) pueden resultar más rentables. Si opta por utilizar los modelos BYOL o BYOS, es posible que estas opciones requieran una permanencia a más largo plazo. En este caso, puede utilizar la conversión de tipos de licencia de License Manager para cambiar sus instancias a un modelo con licencia incluida a fin de optimizar los costos relacionados con la licencia. Si las instancias se lanzaron desde la imagen de su propia máquina virtual (VM), puede volver a utilizar los modelos BYOL o BYOS. Puede optar por hacerlo cuando la carga de trabajo sea más estable o predecible.

Mantenimiento extendido

Si su sistema operativo Ubuntu ha llegado al final del soporte estándar, puede añadir una suscripción de pago a Ubuntu Pro. Añadir una suscripción a Ubuntu Pro proporciona actualizaciones de seguridad durante un período prolongado. Para obtener más información, consulte “Ubuntu Pro” en la documentación de Canonical.

Temas

- Tipos de licencia aptos para la conversión de tipos de licencia en License Manager
- Requisitos previos de conversión para los tipos de licencia de License Manager
- Convertir un tipo de licencia en License Manager

- Conversión de arrendamiento en License Manager
- Solución de problemas de conversión de tipos de licencia en License Manager

Tipos de licencia aptos para la conversión de tipos de licencia en License Manager

Puede utilizar la conversión de tipos de licencia de License Manager con versiones y combinaciones compatibles de licencias de Windows Server y Microsoft SQL Server. También puede utilizar la conversión de tipos de licencia con las suscripciones a Ubuntu Linux.

Contenido

- Tipos de licencia aptos para Windows y SQL Server en License Manager
  - Ediciones de SQL Server
  - Versiones de SQL Server
  - Valores de operación de uso
  - Compatibilidad de medios
  - Rutas de conversión
- Tipos de suscripción aptos para Linux en License Manager

Tipos de licencia aptos para Windows y SQL Server en License Manager

> **Important**
>
> Las instancias que se lanzaron originalmente desde una imagen de máquina de Amazon (AMI) proporcionada por Amazon no son aptas para la conversión de tipos de licencia al modelo BYOL.

Windows y SQL Server deben cumplir ciertos requisitos para poder convertir el tipo de licencia.

Temas

- Ediciones de SQL Server
- Versiones de SQL Server
- Valores de operación de uso

- Compatibilidad de medios
- Rutas de conversión

Ediciones de SQL Server

License Manager admite las siguientes ediciones de SQL Server:

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

Versiones de SQL Server

License Manager admite las siguientes versiones de SQL Server:

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

Valores de operación de uso

La conversión de los tipos de licencia cambia el valor de operación de uso asociada a la instancia. Los valores de operación de uso para cada sistema operativo compatible se indican en la siguiente tabla. Para obtener más información sobre los códigos de facturación, consulte los campos de información de facturación de la AMI.

Detalles del sistema operativo	Operación de uso
Windows Server como BYOL	RunInstancesSQL Server 2008 ----sep----:0800

Detalles del sistema operativo	Operación de uso
Windows Server como BYOL SQL Server (cualquier edición) como BYOL	RunInstances:0800 ----Sept----:0800
Windows Server como modelo con licencia incluida	RunInstances:0800 ----SEP----:0002
Windows Server como modelo con licencia incluida SQL Server (cualquier edición) como BYOL	RunInstances:0002 ----SEP----:0002
Windows Server como modelo con licencia incluida SQL Server Web como modelo con licencia incluida	RunInstances:0002 ----sep----:0202
Windows Server como modelo con licencia incluida SQL Server Standard como modelo con licencia incluida	RunInstances:0202 ----SEP----:0006
Windows Server como modelo con licencia incluida SQL Server Enterprise como modelo con licencia incluida	RunInstances:0006 ----Sept----:0102

Compatibilidad de medios

La siguiente tabla confirma qué medios se pueden usar en qué instancias y modelos de licencia.

Origen	Destino	
	BYOL	Licencia incluida
AWS imagen de Windows Server proporcionada	No	Sí
AWS imagen de SQL Server proporcionada	No	Sí
Su propio medio de Windows Server[1]	Sí	Sí
Su propio medio de SQL Server[2]	Sí	Sí

[1] Indica que la instancia se lanzó originalmente desde su propia máquina virtual (VM) importada. Puede importar su máquina virtual mediante servicios como VM Import/Export o AWS Application Migration Service.

[2] Indica que ha proporcionado su propio medio de instalación de SQL Server (.iso, .exe).

Rutas de conversión

La siguiente tabla confirma si el modelo de licencia de origen se puede convertir a modelo BYOL o licencia incluida. Para obtener más información, consulte Convertir un tipo de licencia en License Manager.

Important

- La configuración de Windows Server como BYOL con SQL Server como licencia incluida es una configuración no compatible.

- Las conversiones especificadas como “no necesarias” no cambiarán el valor de operación de uso.

Origen	Destino					
	Windows Server como BYOL	Windows Server como modelo con licencia incluida	Windows Server como BYOL SQL Server como BYOL	Windows Server como modelo con licencia incluida SQL Server como BYOL	Windows Server como BYOL SQL Server como modelo con licencia incluida	Windows Server como modelo con licencia incluida SQL Server como modelo con licencia incluida
Windows Server como BYOL (su propio medio)	No es necesario	Sí	No es necesario	Sí[1]	No se admite	Sí[1]
Windows Server como modelo con	Sí[2]	No es necesario	Sí [1, 2]	No se necesitan [3]	No se admite	Sí[1]

Origen	Destino					
licencia incluida (su propio medio)						
Windows Server como licencia incluida (imagen AWS proporcionada)	No ✗	No es necesario	No ✗	No se necesitan [3]	No se admite	Sí [1]
Windows Server como BYOL (su propio medio)	No se necesitan [4]	Sí	No es necesario	Sí	No se admite	Sí
SQL Server como BYOL (su propio medio)						

Origen	Destino					
Windows Server como modelo con licencia incluida (su propio medio)	Sí[2]	No se necesitan [4]	Sí[2]	No es necesario	No se admite	Sí
SQL Server como BYOL (su propio medio)						
Windows Server como licencia incluida (imagen AWS proporcionada)	No ✗	No se necesitan [4]	No ✗	No es necesario	No se admite	Sí
SQL Server como BYOL (su propio medio)						

Origen	Destino					
Windows Server como BYOL (su propio medio)	No se admite	No se admite	No se admite	No se admite	No se admite	No se admite
SQL Server como modelo con licencia incluida						

Origen	Destino					
Windows Server como licencia incluida (imagen AWS proporcionada o contenido multimedia)	No ✗	No ✗	No ✗	No ✗	No se admite	No es necesario
SQL Server como licencia incluida (imagen AWS proporcionada)						

Origen	Destino					
Windows Server como modelo con licencia incluida (su propio medio)	Sí [2, 5, 6]	Sí[5]	Sí[2]	Sí	No se admite	No es necesario
SQL Server como modelo con licencia incluida (su propio medio)						

Origen	Destino					
Windows Server como licencia incluida (imagen AWS proporcionada)	No ✗	Sí[5]	No ✗	Sí	No se admite	No es necesario
SQL Server como modelo con licencia incluida (su propio medio)						

✗ Debe implementar una nueva instancia con una configuración alternativa, ya que no se admite la conversión a los tipos de licencia de destino. Para obtener más información, consulte Compatibilidad de medios.

Para otros casos, es posible que deba seguir los siguientes pasos para realizar una conversión de licencia:

[1] Primero debe instalar SQL Server antes de convertirlo a BYOL para SQL Server.

[2] Primero debe modificar la configuración de Windows a fin de usar su propio servidor KMS para la activación de la licencia. Para obtener más información, consulte Convert Windows Server from license included to BYOL.

[3] Primero debe instalar SQL Server cuando realice la conversión de un origen sin SQL Server a un destino con SQL Server (independientemente del tipo de licencia de SQL Server).

[4] Primero debe desinstalar SQL Server cuando realice la conversión de un origen con SQL Server a un destino sin SQL Server (independientemente del tipo de licencia de SQL Server).

[5] Primero debe desinstalar SQL Server antes de convertirlo a SQL Server con licencia incluida.

[6] Primero debe realizar los pasos para [2] y [5]. Una vez completados estos pasos, debe convertir el tipo de licencia a Windows Server como modelo con licencia incluida y, a continuación, convertir el tipo de licencia una vez más a Windows Server como BYOL.

Tipos de suscripción aptos para Linux en License Manager

La conversión de tipos de licencia está disponible para las versiones compatibles de Ubuntu. Las versiones compatibles incluyen actualizaciones como Ubuntu 18.04.1 LTS. Al convertir una suscripción a Ubuntu Pro, las actualizaciones de seguridad se proporcionan durante cinco años adicionales. Para obtener más información, consulte Ubuntu Pro en la documentación de Canonical.

Se puede usar la conversión de tipos de licencia con las siguientes versiones de Ubuntu:

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

Detalles del sistema operativo	Operación de uso
Linux/Unix	RunInstances
Ubuntu Pro	RunInstancesTipos de suscripción de Linux aptos para License Manager ----sep----:0g00

Rutas de conversión para Linux

Ubuntu

Puede convertir cualquier versión compatible de Ubuntu LTS a Ubuntu Pro. Si necesita hacer una conversión de Ubuntu Pro a Ubuntu LTS, tendrá que enviar una solicitud a Soporte. Para obtener más información, consulte Creación de un caso de soporte.

Requisitos previos de conversión para los tipos de licencia de License Manager

Para convertir los tipos de licencia con License Manager, existen una serie de requisitos previos generales y específicos del sistema operativo.

Temas

- General
- Windows
- Linux

General

Debe cumplir los siguientes requisitos previos generales antes de realizar una conversión de tipo de licencia:

- Cuenta de AWS Debe estar registrado en License Manager. Consulte Comience a utilizar License Manager.
- La instancia de destino debe ejecutarse en. AWS No se admiten las instancias locales.
- La instancia de destino debe estar detenida antes de convertir el tipo de licencia. Para obtener más información, consulta Detener e iniciar tu instancia en la Guía del EC2 usuario de Amazon.
- Si la protección contra interrupciones está habilitada en la instancia de destino, se producirá un error en el proceso de conversión. Para obtener más información, consulte Solución de problemas de conversión de tipos de licencia en License Manager.
- La instancia de destino debe configurarse con AWS Systems Manager Inventory. Para obtener más información, consulte Configuración de Systems Manager para EC2 instancias e AWS Systems Manager inventario en la Guía del AWS Systems Manager usuario.
- El usuario o rol debe incluir los permisos siguientes:
  - `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`

Para obtener más información acerca de Systems Manager Inventory, consulte AWS Systems Manager Inventory.

Windows

Las instancias de Windows deben cumplir los siguientes requisitos previos:

- Las instancias que se lanzaron originalmente desde una imagen de máquina de Amazon (AMI) proporcionada por Amazon no son aptas para la conversión de tipos de licencia al modelo BYOL. La EC2 instancia original de Amazon debe lanzarse desde la imagen de su propia máquina virtual (VM). Para obtener más información sobre la conversión de una máquina virtual a Amazon EC2, consulte VM Import/Export.
- Para cambiar la licencia de SQL Server a BYOL, SQL Server debe haberse instalado con su propio medio.

Linux

Las instancias de Linux deben cumplir los siguientes requisitos previos:

- Las instancias deben ejecutar Ubuntu LTS.
- Ubuntu Pro Client debe haberse instalado en el sistema operativo Ubuntu.

- Ejecute el siguiente comando para confirmar si se ha instalado Ubuntu Pro Client:

```
pro --version
```

- Si no encuentra el comando o necesita actualizar la versión, ejecute el siguiente comando para instalar Ubuntu Pro Client:

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

- Las instancias deben poder acceder a varios puntos de conexión para activar su suscripción a Ubuntu Pro y recibir actualizaciones. Debe permitir que el tráfico de salida de la instancia a través del puerto TCP 443 llegue a los siguientes puntos de conexión:
  - contracts.canonical.com: se utiliza para la activación de Ubuntu Pro.
  - esm.ubuntu.com: se utiliza para el acceso al repositorio de APT para la mayoría de los servicios.
  - api.snapcraft.io: se utiliza para instalar y ejecutar instantáneas.
  - dashboard.snapcraft.io: se utiliza para instalar y ejecutar instantáneas.
  - login.ubuntu.com: se utiliza para instalar y ejecutar instantáneas.
  - cloudfront.cdn.snapcraftcontent.com: se utiliza para realizar descargas desde redes de desarrollo de contenido (). CDNs
  - livepatch.canonical.com: se utiliza para descargar parches del servidor Livepatch.

  Para obtener más información, consulte los requisitos de red del cliente Ubuntu Pro en la documentación del cliente Ubuntu Pro y los requisitos de red en la documentación de Canonical Snapcraft.

Convertir un tipo de licencia en License Manager

Puede convertir las licencias de Windows, las licencias de Microsoft SQL Server y las suscripciones a Ubuntu Linux mediante la consola License Manager o AWS CLI. Es posible que deba seguir una serie de pasos adicionales para convertir la licencia o suscripción en el sistema operativo de la instancia.

Puede convertir los tipos de licencia mediante la consola License Manager o la AWS CLI. Al crear una conversión de tipos de licencia, License Manager valida los productos de facturación de la instancia. Si estas validaciones preliminares se realizan correctamente, License Manager crea una conversión de tipos de licencia. Puede comprobar el estado de la conversión de un tipo de

licencia mediante los `get-license-conversion-task` AWS CLI comandos `list-license-conversion-tasks` y.

License Manager puede actualizar los recursos asociados a sus licencias autoadministradas como parte de una conversión de tipos de licencia. En concreto, para cualquier licencia autoadministrada con reglas de detección automatizada de tipo `License Included`, License Manager desasocia el recurso de la conversión de tipos de licencia de la licencia si la regla de detección automatizada `license included` excluye explícitamente el recurso.

Por ejemplo, si su licencia autoadministrada contiene dos reglas de detección automatizada y las dos excluyen Windows Server como modelo con licencia incluida, la conversión de tipos de licencia BYOL a Windows Server como modelo con licencia incluida provocará la desasociación de la instancia de la licencia autoadministrada. Sin embargo, si solo una de las dos reglas de detección automatizada contiene una regla `License Included`, la instancia no se desasocia.

No debe iniciar ni detener la instancia mientras se esté realizando una conversión de tipos de licencia. Cuando la conversión de tipos de licencia se realiza correctamente, su estado cambia de `IN_PROGRESS` a `SUCCEEDED`. Si License Manager encuentra problemas durante el flujo de trabajo, actualiza el estado de la conversión de tipos de licencia a `FAILED` y actualiza el mensaje de estado con un mensaje de error.

> **Note**
>
> La información del producto de facturación de la AMI utilizada para lanzar una instancia no cambia al convertir el tipo de licencia. Para obtener información de facturación precisa, usa la EC2 `DescribeInstances`API de Amazon. Además, si tienes flujos de trabajo existentes en los que se busca información de facturación AMIs, actualiza esos flujos de trabajo para utilizarlos`DescribeInstances`.

Contenido

- Convierta un tipo de licencia para Windows y SQL Server en License Manager
  - Límites de conversión de tipos de licencia
  - Cómo convertir un tipo de licencia mediante la consola License Manager
  - Convierta un tipo de licencia mediante el AWS CLI
- Convierta un tipo de licencia para Linux en License Manager
  - Consideraciones sobre la conversión de tipos de licencia

- Cómo convertir un tipo de licencia mediante la consola License Manager
- Convierta un tipo de licencia mediante el AWS CLI
- Elimine una suscripción a Ubuntu Pro

Convierta un tipo de licencia para Windows y SQL Server en License Manager

Puede usar la consola License Manager o la AWS CLI para convertir el tipo de licencia de las instancias de Windows y SQL Server aptas.

Temas

- Límites de conversión de tipos de licencia
- Cómo convertir un tipo de licencia mediante la consola License Manager
- Convierta un tipo de licencia mediante el AWS CLI

Límites de conversión de tipos de licencia

> **Important**
>
> El uso del software de Microsoft está sujeto a las condiciones de la licencia de Microsoft. Usted es responsable de cumplir las condiciones de la licencia de Microsoft. Esta documentación se proporciona para su comodidad y no tiene derecho a basarse en lo que aquí se describe. Esta documentación no constituye asesoramiento legal alguno. Si tiene alguna duda acerca de los derechos de las licencias del software de Microsoft, consúltesela a su equipo legal, Microsoft o su distribuidor de Microsoft.

License Manager restringe los tipos de conversiones de licencias que se pueden crear de acuerdo con el Contrato de licencia para proveedores de servicios (SPLA) de Microsoft. Algunas de las restricciones a las que está sujeta la conversión de tipos de licencia se enumeran a continuación. Esta lista no es exhaustiva y está sujeta a cambios.

- La EC2 instancia de Amazon debe lanzarse desde tu propia imagen de máquina virtual (VM).
- SQL Server con licencia incluida no se puede ejecutar en un host dedicado.
- Una instancia de SQL Server con licencia incluida debe tener al menos 4 v. CPUs

Cómo convertir un tipo de licencia mediante la consola License Manager

Puede convertir un tipo de licencia mediante la consola License Manager.

> **Note**
>
> Solo se muestran las instancias que están detenidas y que se han asociado mediante AWS Systems Manager Inventory.

Pasos para iniciar una conversión de tipos de licencia en la consola

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Conversión del tipo de licencia y, a continuación, Crear conversión del tipo de licencia.
3. En Sistema operativo de origen, elija la plataforma de la instancia que quiera convertir:
   - Ubuntu LTS
   - Windows BYOL
   - Windows como modelo con licencia incluida
4. (Opcional) Filtre las instancias disponibles especificando un valor para el ID de la instancia o el Valor de operación de uso.
5. Seleccione las instancias cuyas licencias desee convertir y, a continuación, elija Siguiente.
6. Introduzca el Valor de operación de uso para el tipo de licencia, seleccione la licencia a la que va a convertir y pulse Siguiente.
7. Confirme su satisfacción con la configuración de conversión del tipo de licencia y seleccione Iniciar conversión.

Puede ver el estado de la conversión del tipo de licencia desde el panel de conversión del tipo de licencia. La columna Estado de la conversión muestra el estado de la conversión como En curso, Completado o Error.

> **Important**
>
> Si convierte Windows Server de un modelo con licencia incluida a un modelo BYOL, debe activar Windows de acuerdo con su acuerdo de licencia con Microsoft. Para obtener más información, consulta Convert Windows Server from license included to BYOL.

Convierta un tipo de licencia mediante el AWS CLI

Para iniciar una conversión de tipos de licencia en la AWS CLI:

Determine el tipo de licencia de la instancia

1. Compruebe que ha instalado y configurado la AWS CLI. Para obtener más información, consulte Instalar, actualizar y desinstalar la AWS CLI y Configuración de la AWS CLI.

   > **Important**
   >
   > Es posible que necesite actualizar el AWS CLI para ejecutar determinados comandos y recibir todos los resultados necesarios en los siguientes pasos.

2. Compruebe que tiene permisos para ejecutar el `create-license-conversion-task-for-resource` AWS CLI comando. Si desea ayuda con esto, consulte Cree políticas de IAM para License Manager.
3. Para determinar el tipo de licencia actualmente asociado a la instancia, ejecuta el siguiente AWS CLI comando. Sustituya el ID de la instancia por el ID de la instancia para la que desea determinar el tipo de licencia.

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

4. A continuación se muestra una respuesta de ejemplo al comando `describe-instances`. Tenga en cuenta que el valor `UsageOperation` es el código de información de facturación asociado a la licencia. `UsageOperationUpdateTime` es el momento en que se actualizó el código de facturación. Para obtener más información, consulte DescribeInstancesen la referencia de la EC2 API de Amazon.

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

> **Note**
>
> La operación de uso de Windows Server con SQL Server Enterprise BYOL es la misma que la operación de uso de Windows BYOL, ya que se facturan de forma idéntica.

Convierta Windows Server como modelo con licencia incluida a modelo BYOL

Al convertir Windows Server como modelo con licencia incluida a modelo BYOL, License Manager no activa Windows automáticamente. Debes cambiar el servidor KMS de tu instancia del servidor AWS KMS a tu propio servidor KMS.

> **Important**
>
> Para pasar de una licencia incluida a BYOL, la EC2 instancia original de Amazon debe lanzarse desde la imagen de su propia máquina virtual (VM). Para obtener más información sobre la conversión de una máquina virtual a Amazon EC2, consulte VM Import/Export. Las instancias que se lanzaron originalmente desde una imagen de máquina de Amazon (AMI) no son aptas para la conversión de licencias al modelo BYOL.

Consulte su acuerdo de licencia con Microsoft para determinar qué métodos puede utilizar para activar Microsoft Windows Server. Por ejemplo, si utiliza un servidor de KMS, debe obtener la dirección del servidor de KMS de la configuración BYOL original de la instancia.

1. Para convertir el tipo de licencia de la instancia, ejecute el siguiente comando y sustituya el ARN por el ARN de la instancia que desee convertir:

```
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. Para activar Windows después de convertir la licencia, debe apuntar el servidor de KMS de Windows Server de su sistema operativo a sus propios servidores de KMS. Inicie sesión en la instancia de Windows y ejecute el comando siguiente:

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

Convierta Windows Server BYOL a un modelo con licencia incluida

Al convertir Windows Server de BYOL a licencia incluida, License Manager cambia automáticamente el servidor KMS de la instancia al servidor AWS KMS.

Para convertir el tipo de licencia de la instancia de BYOL a un modelo con licencia incluida, ejecute el siguiente comando y sustituya el ARN por el ARN de la instancia que desee convertir:

```
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
```

Convierte Windows Server y SQL Server de BYOL a licencia incluida

Puede cambiar varios productos al mismo tiempo. Por ejemplo, puede convertir Windows Server y SQL Server al mismo tiempo en una misma conversión de tipos de licencia.

Para convertir el tipo de licencia de la instancia de Windows Server de BYOL a modelo con licencia incluida, así como SQL Server Standard de BYOL a modelo con licencia incluida, ejecute el siguiente comando y sustituya el ARN por el ARN de la instancia que desee convertir:

```
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
```

Convierta un tipo de licencia para Linux en License Manager

Puede usar la consola License Manager o la AWS CLI para convertir el tipo de licencia de las instancias de Ubuntu LTS aptas.

Temas

- Consideraciones sobre la conversión de tipos de licencia
- Cómo convertir un tipo de licencia mediante la consola License Manager
- Convierta un tipo de licencia mediante el AWS CLI
- Elimine una suscripción a Ubuntu Pro

Consideraciones sobre la conversión de tipos de licencia

Algunas de las consideraciones a las que está sujeta la conversión de tipos de licencia se enumeran a continuación. Esta lista no es exhaustiva y está sujeta a cambios.

Conversión a Ubuntu

- La instancia debe ejecutar Ubuntu LTS para poder convertir el tipo de licencia a Ubuntu Pro.
- No se puede usar la conversión de tipos de licencia para una suscripción a Ubuntu Pro. Para eliminar una suscripción a Ubuntu Pro, consulte Elimine una suscripción a Ubuntu Pro.
- Ubuntu Pro no está disponible como instancia reservada. Para ahorrar con los precios de las instancias bajo demanda, le recomendamos que utilice Ubuntu Pro con Savings Plans. Para obtener más información, consulte Reserved Instances en la Guía del EC2 usuario de Amazon y What are Savings Plans? en la Guía del usuario de Savings Plans.

Cómo convertir un tipo de licencia mediante la consola License Manager

Puede convertir un tipo de licencia mediante la consola License Manager.

> **Note**
>
> Solo se muestran las instancias que están detenidas y que se han asociado mediante AWS Systems Manager Inventory.

Pasos para iniciar una conversión de tipos de licencia en la consola

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Conversión del tipo de licencia y, a continuación, Crear conversión del tipo de licencia.

3. En Sistema operativo de origen, elija la plataforma de la instancia que quiera convertir:
   - Ubuntu LTS
   - Windows BYOL
   - Windows como modelo con licencia incluida
4. (Opcional) Filtre las instancias disponibles especificando un valor para el ID de la instancia o el Valor de operación de uso.
5. Seleccione las instancias cuyas licencias desee convertir y, a continuación, elija Siguiente.
6. Introduzca el Valor de operación de uso para el tipo de licencia, seleccione la licencia a la que va a convertir y pulse Siguiente.
7. Confirme su satisfacción con la configuración de conversión del tipo de licencia y seleccione Iniciar conversión.

Puede ver el estado de la conversión del tipo de licencia desde el panel de conversión del tipo de licencia. La columna Estado de la conversión muestra el estado de la conversión como En curso, Completado o Error.

Convierta un tipo de licencia mediante el AWS CLI

Para iniciar una conversión de tipo de licencia en AWS CLI, debe confirmar que el tipo de licencia de su instancia es apto y, a continuación, realizar una conversión del tipo de licencia para cambiarlo a la suscripción requerida. Para obtener más información sobre los tipos de suscripción aptos, consulte Tipos de suscripción aptos para Linux en License Manager.

Determine el tipo de licencia de la instancia

Compruebe que ha instalado y configurado la AWS CLI. Para obtener más información, consulte Instalación, actualización y desinstalación AWS CLI y Configuración de AWS CLI.

> **Important**
>
> Puede que necesite actualizar el AWS CLI para ejecutar determinados comandos y recibir todos los resultados necesarios en los siguientes pasos. Compruebe que tiene permisos para ejecutar el `create-license-conversion-task-for-resource` AWS CLI comando. Para obtener más información, consulte Cree políticas de IAM para License Manager.

Para determinar el tipo de licencia actualmente asociado a la instancia, ejecuta el siguiente AWS CLI comando. Sustituya el ID de la instancia por el ID de la instancia para la que desea determinar el tipo de licencia:

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

A continuación se muestra una respuesta de ejemplo al comando `describe-instances`. El UsageOperationvalor es el código de información de facturación asociado a la licencia. Un valor de operación de uso de `RunInstances` indica que la instancia utiliza la licencia proporcionada por AWS . `UsageOperationUpdateTime` es el momento en que se actualizó el código de facturación. Para obtener más información, consulte DescribeInstancesen la referencia de la EC2 API de Amazon.

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

Haga la conversión a Ubuntu Pro

Antes de convertir tu instancia de Ubuntu LTS a Ubuntu Pro, tu instancia debe tener el acceso saliente a Internet configurado para recuperar un token de licencia de los servidores de Canonical e instalar el cliente de Ubuntu Pro. Para obtener más información, consulte Requisitos previos de conversión para los tipos de licencia de License Manager.

Para convertir Ubuntu LTS a Ubuntu Pro, sigue estos pasos:

1. Ejecuta el siguiente comando AWS CLI mientras especificas el ARN de la instancia:

   ```
   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. Ejecute el siguiente comando desde la propia instancia para recuperar los detalles sobre el estado de la suscripción a Ubuntu Pro:

```
pro status
```

3. Confirme que los datos de salida indican que la instancia tiene una suscripción válida a Ubuntu Pro:

```
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
```

Elimine una suscripción a Ubuntu Pro

La conversión de tipos de licencia solo se puede utilizar para convertir Ubuntu LTS a Ubuntu Pro. Si necesita hacer una conversión de Ubuntu Pro a Ubuntu LTS, tendrá que enviar una solicitud a Soporte. Para obtener más información, consulte Creación de un caso de soporte.

Conversión de arrendamiento en License Manager

Puede cambiar la tenencia de una instancia para que se adapte mejor a su caso de uso. Puede usar el modify-instance-placement AWS CLI comando para cambiar entre los siguientes arrendamientos:

- Compartida
- Dedicated Instance
- Host dedicado
- Grupos de recursos de host

Su cuenta debe tener un host dedicado con capacidad disponible para iniciar la instancia a fin de cambiar al tipo de tenencia de hosts dedicados. Para obtener más información acerca de cómo trabajar con hosts dedicados, consulte Utilizar Hosts dedicados en la Guía del usuario de Amazon Elastic Compute Cloud.

Para pasar al tipo de tenencia de grupos de recursos de host, debe tener al menos un grupo de recursos de host en su cuenta. Para lanzar una instancia a un grupo de recursos de hosts, la instancia debe tener el mismo conjunto de licencias asociadas al grupo de recursos de hosts. Para obtener más información, consulte Aloje grupos de recursos en License Manager.

Límites de conversión de tenencias

Las limitaciones siguientes se aplican a las conversiones de tenencias:

- El código de facturación de Linux está permitido en todos los tipos de tenencias.
- El código de facturación de Windows BYOL no está permitido en las tenencias compartidas.
- El código de facturación de Windows Server como modelo con licencia incluida está permitido en todos los tipos de tenencias.
- Todas las ediciones de SQL Server compatibles y los códigos de facturación incluidos en la licencia de SUSE (SLES) están permitidos en las instancias dedicadas y de arrendamiento compartido. Sin embargo, estos códigos de facturación no están permitidos en los hosts dedicados ni en los grupos de recursos de host.
- Los códigos de facturación incluidos en la licencia que no sean de Windows Server no están permitidos ni en los hosts dedicados ni en los grupos de recursos de host.

Cambie el arrendamiento de una instancia mediante el AWS CLI

Una instancia debe tener el estado `stopped` para poder cambiar su tenencia.

Ejecute el siguiente comando para detener la instancia:

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

Para cambiar una instancia de cualquier tenencia a una tenencia `default` o `dedicated`, ejecute los siguientes comandos:

`default`

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

`dedicated`

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

Para cambiar una instancia de cualquier tenencia a una tenencia `host` con ubicación automática, ejecute el siguiente comando:

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

Para cambiar una instancia de cualquier tenencia a una tenencia `host` con un host dedicado específico como destino, ejecute el siguiente comando:

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

Para cambiar una instancia de cualquier tenencia a una tenencia `host` que hace uso de un grupo de recursos de hosts, ejecute el siguiente comando:

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

Solución de problemas de conversión de tipos de licencia en License Manager

Temas de solución de problemas

- Activación de Windows
- La instancia [instance] se lanza desde una AMI propiedad de Amazon. Proporcione una instancia lanzada originalmente desde una AMI BYOL.
- No se pudo validar que la instancia [instance] se lanzara desde una AMI BYOL. Asegúrese de que SSM Agent se esté ejecutando en la instancia.
- Se produjo un error (InvalidParameterValueException) al llamar a la CreateLicenseConversionTaskForResource operación: ResourceId - [instance] se encuentra en un estado no válido para cambiar el tipo de licencia.
- EC2 instance [instance] no se pudo detener. Asegúrese de tener permisos para EC2 StopInstances.

Activación de Windows

La conversión de un tipo de licencia consta de varios pasos. En algunos casos, al convertir instancias de Windows Server de un modelo BYOL a un modelo con licencia incluida, los productos de facturación de una instancia se actualizan correctamente. Sin embargo, es posible que el servidor de KMS no cambie al servidor de AWS KMS.

Para solucionar este problema, siga los pasos de ¿Por qué falló la activación de Windows en mi instancia de EC2 Windows? para activar Windows ya sea con el Systems Manager AWSSupport-ActivateWindowsWithAmazonLicenseManual de automatización o inicie sesión en la instancia y cambie manualmente al servidor AWS KMS.

La instancia [instance] se lanza desde una AMI propiedad de Amazon. Proporcione una instancia lanzada originalmente desde una AMI BYOL.

Debe lanzar su instancia de Amazon EC2 Windows desde una AMI que haya importado para realizar una conversión del tipo de licencia al modelo Bring Your Own License (BYOL). Las instancias que se lanzaron originalmente desde una AMI propiedad de Amazon no son aptas para la conversión de tipos de licencia al modelo BYOL. Para obtener más información, consulte Requisitos previos de conversión para los tipos de licencia de License Manager.

No se pudo validar que la instancia [instance] se lanzara desde una AMI BYOL. Asegúrese de que SSM Agent se esté ejecutando en la instancia.

Para que la conversión de tipos de licencia se realice correctamente, la instancia debe haber estado antes en línea y Systems Manager debe haberla administrado para recopilar el inventario. AWS Systems Manager Agent (SSM Agent) recopilará el inventario de su instancia, que incluye detalles sobre el sistema operativo. Para obtener más información, consulte Verificación del estado de SSM Agent e inicio del agente y Solución de problemas de SSM Agent en la Guía del usuario de AWS Systems Manager .

Se produjo un error (InvalidParameterValueException) al llamar a la **`CreateLicenseConversionTaskForResource`** operación: ResourceId - [instance] se encuentra en un estado no válido para cambiar el tipo de licencia.

Para realizar una conversión de tipos de licencia, la instancia de destino debe estar detenida. Para obtener más información, consulte Requisitos previos de conversión para los tipos de licencia de License Manager y Solucionar problemas de detención de la instancia de la Guía del usuario de Amazon Elastic Compute Cloud.

EC2 instance [instance] no se pudo detener. Asegúrese de tener permisos para EC2 `StopInstances`.

Debe tener permisos para realizar la acción de la `StopInstances` EC2 API en la instancia de destino. Además, si la protección contra interrupciones está habilitada en la instancia de destino, se producirá un error en el proceso de conversión. Para obtener más información, consulte Detener e iniciar la instancia en la Guía del usuario de Amazon Elastic Compute Cloud.

Aloje grupos de recursos en License Manager

Los hosts EC2 dedicados de Amazon son servidores físicos con capacidad de EC2 instancia totalmente dedicada a su uso. Un grupo de recursos de host es una colección de hosts dedicados que se administran como una sola entidad. A medida que lanza las instancias, License Manager asigna los hosts y lanza las instancias en ellos en función de lo que haya configurado. Puede añadir hosts dedicados existentes a un grupo de recursos de host y aprovechar la administración automatizada de hosts con License Manager. Para obtener más información, consulta Hosts dedicados en la Guía del EC2 usuario de Amazon.

Puede usar los grupos de recursos de host para dividir los hosts según su propósito, por ejemplo, entre hosts de pruebas de desarrollo y hosts de producción, por unidades organizativas o según las restricciones de las licencias. Después de añadir un host dedicado a un grupo de recursos de host, no puede lanzar instancias directamente en el host dedicado, sino que debe lanzarlas mediante el grupo de recursos de host.

Configuración

Puede establecer la siguiente configuración para un grupo de recursos de host:

- Asignar hosts automáticamente: indica si Amazon EC2 puede asignar nuevos hosts en tu nombre en caso de que el lanzamiento de una instancia en este grupo de recursos de hosts supere su capacidad disponible.
- Liberar los anfitriones automáticamente: indica si Amazon EC2 puede liberar los hosts no utilizados en tu nombre. Un host no utilizado no tiene ninguna instancia en ejecución.
- Recuperar los hosts automáticamente: indica si Amazon EC2 puede mover instancias de un host que ha fallado inesperadamente a un nuevo host.
- Licencias autoadministradas asociadas: las licencias autoadministradas que se pueden usar para lanzar instancias en este grupo de recursos de host.

- (Opcional) Familias de instancias: los tipos de instancias que se pueden lanzar. De forma predeterminada, puede lanzar cualquier tipo de instancia que sea compatible con un host dedicado. Si hablamos de instancias basadas en Nitro, puede lanzar instancias con distintos tipos de instancias en el mismo grupo de recursos de host. De lo contrario, solo debe lanzar instancias con el mismo tipo de instancia en el mismo grupo de recursos de host.

Contenido

- Crear un grupo de recursos de host en License Manager
- Compartir un grupo de recursos de host en License Manager
- Agregar hosts dedicados a un grupo de recursos de hosts en License Manager
- Lance una instancia en un grupo de recursos de host en License Manager
- Modificar un grupo de recursos de hosts en License Manager
- Eliminar hosts dedicados de un grupo de recursos de hosts en License Manager
- Eliminar un grupo de recursos de hosts en License Manager

Crear un grupo de recursos de host en License Manager

Configure un grupo de recursos de host para permitir que License Manager administre sus hosts dedicados. Para aprovechar al máximo sus licencias más caras, puede asociar una o más licencias autoadministradas basadas en núcleos o sockets a su grupo de recursos de host. A fin de optimizar al máximo el uso de los hosts, puede permitir que todas las licencias autoadministradas basadas en núcleos o sockets se incorporen a su grupo de recursos de host.

Procedimiento para crear un grupo de recursos de host

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Grupos de recursos de host.
3. Seleccione Crear grupo de recursos de host.
4. Para ver los Detalles del grupo de recursos de host, especifique un nombre y una descripción para el grupo de recursos de host.
5. Para la configuración de administración de hosts EC2 dedicados, habilite o deshabilite las siguientes configuraciones según sea necesario:

    - Asignar hosts automáticamente

- Liberar hosts automáticamente
- Recuperar hosts automáticamente

6. (Opcional) Para Configuración adicional, seleccione las familias de instancias que puede lanzar en el grupo de recursos de host.
7. Para las licencias autoadministradas, seleccione una o más licencias autoadministradas basadas en núcleos o sockets.
8. (Opcional) Para Etiquetas, agregue una o más etiquetas.
9. Seleccione Crear.

Compartir un grupo de recursos de host en License Manager

Puede usarlo AWS Resource Access Manager para compartir sus grupos de recursos de host a través de AWS Organizations. Después de compartir un grupo de recursos de host y una licencia autoadministrada, las cuentas miembro pueden lanzar instancias en el grupo de recursos de host compartido. Los nuevos hosts se asignan a la cuenta propietaria del grupo de recursos de host. La cuenta miembro es la propietaria de las instancias. Para obtener más información, consulte la AWS RAM Guía del usuario de .

Agregar hosts dedicados a un grupo de recursos de hosts en License Manager

Puede agregar los hosts existentes a un grupo de recursos de hosts desde la AWS Management Console AWS CLI, o la AWS API. Para agregar sus hosts, debe ser el propietario de la AWS cuenta en la que creó el host dedicado y los grupos de recursos de host. Si su grupo de recursos de host incluye los tipos de instancias y licencias autoadministradas permitidos, el host que añada debe cumplir también estos requisitos.

> **Note**
>
> Si detiene las instancias y desea reiniciarlas, debe realizar las dos tareas siguientes:
>
> - Modificar la instancia para que apunte al grupo de recursos de host.
> - Asociar las licencias autoadministradas para que coincidan con el grupo de recursos de host.

No hay límite en la cantidad de hosts dedicados que puede agregar a un grupo de recursos de hosts. Para obtener más información sobre grupos de recursos, consulte la Guía del usuario de AWS Resource Groups.

Siga estos pasos para agregar uno o varios hosts dedicados a un grupo de recursos:

1. Inicie sesión en la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Seleccione Grupos de recursos de host.
3. En la lista de nombres de grupos de recursos de host, haga clic en el nombre del grupo de recursos de host al que desee agregar el host dedicado.
4. Seleccione Hosts dedicados.
5. Elija Agregar.
6. Elija uno o más hosts dedicados para agregarlos al grupo de recursos de host.
7. Elija Agregar.

   La adición del host puede tardar entre 1 y 2 minutos y, después, aparecerá en la lista de hosts dedicados.

Lance una instancia en un grupo de recursos de host en License Manager

Al lanzar una instancia, puede especificar un grupo de recursos de host. Por ejemplo, puede ejecutar el comando run-instances. Debe asociar una licencia autoadministrada basada en núcleos o sockets a la AMI.

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

También puedes usar la EC2 consola Amazon. Para obtener más información, consulte Lanzamiento de instancias en un grupo de recursos de hosts en la Guía del EC2 usuario de Amazon.

Modificar un grupo de recursos de hosts en License Manager

Puede modificar la configuración de un grupo de recursos de host en cualquier momento. No puede establecer el límite de hosts por debajo del número de hosts existentes en el grupo de recursos de

host. No puede eliminar un tipo de instancia si hay una instancia de ese tipo en ejecución en el grupo de recursos de host.

Procedimiento para modificar un grupo de recursos de host

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Grupos de recursos de host.
3. Seleccione el grupo de recursos de host y Acciones, Editar.
4. Modifique la configuración según sea necesario.
5. Elija Guardar cambios.

Eliminar hosts dedicados de un grupo de recursos de hosts en License Manager

Al eliminar un host del grupo de recursos de host, la instancia que se ejecuta en el host permanece en el host. Las instancias asociadas al grupo de recursos de host permanecen asociadas al grupo, y las instancias directamente conectadas al host a través de la afinidad mantienen la misma propiedad. Si comparte el grupo de recursos del host con otras AWS cuentas, License Manager elimina automáticamente el host compartido y los consumidores reciben una notificación de desalojo para mover sus instancias del host en un plazo de 15 días. Para trabajar con un host dedicado que se ha eliminado de un grupo de recursos de hosts, consulte Trabajar con hosts dedicados en la Guía del EC2 usuario de Amazon.

Siga estos pasos para eliminar un host dedicado de un grupo de recursos:

1. Inicie sesión en la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Seleccione Grupos de recursos de host.
3. Haga clic en el nombre del recurso de host del que desee eliminar un host dedicado.
4. Seleccione Hosts dedicados.
5. Elija el host dedicado que desee eliminar del grupo de recursos de host. O bien, puede buscar un host dedicado por ID de host, tipo de host, estado del host o zona de disponibilidad.
6. Elija Eliminar.
7. Para confirmar, vuelva a seleccionar Eliminar.

Eliminar un grupo de recursos de hosts en License Manager

Puede eliminar un grupo de recursos de host si no tiene hosts.

Procedimiento para eliminar un grupo de recursos de host

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Grupos de recursos de host.
3. Seleccione el grupo de recursos de host y Acciones, Eliminar.
4. Cuando se le pida confirmación, elija Delete (Eliminar).

Búsqueda en el inventario en License Manager

License Manager le permite detectar aplicaciones en las instalaciones mediante Systems Manager Inventory y, a continuación, asociar reglas de asignación de licencias a las aplicaciones. Después de adjuntar las reglas de licencia a estos servidores, puede rastrearlas junto con sus AWS servidores en el panel de control de License Manager.

Sin embargo, License Manager no puede validar las reglas de asignación de licencias para estos servidores en el momento de su lanzamiento o terminación. Para conservar la información sobre los que no son AWS servidores up-to-date, debe actualizar periódicamente la información del inventario mediante la sección de búsqueda de inventario de la consola de License Manager.

Systems Manager almacena datos en los datos de inventario durante 30 días. Durante este periodo, License Manager contabiliza una instancia administrada como activa aunque no permita hacer ping. Una vez que los datos del inventario se hayan depurado de Systems Manager, License Manager marca la instancia como inactiva y actualiza los datos del inventario local. Para mantener la precisión de los recuentos de instancia administrados, recomendamos anular el registro de las instancias de forma manual en Systems Manager para que License Manager puede ejecutar operaciones de limpieza.

La consulta del inventario de Systems Manager requiere una sincronización de datos de recursos para almacenar el inventario en un bucket de Amazon S3, y Amazon Athena para agregar los datos de inventario de las cuentas de la organización AWS Glue y proporcionar una experiencia de consulta rápida. Para obtener más información, consulte Uso de funciones vinculadas a servicios para License Manager.

El seguimiento del inventario de recursos también es útil si su organización no impide que los usuarios de AWS creen instancias derivadas de las AMI o instalen software adicional en las instancias en ejecución. License Manager le proporciona un mecanismo para detectar fácilmente estas instancias y aplicaciones mediante la búsqueda en el inventario. Puede adjuntar reglas a estos recursos descubiertos y realizar un seguimiento y validarlos de la misma manera que las instancias creadas a partir de las gestionadas. AMIs

Contenido

- Trabaje con la búsqueda de inventario en License Manager
- Descubrimiento automatizado del inventario en License Manager

Trabaje con la búsqueda de inventario en License Manager

License Manager utiliza Systems Manager Inventory para detectar el software en las instalaciones. Tras asociar una licencia autoadministrada a los servidores en las instalaciones, License Manager recopila periódicamente el inventario de software y actualiza la información sobre licencias y sus paneles para informar sobre el uso.

Tareas

- Configurar la búsqueda de inventario
- Utilice la búsqueda de inventario
- Añada reglas de descubrimiento automático a una licencia autogestionada
- Asocie una licencia autogestionada a la búsqueda de inventario
- Desasocie una licencia autogestionada de un recurso

Configurar la búsqueda de inventario

Complete los siguientes requisitos antes de utilizar la búsqueda en el inventario de recursos:

- Habilite la detección de inventario entre cuentas integrando License Manager con su AWS Organizations cuenta. Para obtener más información, consulte Configuración en License Manager.
- Cree licencias autoadministradas para administrar servidores y aplicaciones. Por ejemplo, cree una licencia autoadministrada que refleje las condiciones del acuerdo de licencia con Microsoft para SQL Server Enterprise.

Utilice la búsqueda de inventario

Siga los pasos que se describen a continuación para hacer búsquedas en el inventario de recursos. Puede buscar aplicaciones por su nombre (por ejemplo, nombres que comiencen por “SQL Server”) y el tipo de licencia incluida (por ejemplo, una licencia que no sea para “SQL Server Web”).

Busque en su inventario de recursos

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación, seleccione Búsqueda en el inventario.
3. (Opcional) Puede especificar las opciones de filtro para agilizar los resultados de la búsqueda de la siguiente manera.

   EC2 Recursos de Amazon

Nombre del filtro	Descripción	Logical operators (Operadores lógicos)	Valores admitidos
ID de recurso	El ID del recurso.	`Equals`, `Not equals`	
ID de cuenta	El ID de la AWS cuenta propietaria del recurso.	`Equals`, `Not equals`	
nombre de la plataforma	La plataforma del sistema operativo del recurso.	`Equals`, `Not equals`, `Begins with`, `Contains`	
Nombre de la aplicación	Nombre de la aplicación.	`Equals`, `Begins with`	
Nombre incluido en la licencia	El tipo de licencia incluida.	`Equals`, `Not equals`	• `SQL Server Enterprise` •

Nombre del filtro	Descripción	Logical operators (Operadores lógicos)	Valores admitidos
			`SQL Server Standard` • `SQL Server Web` • `Windows Server Datacenter`
Etiqueta	Una clave de etiqueta de metadatos y un valor opcional que se asigna al recurso. Tenga en cuenta que el operador `Not equals` lógico solo está disponible si la detección entre cuentas está habilitada.	`Equals`, `Not equals`	

Recursos de Amazon RDS

Nombre del filtro	Descripción	Logical operators (Operadores lógicos)	Valores admitidos
Edición del motor	La edición del motor de base de datos.	`Equals`	• `oracle-ee` • `oracle-se` • `oracle-se1` • `oracle-se2` • `db2-se` • `db2-ae`

Nombre del filtro	Descripción	Logical operators (Operadores lógicos)	Valores admitidos
Paquete de licencias (solo Oracle)	El módulo de administración asociado a una licencia de Amazon RDS for Oracle.	`Equals`	• `Spatial and Graph` • `Active Data Guard` • `Label Security` • `Oracle On-Line Analytical Processing (OLAP)` • `Diagnosti c Pack and Tuning Pack`

Para obtener más información sobre las licencias de productos de bases de datos de Amazon RDS, consulte las opciones de licencia de RDS para Oracle o las opciones de licencia de RDS para Db2 en la Guía del usuario de Amazon RDS.

Añada reglas de descubrimiento automático a una licencia autogestionada

Tras añadir la información del producto a la licencia autoadministrada, License Manager puede realizar un seguimiento del uso de las licencias en las instancias que tienen esos productos instalados. Para obtener más información, consulte Descubrimiento automatizado del inventario en License Manager.

Procedimiento para añadir reglas de detección automatizada a una licencia autoadministrada

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.

2. Abra la página Búsqueda en el inventario.
3. Seleccione el recurso y elija Agregar reglas de detección automatizada.
4. Para Licencia autoadministrada, seleccione una licencia autoadministrada.
5. Especifique los productos que desea detectar y controlar.
6. (Opcional) Seleccione Detener el seguimiento de instancias cuando el software se desinstale para que la licencia pueda volver a utilizarse una vez que License Manager detecte que el software se ha desinstalado y ha transcurrido cualquier período de afinidad de licencia.
7. (Opcional) Para excluir los recursos de la detección automática, seleccione Agregar regla de exclusión.

   > **Note**
   >
   > Las reglas de exclusión no se aplican a los productos de Amazon RDS (como RDS para Oracle y RDS para Db2).

   a. Elija una Propiedad por la que filtrar. Actualmente, se admiten ID de cuenta y Etiqueta.
   b. Introduzca la información para identificar esa propiedad. Para un ID de cuenta, especifique el ID de AWS cuenta de 12 dígitos como valor. Para Etiqueta, introduzca un par clave-valor.
   c. Repita el paso 7 para añadir reglas adicionales.
8. Elija Agregar.

Asocie una licencia autogestionada a la búsqueda de inventario

Una vez que haya identificado los recursos no administrados que necesita administrar, puede asociarlos manualmente a una licencia autoadministrada, en lugar de utilizar la detección automatizada.

Procedimiento para asociar una licencia autoadministrada a un recurso

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Abra la página Búsqueda en el inventario.
3. Seleccione el recurso y elija Asociar una licencia autoadministrada.
4. Para Nombre de licencia autoadministrada, seleccione una licencia autoadministrada.
5. (Opcional) Seleccione Compartir licencia autoadministrada con todas mis cuentas miembro.

6. Elija Asociar.

Desasocie una licencia autogestionada de un recurso

Si las condiciones de las licencias de sus proveedores de software cambian, puede desasociar los recursos que se asociaron manualmente y, a continuación, eliminar la licencia autoadministrada.

Procedimiento para desasociar una licencia autoadministrada de un recurso

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Licencia autoadministrada.
3. Elija el nombre de la licencia autoadministrada.
4. Seleccione Recursos.
5. Seleccione cada uno de los recursos que desee desasociar de la licencia autoadministrada y elija Desasociar recurso.

Descubrimiento automatizado del inventario en License Manager

License Manager utiliza el inventario de Systems Manager para detectar el uso del software en las EC2 instancias de Amazon y en las instancias locales. Si añade la información del producto a la licencia autoadministrada, License Manager puede realizar un seguimiento del uso de las instancias que tienen esos productos instalados. También puede especificar reglas de exclusión en función de su acuerdo de licencias para decidir qué instancias excluir. Puede excluir las instancias que pertenezcan a una AWS cuenta IDs o estén asociadas a etiquetas de recursos para que no se tengan en cuenta para el descubrimiento automatizado

La detección automatizada se puede añadir a un nuevo conjunto de licencias, a una licencia autoadministrada existente o a los recursos de su inventario. Las reglas para el descubrimiento automatizado se pueden editar en cualquier momento a través de la CLI mediante el comando UpdateLicenseConfigurationAPI. Para editar las reglas en la consola, debe eliminar la licencia autoadministrada existente y crear una nueva.

Para utilizar la detección automatizada, debe añadir la información del producto a su licencia autoadministrada. Puede hacerlo al crear la licencia autoadministrada mediante Búsqueda en el inventario.

No puede desasociar manualmente las instancias a las que se ha hecho un seguimiento mediante detección automatizada. De forma predeterminada, la detección automatizada no desasocia

las instancias de las que se ha hecho un seguimiento una vez desinstalado el software. Puede configurar la detección automatizada para detener el seguimiento de las instancias cuando se desinstala el software.

Después de configurar la detección automatizada, puede realizar un seguimiento del uso de las licencias a través del panel de License Manager.

Requisitos previos

- Habilite la búsqueda de inventario entre cuentas integrando License Manager con su AWS Organizations cuenta. Para obtener más información, consulte Configuración en License Manager.

> **Note**
>
> Las cuentas individuales pueden configurar la detección automatizada, pero no pueden añadir reglas de exclusión.

- Instale el Systems Manager Inventory en sus instancias.

Procedimiento para configurar la detección automatizada al crear una licencia autoadministrada

Puede configurar reglas de detección automatizada y reglas de exclusión al crear una licencia autoadministrada. Para obtener más información, consulte Cree una licencia autogestionada en License Manager.

Procedimiento para añadir reglas de detección automatizada a una licencia autoadministrada existente

Utilice el siguiente proceso para añadir reglas de detección automatizada a las licencias autoadministradas existentes a través de la consola. También puede hacerlo desde el panel Búsqueda en el inventario seleccionando un ID de recurso y Agregar reglas de detección automatizada.

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Licencias autoadministradas.
3. Elija el nombre de la licencia autoadministrada para abrir la página de detalles de la licencia.
4. En la pestaña Reglas de detección automatizada, seleccione Agregar reglas de detección automatizada.

5. Especifique los productos que desea detectar y controlar.

> **Note**
>
> Las siguientes limitaciones se aplican a los productos de bases de datos de Amazon RDS (como Amazon RDS for Oracle y Amazon RDS for Db2):
>
> - Se admite un máximo de una regla que especifique un producto de base de datos de Amazon RDS.
> - Solo se permite una configuración de licencia para cada producto de base de datos de Amazon RDS.

6. (Opcional) Seleccione Detener el seguimiento de instancias cuando el software se desinstale para que la licencia pueda volver a utilizarse una vez que License Manager detecte que el software se ha desinstalado y ha transcurrido cualquier período de afinidad de licencia.
7. (Opcional) Para definir los recursos que se van a excluir de la detección automatizada, seleccione Agregar regla de exclusión.

> **Note**
>
> - Las reglas de exclusión no se aplican a los productos de bases de datos de RDS (como Amazon RDS for Oracle y Amazon RDS for Db2).
> - Las reglas de exclusión solo están disponibles si Detección de recursos entre cuentas se encuentra habilitada.

   a. Elija una Propiedad por la que filtrar. Actualmente, se admiten ID de cuenta y Etiqueta.
   b. Introduzca la información para identificar esa propiedad. Para un ID de cuenta, especifique el ID de AWS cuenta de 12 dígitos como valor. Para Etiqueta, introduzca un par clave-valor.
   c. Repita el paso 7 para añadir reglas adicionales.
8. Cuando haya terminado, pulse Agregar para aplicar la regla de detección automatizada.

Licencias concedidas en License Manager

Las licencias concedidas son licencias para productos que su organización compró en AWS Marketplace, AWS Data Exchange o directamente de un vendedor que integró su software con

derechos de administrador. Los administradores de licencias pueden utilizarlas AWS License Manager para regular el uso de estas licencias y distribuir los derechos de uso, conocidos como derechos, a cuentas específicas. AWS

Las licencias de datos distribuidas a AWS los productos de Data Exchange están disponibles en la AWS cuenta a través AWS de Data Exchange. Para poder distribuir las licencias desde AWS Marketplace, debe habilitar el uso compartido de suscripciones. Para obtener más información, consulte Uso compartido de suscripciones en una organización.

Una vez que un administrador de licencias distribuya el derecho de una AWS Marketplace licencia a una AWS cuenta y el destinatario acepte y active la licencia concedida, la suscripción estará disponible para la AWS cuenta a través de ella. AWS Marketplace La cuenta también tiene acceso al producto. Por ejemplo, si un administrador de licencias compra una imagen de máquina de Amazon (AMI) AWS Marketplace y distribuye un derecho a su AWS cuenta, puede lanzar EC2 instancias de Amazon desde la AMI mediante Amazon. AWS Marketplace EC2

Temas

- Visualización de las licencias concedidas
- Administre sus licencias concedidas en License Manager
- Distribuya los derechos de License Manager
- Aceptación y activación de la concesión en License Manager
- Estado de la licencia para las concesiones en License Manager
- CloudWatch métricas para las cuentas de compradores en License Manager

Visualización de las licencias concedidas

License Manager muestra pestañas para ver y administrar las licencias concedidas en función de los permisos con los que se ha autenticado. La página de licencias concedidas puede mostrar las siguientes pestañas:

Mis licencias

> Esta pestaña está disponible para cualquier usuario que tenga acceso a la visualización de las licencias concedidas en License Manager. La pestaña tiene la sección Mis licencias concedidas, que incluye información sobre cada licencia, como el ID de licencia y el Nombre del producto. En esta página puede ver información adicional sobre cada licencia.

Resumen de licencia (para los administradores de la organización)

Esta pestaña solo está disponible para los administradores de la organización. La pestaña tiene la sección Totales, en la que se muestra la cantidad total de productos y licencias concedidas en todas las cuentas de la organización. También muestra la sección Productos, que incluye una tabla en la que se detallan las propiedades de cada producto, como el nombre del producto y el número de licencias concedidas.

Licencias agregadas (para administradores de organizaciones)

Esta pestaña solo está disponible para los administradores de la organización. La pestaña tiene la sección Licencias concedidas en mi organización, que incluye información sobre cada licencia, como el ID de licencia y el Nombre del producto. En esta página puede ver información adicional sobre cada licencia.

Administre sus licencias concedidas en License Manager

Las licencias que se le hayan concedido aparecerán en la consola License Manager. Los destinatarios deben aceptar y activar las licencias concedidas antes de poder utilizar el producto. La forma de aceptar y activar una licencia depende de si la licencia es de AWS Marketplace origen, de si su cuenta es miembro de una organización y de si todas las funciones están habilitadas para su organización. AWS Organizations

Las licencias concedidas requieren la replicación de los metadatos de las licencias entre regiones. License Manager replica automáticamente cada licencia concedida y su información asociada en otras Regiones de AWS. Esto le permite tener una visión centralizada de todas las regiones en las que se le conceden licencias.

Licencias AWS Marketplace y AWS Data Exchange

- Las licencias de las suscripciones que compre se aceptan y activan automáticamente.
- Si la cuenta de administración de una organización con todas las características habilitadas compra una suscripción y distribuye las licencias a las cuentas miembro, las licencias se aceptan automáticamente en las cuentas miembro. Posteriormente, la cuenta de administración o las cuentas miembro pueden activar la licencia.
- Si la cuenta de administración de una organización con solo características de facturación consolidadas activadas compra una suscripción y distribuye las licencias a las cuentas miembro, cada cuenta miembro debe aceptar y activar las licencias.

Licencias de un vendedor

- Debe aceptar y activar las licencias de los productos que utilizan License Manager para distribuir licencias.
- Si la cuenta de administración de una organización con todas las características habilitadas compra un producto y distribuye las licencias a las cuentas miembro, las licencias se aceptan automáticamente en las cuentas miembro. Posteriormente, la cuenta de administración o las cuentas miembro pueden activar la licencia.
- Si la cuenta de administración de una organización con solo características de facturación consolidadas activadas compra un producto y distribuye las licencias a las cuentas miembro, cada cuenta miembro debe aceptar y activar las licencias.

Console (My licenses)

Puede ver y administrar las licencias concedidas para una sola Cuenta de AWS.

Procedimiento para administrar licencias en su cuenta

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación, seleccione Licencias concedidas.
3. Seleccione la pestaña Mis licencias si no es la selección actual.
4. (Opcional) Utilice los distintos filtros, como los siguientes, para acotar la lista de licencias que se muestran.
   - SKU del producto: identificador del producto de esta licencia, tal como lo definió el emisor de la licencia al crearla. Es posible que haya el mismo SKU de producto en varios ISVs.
   - Destinatario: el ARN del destinatario de la licencia.
   - Estado: estado de la licencia. Por ejemplo, Disponible.
5. Para ver información adicional sobre la licencia, elija el ID de la licencia para abrir la página Información general sobre la licencia.
6. Si el emisor de la licencia es una entidad distinta AWS Marketplace, el estado de la concesión inicial es Pendiente de aceptación. Realice una de las siguientes acciones:
   - Seleccione Aceptar y activar la licencia. El estado resultante de la concesión es Activo.
   - Seleccione Aceptar licencia. El estado resultante de la concesión es Deshabilitado. Cuando esté todo listo para usar la licencia, elija Activar licencia.

- Elija Rechazar licencia. El estado resultante de la concesión es Rechazado. Una vez rechazada una licencia, no podrá activarse.

Si no desea seguir utilizando una licencia que estaba activada, puede volver a la página Información general sobre la licencia y seleccionar Desactivar licencia. Si desea seguir utilizando una licencia que estaba desactivada, puede volver a la página Información general sobre la licencia y seleccionar Activar licencia.

Console (Aggregated licenses)

Puede ver las licencias concedidas que se han agregado de todas las cuentas de su organización.

> **Important**
>
> Para poder utilizar la visión global de la organización para las licencias concedidas, primero debe establecer el enlace AWS Organizations mediante la configuración de la AWS License Manager consola. Para obtener más información, consulte Configuración en License Manager.

Para gestionar las licencias concedidas en todas sus cuentas en AWS Organizations

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación, seleccione Licencias concedidas.
3. Seleccione la pestaña Licencias agregadas si no es la selección actual.
4. (Opcional) Utilice los distintos filtros, como los siguientes, para acotar la lista de licencias que se muestran.
   - SKU del producto: identificador del producto de esta licencia, tal como lo definió el emisor de la licencia al crearla. Es posible que haya el mismo SKU de producto en varios ISVs.
   - Beneficiario: la cuenta de su organización a la que se concede la licencia.
5. Para ver información adicional sobre la licencia, elija el ID de la licencia para abrir la página de información general sobre la licencia.
6. Si el emisor de la licencia es una entidad distinta AWS Marketplace, realice una de las siguientes acciones:
   - Seleccione Activar licencia. El estado resultante de la concesión es Activo.

- Seleccione Desactivar licencia. El estado resultante de la concesión es Desactivado.

Si no desea seguir utilizando una licencia que estaba activada, puede volver a la página Información general sobre la licencia y seleccionar Desactivar licencia. Si desea seguir utilizando una licencia que estaba desactivada, puede volver a la página Información general sobre la licencia y seleccionar Activar licencia.

AWS CLI

Puede usarlo AWS CLI para trabajar con las licencias concedidas.

Procedimiento para administrar licencias concedidas con AWS CLI:

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

Distribuya los derechos de License Manager

Si es administrador de licencias que opera en la cuenta de administración de su organización con todas las características habilitadas, puede distribuir los derechos a su organización a partir de las licencias concedidas mediante la creación de una concesión. Para obtener más información al respecto AWS Organizations, consulte AWS Organizations terminología y conceptos.

Puede especificar el destinatario de la concesión como uno de los siguientes:

- An Cuenta de AWS, que incluye solo la cuenta especificada.
- Un nodo raíz de organización, que incluirá todas las cuentas de su organización.
- Una unidad organizativa (OU) (que no está anidada), que incluye todas las cuentas de la OU especificada y que OUs están anidadas en la OU especificada.

> **Note**
>
> Puede crear hasta 2000 concesiones por licencia.

Puede utilizar la AWS License Manager consola o la AWS CLI para distribuir sus derechos. Puede especificar el ID o el ARN de la organización al crear una concesión en la consola, pero con AWS CLI debe utilizarse el formato ARN. Por ejemplo, ARNs se parecerá a lo siguiente:

ID de la organización en formato ARN

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

OU de la organización en formato ARN

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

Console

Procedimiento para crear una concesión (consola)

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación, seleccione Licencias concedidas.
3. Elija un ID de licencia para abrir la página Información general sobre la licencia.
4. En la sección Concesiones, seleccione Crear concesión.
5. En la página Detalles de la concesión haga lo siguiente:
   a. Introduzca un nombre para la subvención que le ayude a identificar el propósito o el destinatario de la subvención.
   b. Introduzca el Cuenta de AWS ID, AWS Organizations OU ID o ARN, o AWS Organizations ID o ARN del destinatario de la subvención.
   c. Seleccione Crear concesión.
6. En la página Información general sobre la licencia, verá una entrada para la concesión en el panel Concesiones. El estado inicial de la subvención es Aceptación pendiente. El estado cambia a Activo cuando el destinatario acepta la subvención o Rechazado cuando el destinatario rechaza la subvención.

AWS CLI

Puede utilizar el AWS CLI para distribuir un derecho. Debe especificar un ID de organización o una unidad organizativa en formato ARN cuando utilice la AWS License Manager API.

Procedimiento para crear y enumerar las concesiones con AWS CLI:

- create-grant
- list-distributed-grants

La página de detalles de la concesión muestra la lista de cuentas a las que ha concedido acceso al derecho. Tras distribuir una licencia a su organización, puede desactivar o activar las licencias de forma individual en cada cuenta.

Aceptación y activación de la concesión en License Manager

Cuando se crea una concesión para una licencia concedida, se distribuye al destinatario. Una licencia concedida debe aceptarse y activarse antes de que el destinatario de la concesión pueda utilizarla. El proceso de activación de la concesión puede incluir opciones adicionales para las licencias concedidas procedentes de AWS Marketplace.

De forma predeterminada, la página Información general sobre la concesión de una licencia concedida tiene el estado de `Pending Acceptance`. Puede elegir entre `Accept`, `Accept and Activate` o `Reject` la concesión. Las concesiones que se aceptan pero que aún no se han activado tienen el estado `Disabled`. Las concesiones aceptadas y activadas tienen el estado `Active`.

Una licencia concedida debe aceptarse y activarse antes de que el destinatario de la concesión pueda utilizarla. De forma predeterminada, la página de detalles de la concesión de una licencia concedida tiene el estado de Aceptación pendiente. Puede elegir entre Aceptar, Aceptar y activar o Rechazar la licencia. Las concesiones que se aceptan pero que aún no se han activado tienen el estado Disabled. Las concesiones aceptadas y activadas tienen el estado Active.

> **Tip**
>
> Puede aceptar automáticamente concesiones que procedan de la cuenta de administración de su organización. Para habilitar la aceptación automática de las subvenciones, vincula las cuentas de tu organización en la página de configuración de la AWS License Manager consola desde la cuenta de administración.

No puede activar dos licencias para el mismo producto AWS Marketplace al mismo tiempo. Si tiene dos suscripciones (por ejemplo, la oferta pública de un producto y una oferta privada, o bien una licencia suscrita para un producto y una licencia concedida para el mismo producto), puede realizar una de las siguientes acciones:

1. Deshabilite la concesión existente para el mismo producto y, a continuación, active la nueva concesión.
2. Active la nueva concesión y especifique que desea deshabilitar y reemplazar la concesión activa existente por la nueva. Puede utilizar la consola License Manager o la AWS CLI:
   a. Con la consola License Manager, active la nueva concesión seleccionando que Sí desea reemplazar las concesiones activas.
   b. Con la API de `CreateGrantVersion`, active la nueva concesión especificando `ALL_GRANTS_PERMITTED_BY_ISSUER` para el valor `ActivationOverrideBehavior` con el `Status` `Active`.

Console

Puede utilizar la consola License Manager para activar una concesión. Al activar una subvención procedente de AWS Marketplace, es posible que se te presente la opción de sustituir las subvenciones activas:

- Como administrador de licencias, debe especificar si desea reemplazar las concesiones activas al activar una concesión.
- Como concedente, si lo desea, puede especificar si desea reemplazar las concesiones activas al activar una concesión para otra cuenta de su organización.
- Si el concedente que creó la concesión distribuida no especificó si iba a reemplazar las concesiones activas, como beneficiario de la concesión usted debe decidir qué hacer al activar la concesión.

Procedimiento para activar una concesión (consola)

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación, seleccione Licencias concedidas.
3. Elija un ID de licencia para abrir la página Información general sobre la licencia.

4. Elija un nombre de concesión para abrir la página Información general sobre la concesión.
5. Si aparece, seleccione una opción de activación para decidir si desea reemplazar las concesiones activas:
   a. No: esta opción activará la concesión sin reemplazar ninguna concesión activa existente para el destinatario (beneficiario).
   b. Sí: esta opción deshabilitará las concesiones para un mismo producto y activará una nueva concesión para el destinatario definido (beneficiario):
      i. Según lo especificado Cuenta de AWS.
      ii. Cuentas miembro de la OU de la organización especificada.
      iii. Todas las cuentas miembro de la organización.
6. (Opcional) Indique un motivo para activar la subvención.
7. Introduzca **`activate`** en el cuadro de entrada y seleccione Activar.

AWS CLI

Puede usarlo AWS CLI para trabajar con las licencias concedidas.

Para trabajar con las subvenciones distribuidas mediante AWS CLI:

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

Estado de la licencia para las concesiones en License Manager

Las licencias tienen dos estados: el Estado de la licencia, que muestra la disponibilidad general y la capacidad de uso compartido de la licencia, y el Estado de la concesión, que muestra la capacidad de utilizar la licencia.

En la siguiente tabla se muestran los distintos estados de una licencia concedida:

Estado	Descripción
DISPONIBLE	La licencia está disponible para su uso y uso compartido.
PENDING_AVAILABLE	La licencia no está disponible para su uso porque aún se está procesando.
DEACTIVATED	La licencia no está disponible para su uso porque el emisor de la licencia la ha desactiva do.
SUSPENDED	La licencia no está disponible para su uso porque se ha suspendido.
EXPIRED	La licencia no está disponible para su uso porque ha vencido.
PENDING_DELETE	La licencia no está disponible para su uso porque su eliminación se está procesando.
DELETED	La licencia no está disponible para su uso porque se ha cancelado el acuerdo de licencia.

En la siguiente tabla se muestran los distintos estados de una concesión:

Estado	Descripción
PENDING_WORKFLOW	La concesión está en proceso de distribuirse.
PENDING_ACCEPT	La concesión se ha creado y el destinatario de la misma aún no la ha aceptado.
REJECTED	El beneficiario ha rechazado la concesión.
ACTIVE	Se ha aceptado y activado la concesión para su uso por parte del beneficiario. El recurso con licencia puede utilizarse.

Estado	Descripción
FAILED_WORKFLOW	No se pudo distribuir la concesión.
DELETED	El concedente ha eliminado la concesión.
PENDING_DELETE	La concesión que se distribuyó está en proceso de eliminarse.
DISABLED	El destinatario ha aceptado la concesión, pero no se ha activado para su uso.
WORKFLOW_COMPLETE	Se ha distribuido o recuperado la concesión a una organización. Los detalles de la concesión muestran el estado de las subconcesiones a cada cuenta de la organización.

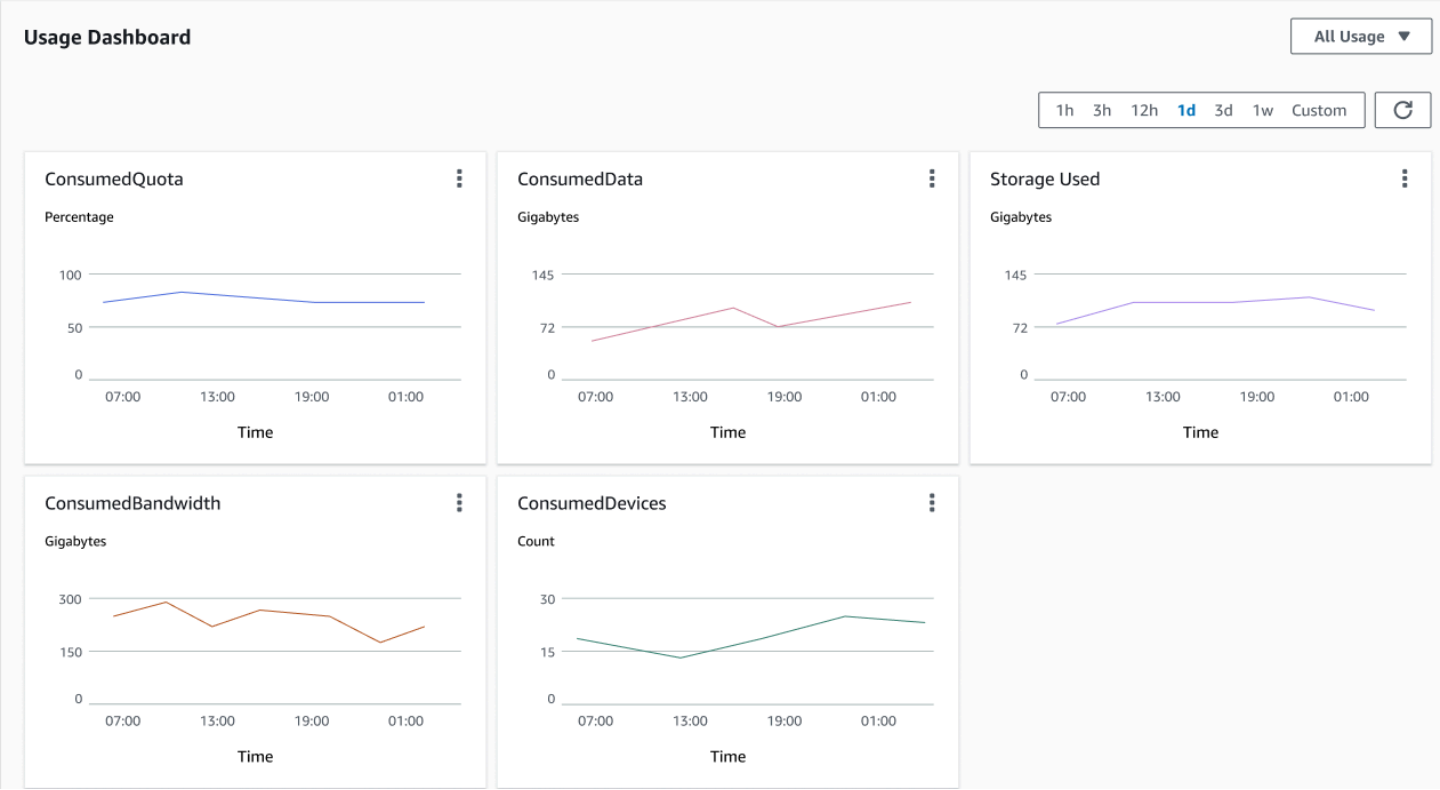
CloudWatch métricas para las cuentas de compradores en License Manager

Cuando se configura la concesión de una licencia emitida por un vendedor con la opción Permitir el envío de registros de uso seleccionada, License Manager emite una CloudWatch métrica a la cuenta del vendedor, la cuenta del comprador raíz y la cuenta en la que se registra el uso. Las cuentas de comprador son las Cuentas de AWS que han adquirido o se les ha concedido una licencia expedida por el vendedor. Para obtener más información, consulte Concesión de licencias a clientes.

Panel de uso

Cuando una aplicación de un vendedor o de un proveedor de software independiente (ISV) registra el uso en una licencia de una cuenta de comprador, la cuenta en la que se registra el uso y la cuenta del comprador raíz ven un CloudWatch widget con registros de uso en la página del panel de control de uso de la consola de License Manager. Los compradores también pueden ver las métricas de las cuentas en las que han distribuido licencias en AWS Organizations. Los gráficos de la página Panel de uso están disponibles para todas las licencias para las que se hayan enviado registros de uso.

La siguiente imagen muestra un ejemplo del panel de uso:



Licencias emitidas por el vendedor en License Manager

Los proveedores de software independientes (ISVs) pueden utilizarlas AWS License Manager para gestionar y distribuir las licencias de software a los usuarios finales. Como emisor, puede realizar un seguimiento del uso de las licencias que emite de forma centralizada mediante el panel de control de License Manager.

License Manager utiliza estándares del sector abiertos y seguros para representar las licencias y permite a los clientes verificar criptográficamente su autenticidad. License Manager asocia cada licencia a una clave asimétrica. Como ISV, usted es el propietario de las AWS KMS claves asimétricas y las almacena en su cuenta.

Las licencias emitidas por el vendedor requieren la replicación de los metadatos de las licencias entre regiones. License Manager replica automáticamente cada licencia emitida por el vendedor y su información asociada en otras regiones.

License Manager admite varios modelos de licencias diferentes, incluidos los siguientes:

- Licencias perpetuas: licencias de por vida sin fecha de vencimiento que autorizan a los usuarios a utilizar el software de forma indefinida.

- Licencias flotantes: licencias que se pueden compartir con varias instancias de la aplicación. Las licencias se pueden pagar por adelantado y se les puede añadir un conjunto fijo de derechos.
- Licencias de suscripción: licencias con fecha de vencimiento que se pueden renovar automáticamente a menos que se desactiven específicamente.
- Licencias basadas en el uso: licencias con condiciones específicas en función del uso, como el número de solicitudes de API, las transacciones o las prestaciones de almacenamiento.

Puede crear licencias en License Manager y distribuirlas a sus clientes con una identidad de AWS IAM o mediante fichas portadoras generadas por License Manager. Los clientes de ISV que dispongan de una AWS cuenta pueden redistribuir los derechos de licencia entre las identidades de sus respectivas organizaciones. AWS Los clientes con concesiones de derechos distribuidos pueden retirar y registrar las concesiones de derechos necesarias de esa licencia mediante la integración del software con License Manager.

Derechos de licencia emitidos por el vendedor en License Manager

License Manager captura las capacidades de licencia emitidas por el vendedor como derechos en la licencia. Las concesiones de derechos se pueden caracterizar por una cantidad limitada o ilimitada. Una concesión de derechos limitada es, por ejemplo, “40 GB de transferencia de datos”. Una concesión de derechos ilimitada es, por ejemplo, “Nivel platino”.

Una licencia recoge todas las concesiones de derechos concedidas, sus fechas de activación y vencimiento, y los datos del emisor. Una licencia es una entidad versionada y cada versión es inmutable. Las versiones de una licencia se actualizan cada vez que se cambia la licencia.

Para retirar o registrar los derechos limitados, las aplicaciones del ISV deben especificar la cantidad de cada capacidad limitada. En el caso de los derechos ilimitados, las aplicaciones del ISV solo tienen que especificar de nuevo el derecho correspondiente para volver a retirarlo o registrarlo. Por último, las capacidades limitadas también indican si los usuarios finales pueden superar el uso de las concesiones de derechos iniciales. License Manager hace un seguimiento del uso y un informe al respecto, y sobre cualquier exceso, para el ISV.

Uso de licencias emitidas por el vendedor en License Manager

License Manager permite realizar un seguimiento centralizado de las licencias en varias regiones, manteniendo un recuento de todos los derechos retirados. License Manager también hace un seguimiento de la identidad del usuario y el identificador de recursos subyacente, si está disponible,

asociado a cada retirada, además de la fecha en que se retiró. Puede realizar un seguimiento de estos datos de series temporales a través de CloudWatch Eventos.

Las licencias pueden tener uno de los siguientes estados:

- Creada: la licencia se ha creado.
- Actualizada: la licencia se ha actualizado.
- Desactivada: la licencia se ha desactivado.
- Eliminada: la licencia se ha eliminado.

Permisos necesarios para rastrear el uso de las licencias emitidas por el vendedor en License Manager

Para empezar a utilizar esta característica, necesita permiso para llamar a las siguientes acciones de la API de License Manager.

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

```
    ]
}
```

Si va a integrarse con License Manager para que los clientes sin una AWS cuenta puedan consumir licencias vendidas fuera de ella AWS Marketplace, debe crear una función de IAM que permita a su aplicación de software llamar a la API de License Manager.

Si las utiliza AWS Management Console para distribuir credenciales temporales a los clientes que no las Cuenta de AWS tengan, License Manager las creará automáticamente `AWSLicenseManagerConsumptionRole` en su nombre. Para obtener más información, consulte Obtenga credenciales temporales para los clientes de ISV sin una cuenta AWS. Para crear este rol a partir de AWS CLI, utilice el comando create-role de AWS IAM, como se muestra en el siguiente ejemplo.

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

El `trust-policy-document.json` archivo proporcionado debería tener el aspecto que se muestra en el ejemplo siguiente, con tu propio Cuenta de AWS ID sustituido por la cuenta del emisor del token.

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

```
}
```

A continuación, utilice el attach-role-policycomando para añadir la política AWSLicenseManagerConsumptionPolicy AWS gestionada al AWSLicenseManagerConsumptionRolerol.

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

Cree licencias emitidas por el vendedor en License Manager

Utilice el procedimiento siguiente para crear un bloque de licencias para concedérselo a los clientes que utilizan AWS Management Console. Como alternativa, puede crear la licencia mediante la acción de la CreateLicenseAPI.

Procedimiento para crear una licencia mediante la consola

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Seleccione Licencias emitidas por el vendedor en el menú de la izquierda.
3. Seleccione Crear licencia.
4. Para el campo Metadatos de la licencia, facilite la siguiente información:
   - Nombre de la licencia: el nombre, de hasta 150 caracteres, que se mostrará a los compradores.
   - Descripción de la licencia: descripción opcional, de hasta 400 caracteres, que diferencia esta licencia de otras licencias.
   - SKU del producto: SKU del producto.
   - Destinatario: nombre del destinatario (empresa o particular).
   - Región de origen: la AWS región de la licencia. Si bien las licencias se pueden consumir en todo el mundo, solo puede cambiarlas en la región principal. La región principal de una licencia no se puede cambiar después de crear la licencia.
   - Fecha de inicio de la licencia: fecha de activación.
   - Fecha de finalización de la licencia: fecha de finalización de la licencia, si corresponde.
5. Para Configuración de consumo, facilite la siguiente información:

- Frecuencia de renovación: si se renueva semanalmente, mensualmente o no se renueva.
- Configuración de consumo: seleccione Opciones de configuración para consumo provisional si la licencia se va a utilizar para una conectividad continua o Préstamo si la licencia se va a utilizar sin conexión. Introduzca el Tiempo máximo de vida (minutos) para establecer la duración de la disponibilidad de la licencia.

6. Para Emisor, facilite la siguiente información:

   - Introduzca una AWS KMS clave: License Manager utiliza esta clave para firmar y verificar al emisor. Para obtener más información, consulte Firma criptográfica de licencias en License Manager.
   - Nombre del emisor: el nombre comercial del vendedor.
   - Vendedor registrado: nombre comercial opcional.
   - URL del acuerdo: la URL del acuerdo de licencia.

7. En Derechos, facilite la siguiente información sobre las capacidades que la licencia otorga a los destinatarios:

   - Nombre: el nombre del destinatario.
   - Tipo de unidad: seleccione el tipo de unidad y, a continuación, indique el número máximo.
   - Seleccione Permitir la comprobación si los destinatarios deben registrar las licencias antes de renovarlas.
   - Marque Excesos permitidos si los destinatarios pueden superar el límite máximo de uso del recurso. Esta opción puede generar cargos adicionales para el destinatario.

8. Seleccione Crear licencia.

Conceda licencias emitidas por el vendedor de License Manager a clientes de ISV

Después de añadir la licencia nueva, puede concederla a un cliente que tenga una cuenta de AWS mediante AWS Management Console. El destinatario debe aceptar la concesión antes de utilizar la licencia. Para obtener más información, consulte Licencias concedidas en License Manager.

Como alternativa, si el cliente no tiene una AWS cuenta, puede usar la API de License Manager para permitir que los clientes consuman licencias.

Procedimiento para conceder una licencia a un cliente mediante la consola

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Seleccione Licencias emitidas por el vendedor en el menú de la izquierda.
3. Elija el ID de la licencia para abrir la página de detalles.
4. En Concesiones, seleccione Crear concesión.
5. En Detalles de la concesión, facilite la siguiente información:
   - Nombre de la concesión: el nombre de la concesión. Se usa para habilitar las capacidades de búsqueda.
   - AWS ID de cuenta: el número de AWS cuenta del destinatario de la licencia.
   - Derechos de licencia
     - Seleccione Consumo si el destinatario puede consumir los derechos concedidos.
     - Seleccione Distribución si el destinatario puede distribuir los derechos concedidos a otras AWS cuentas.
     - Seleccione Permitir la generación de tokens in situ para autenticar las licencias compartidas sin utilizar AWS identidades ni credenciales.
     - Seleccione Permitir el envío de registros de uso para permitir que los destinatarios de las licencias emitan registros de uso para los tipos de uso.
   - Región de origen: la de Región de AWS la licencia.
6. Seleccione Crear concesión.

Obtenga credenciales temporales para los clientes de ISV sin una cuenta AWS

En el caso de los clientes que no AWS tienen una cuenta, puede utilizar los derechos de la misma manera que lo hace con los clientes que tienen una AWS cuenta. Utilice el siguiente procedimiento para obtener AWS credenciales temporales para sus clientes sin una AWS cuenta. Las llamadas a la API deben realizarse en la región principal.

Procedimiento para obtener credenciales temporales para las llamadas a la API de License Manager

1. Ejecute la acción de la CreateTokenAPI para que un token de actualización se codifique como un token JWT.

2. Ejecuta la acción de la GetAccessTokenAPI y especifica el token de actualización que recibiste `CreateToken` en el paso anterior para recibir un token de acceso temporal.
3. Para obtener las AWS credenciales temporales, ejecuta la acción de la AssumeRoleWithWebIdentityAPI y especifica el token de acceso que recibiste `GetAccessToken` en el paso anterior y el AWSLicenseManagerConsumptionRolerol que creaste.

Para crear un token desde la AWS License Manager consola

1. Desde la consola de License Manager, vaya a la página de detalles de la licencia correspondiente al derecho de licencia específico que desee utilizar sin una AWS cuenta.
2. Seleccione Crear token para generar un token de acceso temporal.

> **Note**
>
> La primera vez que genere un token de acceso temporal, se le pedirá que cree un rol de servicio para que License Manager pueda acceder a los servicios en su nombre. Se crea el siguiente rol de servicio: `AWSLicenseManagerConsumptionRole`.

3. Descargue el archivo `token.csv` o copie la cadena del token cuando se genere.

> **Important**
>
> Esta será la única vez que pueda ver o descargar este token. Le recomendamos que descargue el token y almacene el archivo en una ubicación segura. Puede crear tokens nuevos en cualquier momento, hasta el límite de servicio definido.

Consulte las licencias emitidas por el vendedor en License Manager

License Manager permite que varios usuarios consuman simultáneamente los derechos, con capacidades limitadas, de una sola licencia. Llame a la acción CheckoutLicense de la API. A continuación se describen los parámetros.

- Huella digital clave: emisor de licencias de confianza.

  aws:123456789012:issuer:issuer-fingerprint, por ejemplo.

- SKU del producto: identificador del producto de esta licencia, tal como lo definió el emisor de la licencia al crearla. Es posible que haya el mismo SKU de producto en varios. ISVs Por lo tanto, las huellas digitales clave de confianza desempeñan un papel importante.

  1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0daEXAMPLE, por ejemplo.
- Derechos: capacidades que pueden retirarse. Si especifica una capacidad ilimitada, la cantidad es cero. Ejemplo:

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

- Beneficiario: el software como servicio (SaaS) ISVs puede solicitar licencias en nombre de un cliente al incluir el identificador del cliente. License Manager limita la llamada al repositorio de licencias creado en la cuenta del ISV de SaaS.

  usuario@dominio.com, por ejemplo.
- ID de nodo: identificador que se utiliza para bloquear el nodo de la licencia a una sola instancia de la aplicación.

  10.0.21.57, por ejemplo.

Eliminar las licencias emitidas por el vendedor en License Manager

Después de eliminar una licencia, puede recrearla. La licencia y sus datos se conservan y están disponibles para el emisor y los concesionarios de la licencia en modo de solo lectura durante seis meses.

Utilice el procedimiento siguiente para eliminar una licencia que haya creado mediante AWS Management Console. Como alternativa, puede eliminar la licencia mediante la acción de la DeleteLicenseAPI.

Procedimiento para eliminar una licencia mediante la consola

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Seleccione Licencias emitidas por el vendedor en el menú de la izquierda.
3. Seleccione el botón de opción situado junto a la licencia para seleccionarla y eliminarla.
4. Elija Eliminar. Cuando se le pida confirmación, ingrese **`delete`** y elija Eliminar.

Utilice las suscripciones basadas en usuarios de License Manager para los productos de software compatibles

Con las suscripciones basadas en usuarios AWS License Manager, puede adquirir suscripciones de software con licencia totalmente compatibles. Las licencias las proporciona Amazon y conllevan una cuota de suscripción por usuario. Amazon EC2 proporciona Amazon Machine Images (AMIs) preconfiguradas con el software compatible, además de licencias de Windows Server con licencia incluida. Estas licencias se pueden utilizar sin permanencias a largo plazo.

Para utilizar las suscripciones basadas en usuarios, asocie los usuarios de AWS Directory Service for Microsoft Active Directory(AWS Managed Microsoft AD) o de su dominio autogestionado (local) a las instancias que proporcionan el software. EC2 Para que el software con licencia esté disponible, debe crear suscripciones basadas en usuarios y asociarlas a instancias lanzadas desde instancias preconfiguradas. AMIs AWS Systems Managerconfigurará y reforzará las instancias con licencia incluida que lance. Los usuarios deben conectarse al software de escritorio remoto para acceder a las instancias que proporcionan el software.

Cada usuario y vCPU asociados a las instancias con licencia incluida incurren en cargos. Los modelos de precios de Amazon EC2 Reserved Instances y Savings Plan pueden ayudarle a optimizar sus EC2 costes de Amazon. Para obtener más información, consulte Instancias reservadas en la Guía del usuario de Amazon Elastic Compute Cloud. Las suscripciones basadas en usuarios se facturan desde la primera mitad del mes hasta final de mes.

Temas

- Consideraciones sobre el uso de suscripciones basadas en usuarios en License Manager
- Cargos de suscripción en License Manager
- Requisitos previos para crear suscripciones basadas en usuarios en License Manager
- Productos de software compatibles para suscripciones basadas en usuarios en License Manager

- Active Directory
- Software adicional
- Comience con las suscripciones basadas en usuarios en License Manager
- Configure el GPO de Active Directory para sesiones de usuarios remotos más activas
- Lance una instancia a partir de una licencia incluida (AMI)
- Conéctese a una instancia de suscripción basada en usuarios con RDP
- Modifique la configuración del firewall de su suscripción a Microsoft Office
- Administre los usuarios de suscripción para las suscripciones basadas en usuarios de License Manager
- Anular el registro de un Active Directory desde la configuración de License Manager
- Solucionar problemas de suscripciones basadas en usuarios en License Manager

Consideraciones sobre el uso de suscripciones basadas en usuarios en License Manager

Cuando se utilizan suscripciones basadas en usuarios con License Manager, se tienen en cuenta las siguientes consideraciones:

- La AWS Marketplace suscripción a los Servicios de Escritorio Remoto de Microsoft (`Win Remote Desktop Services SAL`) con licencia incluida tiene una cuota mensual por usuario, sin prorrateo.
- De forma predeterminada, las instancias que ofrecen suscripciones basadas en usuarios admiten hasta dos sesiones de usuario activas a la vez. Para habilitar más de dos sesiones de usuario activas, puede configurar un objeto de política de grupo (GPO) de Active Directory y establecer el modo de licencia RDS de Microsoft en. `Per User` Para obtener más información, consulte los requisitos previos de. Configure el GPO de Active Directory para sesiones de usuarios remotos más activas
- Al crear usuarios locales con privilegios de administrador en instancias que ofrecen suscripciones basadas en usuarios, es posible que el estado de la instancia cambie a «en mal estado». License Manager puede terminar instancias que no estén en buen estado debido a la falta de conformidad. Para obtener más información, consulte Solución de problemas de conformidad de las instancias.
- Al configurar Active Directory con productos de Microsoft Office, la VPC debe tener puntos de enlace de VPC aprovisionados en al menos una subred. Si quiere eliminar todos los recursos de punto final de la VPC creados por License Manager, debe eliminar cualquier Active Directory que

esté configurado en la configuración del License Manager. Para obtener más información, consulte Anular el registro de un Active Directory desde la configuración de License Manager.

- La clave de la etiqueta `AWSLicenseManager` con el valor `UserSubscriptions` asignado por License Manager a sus instancias no debe modificarse ni eliminarse.
- Para que el servicio funcione como se espera, las dos interfaces de red creadas para License Manager no deben modificarse ni eliminarse.
- Los objetos que License Manager crea en la unidad organizativa AWS reservada (OU) del AWS Managed Microsoft AD directorio no se deben modificar ni eliminar.
- Las instancias implementadas para las suscripciones basadas en usuarios deben ser nodos administrados con AWS Systems Manager y estar unidas al mismo dominio. Para obtener información sobre cómo mantener las instancias administradas por Systems Manager, consulte la sección Solucionar problemas de suscripciones basadas en usuarios en License Manager de esta guía.
- Para dejar de incurrir en cargos de suscripción a Microsoft Office o Visual Studio para un usuario, debe desasociar al usuario de todas las instancias a las que esté asociado. Para obtener más información, consulte Desasociar usuarios de una instancia que proporciona suscripciones basadas en usuarios de License Manager.

Cargos de suscripción en License Manager

La suscripción y la facturación en License Manager varían según el producto de suscripción que se utilice.

Suscripciones a Microsoft Office y Visual Studio

En el caso de las suscripciones a Microsoft Office y Visual Studio, la facturación se detiene en cuanto se desvincula al usuario de todas las instancias que ofrecen el producto de suscripción y se cancela su suscripción al producto.

Suscripciones a Microsoft Remote Desktop Services (RDS)

Microsoft RDS se factura por usuario y mes en función de una combinación de la suscripción de usuario y el token de licencia de acceso de cliente (CAL) que se emite desde el servidor de licencias cuando el usuario se conecta a una instancia que proporciona el producto de suscripción.

Facturación de Microsoft RDS en License Manager

La facturación de Microsoft RDS comienza cuando el usuario de Active Directory se suscribe a través de License Manager y finaliza después de que caduque el token de licencia de acceso de cliente (CAL), 60 días después de la fecha de emisión, sin prorrateo durante meses parciales. La facturación continúa hasta que caduque el token, incluso si cancelas la suscripción del usuario.

Si un usuario que se ha dado de baja sigue iniciando sesión después de que caduque el token de licencia, volverá a suscribirse automáticamente y la facturación se prolongará hasta que vuelva a darse de baja y su token caduque.

Del mismo modo, si un usuario que nunca se ha suscrito, pero inicia sesión en una instancia asociada al servidor de licencias, License Manager lo suscribe automáticamente y comienza la facturación de RDS. La facturación continúa hasta que se cancele la suscripción y caduque su token.

Para dejar de facturar a un usuario al final del mes en curso, debe eliminar ese usuario del Active Directory que está configurado para el servidor de licencias antes de cancelar la suscripción.

> **Warning**
>
> Si quita a un usuario de Active Directory que todavía tiene una suscripción activa a Microsoft Office o Visual Studio, ese usuario ya no podrá acceder a las instancias a las que esté asociado.

Los siguientes escenarios de ejemplo muestran cómo funciona la facturación de RDS.

Escenario 1: suscripción y facturación estándar

El siguiente escenario muestra un conjunto estándar de acciones que afectan a la facturación de un usuario de Active Directory (AD) que se suscribió el 15 de diciembre de 2024, pero que nunca accedió a una instancia de suscripción.

Acción: si el usuario nunca cancela su suscripción, la facturación continúa indefinidamente.

El usuario de AD se ha suscrito	Comienza la facturación	CAL emitida	La CAL vence	El usuario se dio de baja	Usuario eliminado de AD	Finaliza la facturación
15/12/2024	15/12/2024	--	N/A	--	--	--

Acción: El 15 de enero de 2025 se cancelará la suscripción del usuario.

El usuario de AD se ha suscrito	Comienza la facturación	CAL emitida	La CAL vence	El usuario se dio de baja	Usuario eliminado de AD	Finaliza la facturación
15/12/2024	15/12/2024	--	N/A	1/15/2025	No	1/31/2025

Escenario 2: Cómo afecta el token de licencia a la suscripción y la facturación de los usuarios

En el siguiente escenario, se muestra cómo la caducidad del token de licencia afecta a la suscripción de un usuario de Active Directory (AD) suscrito el 15 de septiembre de 2024 e inicia sesión en una instancia de producto de suscripción unida a un dominio el mismo día.

Acción: suscripción inicial e inicio de sesión para un usuario de AD.

Usuario de AD suscrito	Comienza la facturación	CAL emitida	La CAL vence	El usuario se dio de baja	Usuario eliminado de AD	Finaliza la facturación
15 de septiembre de 2024	15 de septiembre de 2024	15 de septiembre de 2024	15/11/2024	--	--	--

Acción: El mismo usuario de AD cancelará su suscripción el 19 de octubre de 2024. Sin embargo, dado que el usuario no se eliminó del directorio, la facturación continúa hasta el final del mes durante el cual caduca el token de licencia.

El usuario de AD se ha suscrito	Comienza la facturación	CAL emitida	La CAL vence	El usuario se dio de baja	Usuario eliminado de AD	Finaliza la facturación
15 de septiembre de 2024	15 de septiembre de 2024	15 de septiembre de 2024	15/11/2024	10/19/2024	--	11/30/2024

Acción alternativa: el administrador de AD elimina al usuario del directorio el 20 de octubre de 2024 y, a continuación, cancela la suscripción del usuario al día siguiente. En este caso, la facturación se detiene al final del mes durante el cual se elimina al usuario del directorio.

El usuario de AD está suscrito	Comienza la facturación	CAL emitida	La CAL vence	El usuario se dio de baja	Usuario eliminado de AD	Finaliza la facturación
15 de septiembre de 2024	15 de septiembre de 2024	15 de septiembre de 2024	15/11/2024	21/10/2024	10/20/2024	10/31/2024

Escenario 3: el usuario cancelado se vuelve a suscribir

En el siguiente escenario, se muestra cómo un usuario de Active Directory (AD) cancelado y cuyo token de licencia ha caducado se vuelve a suscribir automáticamente cuando accede a una instancia de producto de suscripción unida a un dominio.

Acción: suscripción inicial e inicio de sesión para un usuario de AD.

Usuario de AD suscrito	Comienza la facturación	CAL emitida	La CAL vence	El usuario se dio de baja	Usuario eliminado de AD	Finaliza la facturación
15 de septiembre de 2024	15 de septiembre de 2024	15 de septiembre de 2024	15/11/2024	--	--	--

Acción: El mismo usuario de AD cancelará su suscripción el 19 de octubre de 2024. Sin embargo, dado que el usuario no se eliminó del directorio, la facturación continúa hasta el final del mes durante el cual caduca el token de licencia.

El usuario de AD se ha suscrito	Comienza la facturación	CAL emitida	La CAL vence	El usuario se dio de baja	Usuario eliminado de AD	Finaliza la facturación
15 de septiembre de 2024	15 de septiembre de 2024	15 de septiembre de 2024	15/11/2024	10/19/2024	--	11/30/2024

Acción: el mismo usuario de AD accede a una instancia de producto de suscripción unida a un dominio después de que caduque el token de licencia anterior, pero antes de que finalice la facturación. La facturación continúa hasta que el usuario vuelva a cancelar la suscripción y su nuevo token caduque.

El usuario de AD está suscrito	Comienza la facturación	CAL emitida	La CAL vence	El usuario se dio de baja	Usuario eliminado de AD	Finaliza la facturación
11/20/2024 (re-subscribed)	billing continues	11/20/2024	1/20/2025	--	--	--

Escenario 4: Suscripción automática al acceder a la instancia

En el siguiente escenario, se muestra cómo un usuario de Active Directory (AD) que nunca estuvo suscrito a RDS SAL se suscribe automáticamente al iniciar sesión en una instancia de producto de suscripción unida a un dominio.

Acción: un usuario de AD que nunca se suscribió a RDS SAL inicia sesión en una instancia de producto de suscripción unida a un dominio el 15 de septiembre de 2024 y se suscribe automáticamente. La facturación comienza y continúa hasta que el usuario cancele la suscripción y caduque su nuevo token.

El usuario de AD está suscrito	Comienza la facturación	CAL emitida	La CAL vence	El usuario se dio de baja	Usuario eliminado de AD	Finaliza la facturación
15 de septiembre de 2024 (suscripción automática)	15 de septiembre de 2024	15 de septiembre de 2024	15/11/2024	--	--	--

Para obtener más información sobre cómo CALs funciona Microsoft RDS por usuario, consulte la CALs sección Por usuario del artículo sobre la licencia de implementación de escritorio remoto en el sitio web de Microsoft Learn.

Requisitos previos para crear suscripciones basadas en usuarios en License Manager

Los siguientes requisitos previos deben implementarse en su entorno antes de poder crear suscripciones basadas en usuarios.

Contenido

- Roles y permisos de IAM
  - AWS KMS Política de claves para las credenciales del servidor de licencias
- Active Directory
- Grupos de seguridad
- Configuración de red
- Instancias que ofrecen productos de suscripción basados en el usuario
- Servicios de escritorio remoto de Microsoft
  - Credenciales administrativas secretas

Roles y permisos de IAM

Debe permitir que License Manager cree un rol vinculado a servicios para incorporar las suscripciones basadas en usuarios a su Cuenta de AWS . En la consola de License Manager, aparece un mensaje en Suscripciones basadas en usuarios si el rol aún no se ha creado. Tras responder a la solicitud y aceptar permitir que License Manager cree el rol, elija Create para continuar. Para obtener más información, consulte Uso de funciones vinculadas a servicios para License Manager.

Para crear suscripciones basadas en usuarios, su usuario o rol debe tener los siguientes permisos:

- Amazon EC2: trabaja con interfaces y subredes de red.
  - `ec2:CreateNetworkInterface`
  - `ec2:DeleteNetworkInterface`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:CreateNetworkInterfacePermission`
  - `ec2:DescribeSubnets`
- AWS Directory Service— Administrar Active Directories.
  - `ds:DescribeDirectories`
  - `ds:AuthorizeApplication`
  - `ds:UnauthorizeApplication`
  - `ds:GetAuthorizedApplicationDetails`
  - `ds:DescribeDomainControllers`
- Route 53: configurar el enrutamiento.
  - `route53:DeleteHealthCheck`
  - `route53:ChangeResourceRecordSets`
  - `route53:GetHostedZone`
  - `route53:ListHostedZonesByName`
  - `route53:ListHostedZones`
  - `route53:ListHostedZonesByVPC`
  - `route53:CreateHostedZone`
  - `route53:DeleteHostedZone`
  - `route53:ListResourceRecordSets`

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

Para crear suscripciones basadas en usuarios para los productos de Microsoft Office, su usuario o rol también debe tener los siguientes permisos adicionales:

- `ec2:CreateVpcEndpoint`
- `ec2:DeleteVpcEndpoints`
- `ec2:DescribeVpcEndpoints`
- `ec2:ModifyVpcEndpoint`
- `ec2:DescribeSecurityGroups`

AWS KMS Política de claves para las credenciales del servidor de licencias

Para usar su propia clave KMS para cifrar y descifrar el secreto de las credenciales administrativas del servidor de licencias RDS de Microsoft, debe adjuntar una política a la función que utiliza para acceder a las operaciones del License Manager. El siguiente ejemplo muestra una política que concede permiso a Secrets Manager para acceder a la clave de KMS para cifrar y descifrar el secreto de credenciales del servidor de licencias RDS de Microsoft.

```
{
"Version": "2012-10-17",
"Id": "key-policy",
"Statement": [
    {
        "Sid": "Enable IAM User Permissions",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:role/RoleName"
        },
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "secretsmanager.*.amazonaws.com"
            }
```

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

Active Directory

Para usar las suscripciones basadas en usuarios de License Manager, debe crear un Active Directory (AD) que contenga información de usuario para los usuarios del producto de suscripción. Según la configuración, puede utilizar un AWS Managed Microsoft AD AD autogestionado o uno autogestionado.

Si usa directorios activos AWS administrados y autoadministrados, debe establecer una confianza bidireccional en el bosque entre los directorios. Para obtener más información, consulte el tutorial: Crear una relación de confianza entre su dominio de Active Directory AWS Managed Microsoft AD y su dominio autoadministrado en la AWS Directory Service Guía de administración.

> **Note**
>
> Las subredes que están configuradas para su directorio deben ser todas de la misma VPC que la suya. Cuenta de AWS No se admiten las subredes compartidas.

AWS Los Active Directories administrados tienen las siguientes restricciones.

- No se admiten los directorios que se comparten con usted.
- No se admite la autenticación multifactorial

Requisito previo para los filtros basados en etiquetas

Si va a utilizar filtros basados en etiquetas para su Active Directory, primero debe incorporarse al Explorador de recursos de AWS servicio de la siguiente manera:

1. Abra la consola del Explorador de recursos en https://resource-explorer.console.aws.amazon.com/resource-explorer.
2. Elija Activar Resource Explorer.
3. En la página de configuración del explorador de recursos, elija una opción de configuración, de la siguiente manera.

   Configuración Rápida

   Seleccione esta opción para la configuración básica.

   Configuración avanzada

   Seleccione esta opción para una configuración personalizada. Asegúrese de crear un índice para, al menos, la región en la que reside su Active Directory.
4. Seleccione una región para la región del índice del agregador.
5. Seleccione Activar el explorador de recursos para guardar la configuración.
6. En el panel de navegación, selecciona Vistas y, a continuación, selecciona Crear vista.

   > **Note**
   >
   > Para mostrar el panel de navegación si está oculto, selecciona el icono del menú (tres barras horizontales).

7. a. En la página Crear vista, introduce **`license-manager-user-subscriptions-view`** el nombre.
   b. Compruebe que el filtro de recursos esté configurado para incluir todos los recursos.
   c. En la sección Atributos de recursos adicionales, compruebe que la casilla Etiquetas esté seleccionada.
8. Seleccione Crear vista para terminar.

Para obtener más información sobre la creación de un AWS Managed Microsoft AD directorio, consulte AWS Managed Microsoft AD los requisitos previos y Cómo crear un AWS Managed Microsoft AD directorio en la Guía del AWS Directory Service usuario.

Para asociar usuarios AWS Managed Microsoft AD, debe aprovisionar los usuarios en su AWS Managed Microsoft AD directorio. Para obtener más información, consulte Administración de usuarios y grupos en AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service .

Grupos de seguridad

Los grupos de seguridad controlan el tráfico de red que entra y sale de los recursos de la red. Para garantizar que los recursos de su entorno de suscripción basado en usuarios puedan comunicarse, sus grupos de seguridad deben cumplir los siguientes criterios.

Grupo de seguridad para puntos finales de VPC

Identifique o cree un grupo de seguridad que permita la conectividad de los puertos TCP entrantes. 1688 Al configurar los ajustes de la VPC, especificará este grupo de seguridad. Para obtener más información, consulte Trabajar con grupos de seguridad.

License Manager asocia este grupo de seguridad a los puntos finales de la VPC que crea en su nombre al configurar la VPC. Para obtener más información, consulte Acceda a un Servicio de AWS mediante un punto de conexión de VPC de interfaz en la Guía de AWS PrivateLink .

Grupo de seguridad para los controladores de dominio de Active Directory

Asegúrese de que el grupo de seguridad que utiliza para los controladores de dominio de AD permita el tráfico saliente a la IPv4 dirección de la interfaz de red de cada controlador de dominio.

Grupo de seguridad para instancias de suscripción basadas en usuarios

Identifique o cree un grupo de seguridad que permita los siguientes accesos hacia y desde su instancia. Para obtener más información, consulte Trabajar con grupos de seguridad.

- 3389Conectividad de puerto TCP entrante desde las fuentes de conexión aprobadas.
- 1688Conectividad de puertos TCP salientes para llegar a los puntos finales de la VPC y comunicarse con ellos. AWS Systems Manager

Configuración de red

License Manager crea dos interfaces de red que utilizan el grupo de seguridad predeterminado de la VPC en la que se aprovisiona AWS Managed Microsoft AD . Estas interfaces se utilizan para que el servicio interactúe con su directorio. Para obtener más información, consulte Paso 2: Registre su Active Directory en License Manager y Qué se crea en la Guía de administración de AWS Directory Service .

Una vez finalizado el proceso de aprovisionamiento, puede asociar un grupo de seguridad diferente a las interfaces creadas por License Manager.

Resolución de los DNS

El Active Directory que haya registrado para las suscripciones basadas en usuarios debe estar accesible desde cualquier VPCs subred que haya configurado en los ajustes de License Manager. Para garantizar que se pueda acceder a los nodos de Active Directory, configure la resolución de DNS de la siguiente manera:

- Configure el reenvío de DNS entre Active Directories VPCs y los que están configurados en la configuración de License Manager para las suscripciones basadas en usuarios. Puede utilizar Amazon Route 53 u otro servicio de DNS para el reenvío de DNS. Para obtener más información, consulte la entrada del blog “Integrating your Directory Service’s DNS resolution with Amazon Route 53 Resolvers”.
- Habilitar los nombres de host DNS y la resolución de DNS en la VPC. Para obtener más información, consulte Ver y actualizar los atributos de DNS de su VPC.

Instancias que ofrecen productos de suscripción basados en el usuario

Para que las instancias de suscripción basadas en usuarios funcionen según lo esperado, debe cumplir los siguientes requisitos previos:

- Configure un grupo de seguridad para sus instancias tal y como se describe en. Grupos de seguridad
- Asegúrese de que las instancias lanzadas para proporcionar suscripciones basadas en usuarios con Microsoft Office tengan una ruta a la subred en la que se aprovisionan los puntos de conexión de VPC.
- Las instancias que ofrecen suscripciones basadas en usuarios deben ser administradas por AWS Systems Manager personas para que estén en buen estado. Además, sus instancias deben poder

activar sus licencias de suscripción basadas en el usuario para seguir cumpliendo con las normas tras la activación de la licencia.

> **Note**
>
> License Manager intentará recuperar las instancias en mal estado, pero se terminarán las que no puedan volver a un estado correcto. Para obtener información sobre la solución de problemas en torno a cómo mantener las instancias administradas por Systems Manager y la conformidad de las instancias, consulte la sección Solucionar problemas de suscripciones basadas en usuarios en License Manager de esta guía.

- Debe disponer de un rol de perfil de instancia asociado a las instancias que proporcionan los productos de suscripción basada en usuarios que permita a AWS Systems Manager administrar el recurso. Para obtener más información, consulte Crear un perfil de instancias de IAM para Systems Manager en la Guía del usuario de AWS Systems Manager .
- Debe hacerlo Desvincular a los usuarios de una instancia antes de cerrar la instancia.

Servicios de escritorio remoto de Microsoft

El servidor de licencias de Microsoft Remote Desktop Services requiere un usuario administrativo definido en el Active Directory asociado. Ese usuario debe poder realizar las siguientes tareas:

- Cree una unidad organizativa en el dominio de Active Directory
- El dominio une las instancias (crea un ordenador) dentro de la OU que se crea
- Agregue un objeto informático a un grupo de servidores de Terminal Server dentro del dominio de Active Directory
- Delegue el control de los objetos de usuario del dominio de Active Directory para leer y escribir el servidor de licencias de Terminal Server, a fin de generar informes del servidor de licencias.

Para obtener más información sobre la delegación, consulte Delegación de control en los servicios de dominio de Active Directory.

Credenciales administrativas secretas

License Manager se utiliza AWS Secrets Manager para administrar las credenciales necesarias para las tareas de administración de usuarios en el servidor de licencias de Microsoft Remote Desktop Services. Antes de poder configurar el servidor de licencias, debe crear un secreto en

Secrets Manager que contenga las credenciales del usuario que realiza las tareas de administración de usuarios en el servidor de licencias. Al configurar los ajustes del servidor de licencias, debe proporcionar el ID del secreto que ha creado.

> **Note**
>
> Debe ser el mismo usuario que haya definido para la generación de informes del servidor de licencias de RDS.

Para crear un secreto, siga las instrucciones detalladas de la página Crear un AWS Secrets Manager secreto de la Guía del usuario de Secrets Manager, con los siguientes ajustes específicos de License Manager.

> **Important**
>
> Para usar el secreto, License Manager depende de los nombres de clave exactos, el valor del nombre de usuario y la clave de cifrado que se especifican en la siguiente lista. El nombre secreto debe empezar por el siguiente prefijo:`license-manager-user-`.

Se abre la página Elija tipo de secreto.

- Tipo de secreto: elija otro tipo de secreto.
- Pares clave/valor: especifique los siguientes pares de claves para guardarlos en el secreto.

  Nombre de usuario
  - Clave: `username`
  - Valor: `Administrator`

  Contraseña
  - Clave: `password`
  - Valor: *`The password`*
- Clave de cifrado: para especificar una clave de KMS distinta de la `aws/secretsmanager` clave, debe adjuntar una política a la función que utilice para acceder a las operaciones de License Manager. Para obtener más información, consulte Roles y permisos de IAM.

En la página de configuración secreta:

- Nombre secreto: especifique un nombre para el secreto que comience con el prefijo que License Manager usa para identificar los secretos de las credenciales del servidor de licencias. Por ejemplo:

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

En estas instrucciones se presupone que está utilizando el AWS Management Console para crear el secreto. La Guía del usuario de Secrets Manager también incluye instrucciones detalladas para otros métodos. Para obtener más información sobre Secrets Manager, consulte Qué es Secrets Manager. Para obtener información relacionada específicamente con los costos, consulte los precios AWS Secrets Manager en la Guía del usuario de Secrets Manager.

Productos de software compatibles para suscripciones basadas en usuarios en License Manager

AWS License Manager admite suscripciones basadas en usuarios para Microsoft Visual Studio y Microsoft Office. License Manager rastrea el uso del software compatible. Se requiere una única suscripción a Windows Server Remote Desktop Services Subscriber Access License (RDS SAL) para que cada usuario pueda acceder a una instancia con licencia incluida que proporciona un producto de suscripción basada en usuarios. Para obtener más información, consulte Comience con las suscripciones basadas en usuarios en License Manager.

Plataformas de sistema operativo (SO) compatibles con Windows

Puede encontrar Windows AMIs que incluye productos cubiertos por la licencia SAL de RDS para las siguientes plataformas de sistema operativo Windows:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Software compatible para suscripciones basadas en usuarios

License Manager admite licencias basadas en usuarios con el siguiente software.

- Microsoft Visual Studio

- Microsoft Office

Microsoft Visual Studio

Microsoft Visual Studio es un entorno de desarrollo integrado (IDE) que permite a los desarrolladores crear, editar, depurar y publicar aplicaciones. El Microsoft Visual Studio proporcionado AMIs incluye el AWS kit de herramientas para la refactorización de.NET y el. AWS Toolkit for Visual Studio

Ediciones compatibles

- Visual Studio Professional 2022
- Visual Studio Enterprise 2022

En la siguiente tabla se detallan los nombres de las suscripciones de software y el valor de producto asociado que se utilizan para las operaciones de la API de suscripción basada en usuarios de License Manager.

Nombre de la suscripción de software	Valor del producto
Visual Studio Enterprise 2022	`VISUAL_STUDIO_ENTERPRISE`
Visual Studio Professional 2022	`VISUAL_STUDIO_PROFESSIONAL`

Microsoft Office

Microsoft Office representa un conjunto de software desarrollado por Microsoft para diversos casos de uso de productividad, como trabajar con documentos, hojas de cálculo y presentaciones de diapositivas.

Ediciones compatibles

- Office LTSC Professional Plus 2021

En la siguiente tabla se detallan los nombres de las suscripciones de software y el valor de producto asociado que se utilizan para las operaciones de la API de suscripción basada en usuarios de License Manager.

Nombre de la suscripción de software	Valor del producto
Office LTSC Professional Plus 2021	`OFFICE_PROFESSIONAL_PLUS`

Active Directory

License Manager admite suscripciones basadas en usuarios para Microsoft Visual Studio, Microsoft Office y Remote Desktop Services Subscriber Access License (RDS SAL). Los productos pueden admitir Active Directory AWS Managed Microsoft AD o uno autoadministrado que esté implementado en su AWS entorno o que tenga conectividad de red a una VPC de su entorno. AWS

Esta tabla indica qué tipos de Active Directory admite cada producto de software cuando se usa con suscripciones basadas en usuarios:.

Producto de software	AWS Managed Microsoft AD	AD autogestionado
Microsoft Visual Studio	Compatible	No compatible
Microsoft Office	Compatible	No compatible
Producto RDS SAL	Soportado	Compatible

Software adicional

Puede instalar software adicional en sus instancias que no se encuentre disponible como suscripciones basadas en usuarios. License Manager no hace ningún seguimiento de las instalaciones de software adicionales. Estas instalaciones deben realizarse con la cuenta administrativa de su Active Directory. Si usa una AWS Managed Microsoft AD, la cuenta administrativa (Admin) se crea de forma predeterminada en su directorio. Para obtener más información, consulte Cuenta de administrador en la Guía de administración de AWS Directory Service .

Para instalar software adicional con la cuenta administrativa de Active Directory, debe:

- Suscriba la cuenta administrativa al producto proporcionado por la instancia.
- Asocie la cuenta administrativa a la instancia.

- Conéctese a la instancia mediante la cuenta administrativa para realizar la instalación.

Para obtener más información, consulte Comience con las suscripciones basadas en usuarios en License Manager.

Comience con las suscripciones basadas en usuarios en License Manager

En los pasos siguientes se detalla cómo puede empezar a utilizar las suscripciones basadas en usuarios. En estos pasos se presupone que ya ha implementado los requisitos previos necesarios. Para obtener más información, consulte la Requisitos previos para crear suscripciones basadas en usuarios en License Manager.

Pasos

- Paso 1: Suscríbase a un producto
- Paso 2: Registre su Active Directory en License Manager
- Paso 3: Configurar el servidor de licencias RDS
- Paso 4: Lanza una instancia para ofrecer suscripciones basadas en usuarios
- Paso 5: Asociar usuarios a una instancia de suscripción basada en usuarios

Paso 1: Suscríbase a un producto

Los productos de Microsoft, como Office o Visual Studio, requieren una suscripción activa antes de poder asociar usuarios de Active Directory a una instancia que incluya esos productos. Los productos de suscripción que se muestran con el estado de suscripción de Marketplace como Inactivo aún no están suscritos.

Cuando se suscribe a un producto de suscripción basado en usuarios de Microsoft desde el AWS Marketplace, License Manager agrega automáticamente una suscripción a los Servicios de Escritorio Remoto (RDS) de Microsoft para su cuenta, si aún no tiene una. El RDS es necesario para acceder de forma remota a los escritorios gráficos y a las aplicaciones de Windows basadas en suscripciones en las EC2 instancias lanzadas con licencia incluida. AMIs

Puede suscribirse a sus productos directamente en los siguientes enlaces AWS Marketplace :

- Visual Studio Professional
- Visual Studio Enterprise

- Office LTSC Professional Plus 2021
- Win Remote Desktop Services SAL

Descubra los productos y suscríbase a ellos desde la consola de License Manager

También puede descubrir los productos correspondientes a los que suscribirse en la consola License Manager.

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, en Suscripciones basadas en usuarios, seleccione Productos.
3. Elige el nombre de un producto para ver los detalles de la suscripción.
4. Seleccione Ver en AWS Marketplace.
5. Revise los detalles de la suscripción y seleccione Continuar para suscribirse.
6. Revise las condiciones y seleccione Aceptar condiciones si desea continuar.

Si acepta las condiciones, tendrá que tramitarse la suscripción del producto. Se indicará que la suscripción está en curso hasta que se complete el proceso. Puede repetir estos pasos para cualquier otro producto configurado que necesite. Una vez que todos los productos necesarios tengan una suscripción activa, puede continuar con la suscripción de los usuarios de Active Directory a los productos.

> **Note**
>
> En el caso de los períodos de facturación que no se hayan cerrado (marcados como estado de facturación pendiente), su factura estimada por los cargos relacionados con el número de usuarios y los costes relacionados tarda 48 horas en AWS Billing aparecer. Para obtener más información, consulte Visualización de su factura en la Guía del usuario de AWS Billing .

Paso 2: Registre su Active Directory en License Manager

License Manager requiere que los usuarios de suscripción estén definidos en Active Directory para poder asociarlos a suscripciones basadas en usuarios. Puede ser un Active Directory AWS Managed Microsoft AD o uno autogestionado, en función de sus suscripciones.

- Si se suscribe únicamente a productos independientes de Microsoft Office o Visual Studio, debe configurar un AWS Managed Microsoft AD.
- Si se suscribe a Win Remote Desktop Services SAL, puede utilizar un Active Directory AWS Managed Microsoft AD o uno autogestionado.

Para usar Microsoft Office con suscripciones basadas en usuarios, debe conceder permiso al License Manager para actualizar la configuración de la VPC. Al configurar la VPC, License Manager crea puntos de enlace de la VPC en su nombre. Estos puntos de conexión son necesarios para que los recursos se conecten a los servidores de activación y garanticen su conformidad.

Debe configurar el reenvío de DNS para todas las suscripciones adicionales VPCs que registre para las suscripciones basadas en usuarios. Si tiene varias suscripciones basadas en usuarios Regiones de AWS, cada región debe tener su propio Active Directory con el reenvío de DNS configurado.

> **Important**
>
> Debe permitir que License Manager cree el rol vinculado al servicio requerido para poder continuar. Para obtener más información, consulte la Requisitos previos para crear suscripciones basadas en usuarios en License Manager.

Los pasos de registro varían en la consola y dependen de los productos a los que se haya suscrito. Si se ha suscrito`Win Remote Desktop Services SAL`, seleccione la pestaña RDS SAL de Microsoft. Si está suscrito a Microsoft Office o Visual Studio y NO a RDS SAL, seleccione la pestaña Suscripciones MSO independientes.

Microsoft RDS SAL

Regístrese AWS Managed Microsoft AD

Para registrarse AWS Managed Microsoft AD como su Active Directory para las suscripciones basadas en usuarios, siga estos pasos:

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Diríjase a Suscripciones basadas en usuarios en la sección Configuración del panel de navegación izquierdo.
3. En la pestaña Servicios de escritorio remoto (RDS) de la página Suscripciones basadas en usuarios, seleccione Registrar Active Directory.

4. Seleccione la opción Active Directory AWS administrado para introducir los detalles.
5. Seleccione el directorio administrado de la lista de AWS Active Directory o cree un nuevo directorio administrado y, a continuación, vuelva a seleccionarlo.
6. Elija Registrar para registrar su Active Directory AWS administrado.

Registre Active Directory autogestionado

Para registrar un Active Directory autoadministrado para suscripciones basadas en usuarios, siga estos pasos:

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Diríjase a Suscripciones basadas en usuarios en la sección Configuración del panel de navegación izquierdo.
3. En la pestaña Servicios de escritorio remoto (RDS) de la página Suscripciones basadas en usuarios, seleccione Registrar Active Directory.
4. Seleccione la opción Active Directory autogestionada para introducir los detalles.
5. Introduzca el dominio de Active Directory, junto con IPv4 las direcciones privadas principales y secundarias del directorio.
6. En la sección Redes, seleccione la VPC y las dos subredes en las que reside su Active Directory.
7. Seleccione el secreto de credenciales administrativas que creó como parte de los requisitos previos para su suscripción a Microsoft RDS.

Stand-alone MSO subscriptions

Regístrese AWS Managed Microsoft AD

Para registrarse AWS Managed Microsoft AD como Active Directory para las suscripciones de Microsoft Office y Visual Studio basadas en usuarios, siga estos pasos:

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Diríjase a Suscripciones basadas en usuarios en la sección Configuración del panel de navegación izquierdo.
3. En la página Suscripciones basadas en usuarios, seleccione la pestaña del producto de suscripción de Microsoft Office o Visual Studio que desee registrar y, a continuación, elija Registrar Active Directory.

4. Seleccione el directorio administrado de la lista de AWS Active Directory o cree un nuevo directorio administrado y, a continuación, vuelva y selecciónelo.
5. Elija Registrar para registrar su Active Directory AWS administrado.

Al registrar su Active Directory, License Manager crea dos interfaces de red para que el servicio pueda comunicarse con su directorio. La interfaz de red tendrá una descripción similar a la interfaz de red para la que se AWS creó LicenseManager *<directory_id>*.

Registro de Active Directory desde AWS CLI

Puede registrar su Active Directory como proveedor de identidad para las suscripciones basadas en usuarios con el RegisterIdentityProvideroperación.

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

Configure Active Directory y su VPC para las suscripciones basadas en usuarios ()AWS CLI

Puede registrar su Active Directory como proveedor de identidades y configurar su VPC para las suscripciones basadas en usuarios con RegisterIdentityProvideroperación.

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

Para obtener más información acerca de los productos de software disponibles, consulte Productos de software compatibles para suscripciones basadas en usuarios en License Manager.

Paso 3: Configurar el servidor de licencias RDS

El servidor de licencias de Microsoft Remote Desktop Services (RDS) emite licencias de acceso de suscriptor (SALs) a los usuarios de Active Directory cuando acceden a EC2 instancias que ofrecen productos de Microsoft de suscripción basados en usuarios. Tras completar los pasos 1 y 2, puede configurar el servidor de licencias de la siguiente manera.

Asegúrese de haber completado el formulario Requisitos previos de una suscripción basada en el usuario de RDS antes de empezar. Este proceso supone que ya ha configurado su Active Directory.

Configure el servidor de licencias de RDS para las suscripciones basadas en usuarios (consola)

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Vaya a la página de suscripciones basadas en usuarios, en Configuración, en el panel de navegación izquierdo.
3. En la pestaña Servicios de escritorio remoto (RDS), debería ver uno o más Active Directories en la lista. Es posible que aparezca un mensaje que le indique que necesita configurar el RDS para su Active Directory.
4. En el mensaje o en el menú Acciones, seleccione Configurar el servidor de licencias de RDS.
5. En el cuadro de diálogo Configurar el servidor de licencias RDS, puede configurar los siguientes ajustes:

   Active Directory

   En esta sección se incluyen los detalles clave del directorio que está conectado al servidor de licencias RDS que configure.

   Secret

   Debe elegir un secreto existente o crear uno nuevo para las credenciales que se utilizan para las tareas de administración de usuarios en el servidor de licencias. La primera parte del nombre secreto debe seguir el patrón que se describe en la sección secreta de las credenciales administrativas delRequisitos previos de una suscripción basada en el usuario.

   Etiquetas

   Si lo desea, puede introducir etiquetas para el recurso del servidor de licencias.
6. Elija Configurar para guardar la configuración.

Paso 4: Lanza una instancia para ofrecer suscripciones basadas en usuarios

Tras suscribirse a un producto, debe lanzar instancias para que los usuarios se conecten a ellas desde la AWS Marketplace AMI que incluye el producto. Tras lanzar una instancia, AWS Systems Manager intenta unirla al dominio de Active Directory y realizar una configuración y un reforzamiento adicionales del recurso. Las configuraciones necesarias para que la instancia esté lista para su uso pueden tardar unos 20 minutos en completarse. Puede confirmar que el recurso está listo para usarse en la página Asociación de usuarios de la consola License Manager comprobando que el Estado de la instancia sea Activo.

Para lanzar una instancia con suscripciones basadas en usuarios, consulte. Lance una instancia a partir de una licencia incluida (AMI)

Paso 5: Asociar usuarios a una instancia de suscripción basada en usuarios

Una vez que se haya suscrito a la AWS Marketplace AMI del producto correspondiente, puede suscribir a los usuarios a un producto y asociarlos a una instancia que proporcione el producto. Puede suscribir a los usuarios a los productos y asociarlos a una instancia en un solo paso o por separado. Al suscribir a un usuario, se comprueba el directorio para garantizar que la identidad del usuario exista en él. Se crea una suscripción para cada usuario al que se suscriba al producto.

Cada usuario debe tener una suscripción a la licencia de acceso de suscriptor (RDS SAL) de Windows Server Remote Desktop Services y al producto que vaya a utilizar.

Cuando su cuenta se ha suscrito a RDS SAL como se detalla enPaso 1: Suscríbase a un producto, License Manager suscribe automáticamente a los usuarios de su Active Directory a RDS SAL cuando se suscriben a un producto de suscripción basado en usuarios.

> **Note**
>
> Si un usuario que nunca se ha suscrito inicia sesión en una instancia asociada a RDS SAL, License Manager la suscribe automáticamente e inicia la facturación de Microsoft RDS. La facturación continúa hasta que se cancele la suscripción y caduque el token de licencia emitido por el servidor de licencias SAL de RDS.
> Del mismo modo, si un usuario previamente suscrito cancela su suscripción, pero sigue iniciando sesión después de que caduque su token de licencia SAL de RDS, volverá a suscribirse automáticamente y la facturación continuará hasta que se cancele de nuevo la suscripción y su token caduque.

Para obtener más información sobre los cargos y la facturación de las suscripciones, consulte. Cargos de suscripción en License Manager

La página de productos de License Manager muestra las suscripciones activas y muestra su estado de suscripción a Marketplace como Activo. En la página de detalles del producto, License Manager muestra las suscripciones de usuario activas con el estado Suscrito.

> **Important**
>
> Si su Active Directory no está configurado con el producto, aparece una barra de notificaciones en la parte superior de la consola en la que se le indica que debe ajustar la configuración del directorio. En la barra de notificaciones, seleccione Abrir configuración para acceder a la página Configuración de License Manager y editar el directorio.
> Cada usuario debe tener una suscripción tanto a RDS SAL como al producto que vaya a utilizar. No se podrá suscribir a los usuarios a un producto cuyo Estado de suscripción de Marketplace sea Inactivo.

Suscripción de usuarios a un producto y asociación a una instancia

Al seleccionar una instancia a la que asociar los usuarios, también puede suscribirlos a los productos que ofrece la instancia si aún no están suscritos. Usa uno de los siguientes métodos para suscribir y asociar usuarios.

Console

Para asociar usuarios a una instancia, sigue estos pasos:

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, en Suscripciones basadas en usuarios, seleccione Asociación de usuarios.
3. Seleccione la instancia a la que desee asociar los usuarios y, a continuación, elija una de las siguientes opciones:

   Asocia usuarios

   Especifique hasta 20 nombres de usuario que existan en su directorio, incluido el nombre de dominio si existen en un dominio de confianza, y elija Asociar. Si utilizas este método, los usuarios ya deben estar suscritos a los productos que ofrece la instancia.

   Suscríbase y asocie usuarios

   Especifique hasta 20 nombres de usuario que existan en su directorio, incluido el nombre de dominio si existen en un dominio de confianza, y elija Suscríbete y asocia.

(Opcional) Revise las asociaciones de usuarios

En la página de asociación de usuarios, los usuarios que ha seleccionado se muestran en Usuarios con el estado de asociación asociado.

(Opcional) Revisa los usuarios suscritos

En la página de productos, elige el nombre del producto. Los usuarios suscritos se muestran en Usuarios con el estado Suscrito.

AWS CLI

Puede asociar los usuarios a una instancia lanzada para proporcionar a la suscripción basada en usuarios la AssociateUseroperación.

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

Procedimiento de asociación de usuarios de Active Directory autogestionado a una instancia (AWS CLI)

Puede asociar los usuarios de su Active Directory autogestionado a una instancia lanzada para proporcionar a la suscripción basada en usuarios el AssociateUseroperación.

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

Para obtener más información acerca de los productos de software disponibles, consulte Productos de software compatibles para suscripciones basadas en usuarios en License Manager.

Suscripción de usuarios a un producto

Puede suscribir usuarios a un producto mediante uno de los siguientes métodos.

Console

Suscribir usuarios a un producto (consola)

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, en Suscripciones basadas en usuarios, seleccione Productos.

3. Seleccione un producto para suscribir a los usuarios en el que el estado de suscripción de Marketplace sea Activo.
4. Si el producto es Microsoft RDS, seleccione el Active Directory registrado que contiene los usuarios a los que desea suscribirse.
5. Elija Suscribir usuario para continuar.
6. Especifique hasta 20 nombres de usuario que existan en su directorio, incluido el nombre de dominio si se encuentran en un dominio de confianza, y seleccione Suscribirse.

   Los usuarios que tienen una suscripción aparecen en Usuarios con el estado Suscrito.

AWS CLI

Suscribe a los usuarios a un producto ()AWS CLI

Puede suscribir a los usuarios a un producto que esté registrado con su proveedor de identidad mediante el StartProductSubscriptionoperación.

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

Suscriba a los usuarios a un producto con un Active Directory autogestionado ()AWS CLI

Puede suscribir a los usuarios de su Active Directory autogestionado a un producto registrado en su AWS Managed Microsoft AD directorio mediante el StartProductSubscriptionoperación.

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

Para obtener más información acerca de los productos de software disponibles, consulte Productos de software compatibles para suscripciones basadas en usuarios en License Manager.

Los usuarios que cuenten con una suscripción se mostrarán en Usuarios con el Estado Suscrito.

Configure el GPO de Active Directory para sesiones de usuarios remotos más activas

De forma predeterminada, Microsoft RDS permite un máximo de dos sesiones de usuario al mismo tiempo en una instancia de EC2 Windows que proporciona productos de suscripción basados en usuarios. Después de configurar los puntos finales del servidor de licencias, puede configurar Microsoft RDS para permitir más de dos sesiones de usuario al mismo tiempo con un objeto de política de grupo (GPO) de Active Directory, de la siguiente manera.

Requisito previo

Debe haber creado un servidor de licencias en su entorno. Para crear un servidor de licencias, consultePaso 3: Configurar el servidor de licencias RDS.

1. La herramienta que utilice para configurar el GPO depende del lugar desde el que lo ejecute, de la siguiente manera:

   Configuración central desde el controlador de dominio

   Inicie sesión en su controlador de dominio de Active Directory como administrador y abra la Consola de administración de políticas de grupo de Windows.

   Configure la política de grupo en el host de la sesión

   Inicie sesión en su servidor de licencias como administrador y abra el editor de políticas de grupo local.
2. Desde la consola de administración o el editor de políticas, edite la política de grupo para especificar los hosts de sesión que se conectan a través de Microsoft RDS. Puede encontrar el punto final de su servidor de licencias de RDS en la página de detalles del producto License Manager o con el list-license-server-endpointscomando de. AWS CLI
3. Defina el modo de licencia del host de sesión de escritorio remoto en y `Per User` guárdelo.

Para obtener más información sobre la configuración del servidor de licencias de RDS para License Manager, consulte the section called “Paso 3: Configurar RDS” el tema Introducción. Para obtener más información acerca de la configuración de los hosts de sesión de Microsoft RDS, consulte Licenciar los hosts de sesión de Remote Desktop.

Lance una instancia a partir de una licencia incluida (AMI)

Tras suscribirse a un producto, debe lanzar instancias para que los usuarios se conecten a ellas desde la AWS Marketplace AMI que incluye el producto. Tras lanzar una instancia, AWS Systems Manager intenta unirla al dominio de Active Directory y realizar una configuración y un reforzamiento adicionales del recurso. Las configuraciones necesarias para que la instancia esté lista para su uso pueden tardar unos 20 minutos en completarse. Puede confirmar que el recurso está listo para usarse en la página Asociación de usuarios de la consola License Manager comprobando que el Estado de la instancia sea Activo.

> **Important**
>
> Las instancias que lance deben cumplir los requisitos previos necesarios para garantizar su conformidad. Los recursos que no puedan completar la configuración inicial se cancelarán. Para obtener más información, consulte Requisitos previos para crear suscripciones basadas en usuarios en License Manager y Solucionar problemas de suscripciones basadas en usuarios en License Manager.

Lanza una instancia con suscripciones basadas en usuarios

1. Accede a la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En Imágenes, seleccione Catálogo de AMI.
3. Elija AWS Marketplace AMIs.
4. Introduzca el nombre del producto en el cuadro de búsqueda y pulse Intro. Por ejemplo, puede buscar **`Visual Studio`**.
5. En Editor, seleccione Amazon Web Services.
6. Haga clic en Seleccionar para el producto en el que desee lanzar una instancia para proporcionar suscripciones basadas en usuarios.
7. Seleccione Continuar para continuar.
8. Seleccione Lanzar la instancia con AMI.
9. Complete los pasos del asistente y asegúrese de hacer todo lo siguiente:
    a. Elija un tipo de instancia basado en Nitro que no se base en Graviton.
    b. Elija una VPC y una subred desde las que la instancia pueda conectarse a su directorio de AWS Managed Microsoft AD .

c. Elija un grupo de seguridad que permita la conectividad de la instancia a su Active Directory.

d. Amplíe los Detalles avanzados y elija un rol de IAM que permita la funcionalidad de Systems Manager para la instancia.

10. Seleccione Iniciar instancia.

Si tiene instancias en ejecución de la AWS Marketplace AMI, debe suscribir a los usuarios al producto y asociarlos a instancias que proporcionan el producto para que puedan usarlo.

Lanzar una instancia desde una versión de sistema operativo específica (AMI)

Al lanzar una instancia desde una AMI compatible con `Office LTSC Professional Plus` Microsoft Visual Studio, el inicio se realiza de forma predeterminada con la última versión de la AMI del sistema operativo Windows (por ejemplo, Windows Server 2025). Para iniciar con una versión de sistema operativo (AMI) específica, siga estos pasos.

1. Abra la AWS Marketplace consola en https://console.aws.amazon.com/market.
2. Elija Administrar suscripciones del panel de navegación.
3. Para optimizar los resultados de la suscripción, puedes buscar todo o parte del nombre de la suscripción. Por ejemplo, `Office LTSC Professional Plus 2021` o `Visual Studio Enterprise`.
4. Selecciona Lanzar nueva instancia en el panel de suscripción. Esto abre una página de configuración de lanzamiento.
5. Para lanzar una instancia desde una AMI basada en una versión anterior de la plataforma del sistema operativo Windows, seleccione el enlace completo al AWS Marketplace sitio web, ubicado en la versión de software. Esto le llevará a una página de configuración donde podrá seleccionar de una lista de versiones.
6. La lista muestra las últimas versiones de AMI para las plataformas de sistema operativo Windows compatibles. Seleccione la versión del sistema operativo Windows desde la que desee iniciar.

Conéctese a una instancia de suscripción basada en usuarios con RDP

Una vez que haya asociado a los usuarios a la instancia que proporciona el producto, pueden conectarse a la instancia si el Estado de la instancia es Activo. Los usuarios deberán conectarse con sus credenciales de usuario del dominio para poder utilizar el producto con su identidad asociada.

> **Important**
>
> El proceso de crear la EC2 instancia y prepararla para los usuarios puede tardar unos 20 minutos. El estado de asociación de la instancia debe ser Activo para poder acceder a ella y utilizar el producto.

Procedimiento de conexión a instancias de suscripción basada en usuarios

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, en Suscripciones basadas en usuarios, seleccione Asociación de usuarios.
3. En la página Asociación de usuarios, confirme que el Estado de la instancia sea Activo.
4. Anote el ID de la instancia, ya que lo necesitará para recopilar los detalles de la conexión.
5. Siga los pasos que se indican en Conectarse a una instancia de Windows mediante RDP y asegúrese de especificar el nombre de usuario completo del usuario asociado.

Modifique la configuración del firewall de su suscripción a Microsoft Office

Un firewall protege los recursos de la red del tráfico entrante o saliente no autorizado. Las reglas que defina para su grupo de seguridad actúan como firewall para los recursos de VPC que trabajan juntos para proporcionar suscripciones basadas en usuarios a instancias de Microsoft Office en EC2 Windows.

Puede seguir los siguientes pasos para editar las subredes y el grupo de seguridad. License Manager usa su configuración para aprovisionar puntos finales para Microsoft Office. AWS PrivateLinkPara obtener más información sobre los puntos de enlace de VPC, consulte ¿Qué es? AWS PrivateLink en la documentación de Amazon Virtual Private Cloud.

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Vaya a la página de suscripciones basadas en usuarios, en Configuración, en el panel de navegación izquierdo.
3. Para editar la configuración del firewall, seleccione la pestaña del producto de suscripción de Microsoft Office y, a continuación, elija Editar en la parte superior de la sección Firewall. Se abrirá el cuadro de diálogo Editar firewall.

4. Tras cambiar la configuración, seleccione Guardar para actualizar o Cancelar para conservar la configuración actual.

License Manager puede tardar unos minutos en completar los cambios de esta configuración.

Administre los usuarios de suscripción para las suscripciones basadas en usuarios de License Manager

Para garantizar la precisión de la facturación y los informes de las suscripciones a productos de Microsoft Office y Visual Studio en License Manager y para evitar el acceso no autorizado a los recursos de suscripción, puede administrar el acceso de los usuarios de la siguiente manera.

Desvincular a los usuarios de una instancia

Desasocie a un usuario de una instancia que aloja una suscripción a un producto de Microsoft Office o Visual Studio basado en usuarios de License Manager para eliminar el acceso al recurso.

Cancelar la suscripción de usuarios

Dé de baja a los usuarios de las suscripciones de productos de Microsoft Office o Visual Studio basadas en usuarios AWS License Manager para dejar de incurrir en cargos de suscripción para esas personas.

> **Note**
>
> La eliminación de un usuario de Active Directory no alterará las asociaciones de usuarios ni las suscripciones de los productos de Microsoft Office y Visual Studio. Debe desasociar al usuario en License Manager de la página de detalles del producto de suscripción para eliminar su asociación con una instancia. A continuación, debe cancelar la suscripción del usuario.
> Este tema no trata sobre la administración de Active Directory.

Contenido

- Desasociar usuarios de una instancia que proporciona suscripciones basadas en usuarios de License Manager
- Cancelar la suscripción de usuarios a productos basados en usuarios en License Manager

Desasociar usuarios de una instancia que proporciona suscripciones basadas en usuarios de License Manager

Para eliminar el acceso de los usuarios a una instancia que proporciona suscripciones basadas en usuarios de License Manager, puede desasociar al usuario suscrito de esa instancia. Este cambio no afecta al estado de la suscripción del usuario. Para cancelar la suscripción de un usuario y detener los cargos de suscripción para esa persona, consulte[Cancelar la suscripción de usuarios a productos basados en usuarios en License Manager](#).

Desvincular a los usuarios de suscripción de una instancia

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, en Suscripciones basadas en usuarios, seleccione Asociación de usuarios.
3. Seleccione la instancia de la que desea desasociar los usuarios.
4. Seleccione los nombres de usuario para los que desee realizar la desasociación y, a continuación, seleccione Desasociar usuarios.

Cancelar la suscripción de usuarios a productos basados en usuarios en License Manager

Debe cancelar la suscripción de un usuario de un producto de suscripción basado en usuarios de Microsoft Office o Visual Studio para dejar de incurrir en cargos por él. Microsoft RDS se factura por usuario y mes en función de una combinación de la suscripción de usuario y el token de licencia de acceso de cliente (CAL) que se emite desde el servidor de licencias cuando el usuario se conecta a una instancia que proporciona el producto de suscripción. Para obtener más información, consulte Facturación de Microsoft RDS en License Manager.

> **Important**
>
> En el caso de los productos de suscripción basados en usuarios de Microsoft Office o Visual Studio, primero debe desasociar al usuario de Active Directory de todas las instancias a las que esté asociado actualmente para poder cancelar su suscripción.

Anule la suscripción de los usuarios a productos basados en usuarios

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, en Suscripciones basadas en usuarios, seleccione Productos.
3. Seleccione el producto del que quiera cancelar la suscripción de los usuarios.
4. Seleccione los nombres de usuario para cancelar la suscripción y, a continuación, seleccione Cancelar la suscripción de usuarios.

Anular el registro de un Active Directory desde la configuración de License Manager

Puede anular el registro de Active Directory desde la configuración de License Manager si ya no quiere usarlo para suscripciones basadas en usuarios. Al anular el registro de la configuración del directorio de los ajustes de License Manager, no se elimina el directorio. Al anular el registro del directorio en la configuración, ya no podrá asociar usuarios de ese directorio para las suscripciones basadas en usuarios en License Manager.

Requisitos previos

Antes de anular el registro del directorio en la configuración de License Manager, debe realizar las siguientes tareas:

1. Desvincular a los usuarios de una instanciade cada instancia que haga referencia al directorio del que desee anular el registro.
2. Una vez que todos los usuarios de la suscripción se hayan desasociado de la instancia, finalice la instancia. Repita este procedimiento hasta que se cancelen todas las instancias que hacen referencia a Active Directory.
3. También es necesario Cancelar la suscripción de usuarios que pertenezcan al Active Directory y cancele el registro para que no se produzcan cambios en ellas.

Anule el registro

> **Important**
>
> Si los usuarios de RDS SAL de Microsoft utilizan Active Directory, debe eliminar el punto final del servidor de licencias asociado antes de anular el registro y eliminar el AD.

Anular el registro de Active Directory desde la configuración de License Manager

Cuando haya completado todas las tareas previas, abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.

1. En el panel de navegación izquierdo, elija Configuración.
2. En la página de configuración, en la AWS Managed Microsoft AD sección, seleccione Eliminar.
3. Introduzca el texto necesario para confirmar que desea eliminar el directorio y seleccione Eliminar.

Tras seleccionar Eliminar, la AWS Managed Microsoft ADsección de la página de configuración muestra su ID de directorio con el estado de la configuración. Una vez finalizado el proceso de configuración, el directorio se elimina de la AWS Managed Microsoft ADsección.

Solucionar problemas de suscripciones basadas en usuarios en License Manager

A continuación, se ofrecen algunas sugerencias para solucionar problemas que puedan producirse con las suscripciones basadas en usuarios en AWS License Manager.

Contenido

- Solucione los problemas de conformidad de las instancias
- Solucione problemas de conformidad con las licencias
- Solucione los problemas de conectividad de las instancias
- Solucione problemas al unirse al dominio
- Solucionar problemas de conectividad de Systems Manager
- Solución de problemas de Systems Manager Run Command
- Solución de problemas relacionados con las licencias de Microsoft RDS
- Solucionar errores de activación de Microsoft Office

Solucione los problemas de conformidad de las instancias

Las instancias que proporcionan suscripciones basadas en usuarios deben mantenerse en buen estado para garantizar su conformidad. Las instancias marcadas como en mal estado ya no cumplen los requisitos previos requeridos. License Manager intentará volver a poner las instancias en buen estado, pero se terminarán las que no puedan volver a un estado correcto.

Las instancias que se hayan lanzado para proporcionar suscripciones basadas en usuarios y no puedan completar la configuración inicial se terminarán. En esta situación, debe corregir el problema de configuración y lanzar nuevas instancias para proporcionar suscripciones basadas en usuarios. Para obtener más información, consulte la Requisitos previos para crear suscripciones basadas en usuarios en License Manager.

Solucione problemas de conformidad con las licencias

Si configuró su Active Directory para proporcionar suscripciones basadas en usuarios con Microsoft Office, debe asegurarse de que sus recursos puedan conectarse a los puntos finales de VPC que crea License Manager. Los puntos de conexión requieren tráfico de entrada en el puerto TCP 1688 desde las instancias que proporcionan suscripciones basadas en usuarios.

Puede usar Reachability Analyzer para confirmar que la configuración de red de las instancias que proporcionan suscripciones basadas en usuarios y los puntos de conexión de VPC se han configurado correctamente. Puede especificar un ID de instancia lanzado en una subred que proporcione suscripciones basadas en usuarios como origen y un punto de conexión de VPC aprovisionado para productos de Microsoft Office como destino. Especifique TCP como protocolo y 1688 como puerto de destino para la ruta que se va a analizar. Para obtener más información, consulte ¿Cómo puedo solucionar los problemas de conectividad de mi puerta de enlace y mis puntos de conexión de VPC de interfaz?

Solucione los problemas de conectividad de las instancias

Los usuarios deben poder usar RDP para conectarse a las instancias que proporcionan suscripciones basadas en usuarios para poder usar los productos que contienen. Para obtener más información sobre la solución de problemas de conectividad de instancias, consulta Solución de problemas de conexión a tu instancia de Windows en la Guía del EC2 usuario de Amazon.

Solucione problemas al unirse al dominio

Los usuarios deben poder conectarse a las instancias que proporcionan los productos de suscripción basados en usuarios con sus identidades de usuario desde el Active Directory configurado en la configuración de License Manager. Las instancias que no se unan al dominio se terminarán.

Para solucionar el problema, es posible que tenga que lanzar una instancia y unirse manualmente al dominio a fin de que el recurso no se termine antes de poder investigar. La instancia debe recibir y ejecutar correctamente el comando de ejecución de Systems Manager y, además, debe poder completar la unión al dominio en el sistema operativo. Para obtener más información, consulte Descripción de los estados del comando en la Guía del usuario de AWS Systems Manager y How to troubleshoot errors that occur when you join Windows-based computers to a domain en el sitio web de Microsoft.

Si lanza instancias desde una AMI personalizada que utiliza la AMI de un producto de suscripción basado en el usuario como imagen base, debe realizar los pasos de Sysprep en la AMI personalizada para garantizar un nombre de equipo único en el momento del lanzamiento. Antes de ejecutar Sysprep con /generalize, asegúrese de eliminar la máquina del dominio.

Solucionar problemas de conectividad de Systems Manager

Las instancias que ofrecen suscripciones basadas en usuarios deben gestionarse por, de lo AWS Systems Manager contrario, se cancelarán. Para obtener más información, consulte Solución de problemas de SSM Agent y Solución de problemas de disponibilidad de nodos administrados en la Guía del usuario de AWS Systems Manager .

Solución de problemas de Systems Manager Run Command

Run Command, una función de Systems Manager, se usa con instancias que proporcionan suscripciones basadas en usuarios para unirse al dominio, endurecer el sistema operativo y realizar auditorías de acceso para el producto incluido. Para obtener más información, consulte Descripción de los estados del comando en la Guía del usuario de AWS Systems Manager .

Solución de problemas relacionados con las licencias de Microsoft RDS

Si tiene problemas con la emisión de la CAL (licencia de acceso de cliente), compruebe si hay servidores de licencias Microsoft RDS adicionales en su granja de servidores o en su grupo de servidores Terminal Server. No recomendamos tener servidores de licencias adicionales en estas ubicaciones, ya que esto puede interferir con la emisión de las CAL y provocar complicaciones en materia de licencias.

Para resolver este problema, asegúrese de que solo los servidores RDS de Microsoft previstos permanezcan en la granja de servidores y en el grupo de servidores Terminal Server.

Al solucionar problemas de licencias, tenga en cuenta que las conexiones que utilizan el the /admin flag bypass standard licensing checks, as this flag is intended for administrative purposes, and doesn't consume a CAL. This can mask underlying licensing problems. To diagnose licensing issues, verify that standard user connections (without the /admin indicador funcionan correctamente para la administración de licencias.

Solucionar errores de activación de Microsoft Office

Si se produce un error en la activación de Microsoft Office, compruebe que la instancia tenga acceso a la VPC definida para License Manager. Cualquiera de las siguientes opciones cumple este requisito:

- La instancia se ejecuta en la VPC que está integrada con License Manager (a través del punto de conexión de la VPC)
- La instancia se ejecuta en una VPC emparejada con la VPC integrada en License Manager.

Para resolver este problema, asegúrese de mover la instancia a la VPC correcta o establezca un emparejamiento de VPC con la VPC integrada en License Manager.

Gestione las suscripciones de Linux en License Manager

Con AWS License Manager, puedes ver y gestionar las suscripciones comerciales de Linux que utilizan tus EC2 instancias de Amazon. Puedes realizar un seguimiento del uso de tus suscripciones de Linux para las cuentas Regiones de AWS y cuentas AWS Organizations que hayas definido en tu configuración. License Manager le ofrece una vista completa de las instancias en ejecución que utilizan suscripciones de Linux. También indica si una instancia tiene más de una suscripción definida.

Los datos que descubre License Manager se agregan y se muestran en la consola de License Manager y en el CloudWatch panel de control de Amazon. También puede acceder a los datos de su suscripción a través de la API de suscripción de License Manager Linux o asociada SDKs. AWS CLI

Las suscripciones a licencias de Linux pueden proceder de las siguientes fuentes:

Suscripción incluida AMIs

- Red Hat Enterprise Linux (RHEL)
- Modelo Bring Your Own Subscription (BYOS) de RHEL con el programa Red Hat Cloud Access
- SUSE Linux Enterprise Server
- AMI de Ubuntu Pro incluida en la suscripción

Proveedores de suscripción de terceros

- Suscripción a RHEL de Red Hat Subscription Manager (RHSM)

La detección de suscripciones de Linux utiliza el modelo de coherencia final. Un modelo de coherencia determina la manera y el momento en que se cargan los datos y se presentan en la vista de suscripciones de Linux. Con este modelo, License Manager garantiza que los datos de su suscripción a Linux se actualicen periódicamente a partir de sus recursos. En el caso de que algunos datos no se ingieran durante estos intervalos, la información se entrega en la siguiente emisión métrica. Este comportamiento puede retrasar la visualización de los recursos, como las instancias de Linux EC2 comerciales recién lanzadas, en el panel de suscripciones de Linux.

> **Note**
>
> La detección inicial de los recursos puede tardar hasta 36 horas en completarse y las instancias recién lanzadas tardan hasta 12 horas en detectarse y notificarse. Una vez descubiertos tus recursos, CloudWatch las métricas de Amazon se emiten cada hora para los datos de suscripciones de Linux.

Si sus cuentas están activas AWS Organizations, puede registrar una cuenta de miembro como administrador delegado. Para obtener más información, consulte Configuración de administrador delegado en License Manager.

Se detectaron suscripciones duplicadas

Cuando License Manager detecta dos suscripciones de Linux en la misma EC2 instancia, activa la alerta de suscripción duplicada. Puede ver y filtrar los datos de suscripción de Linux desde la página Instancias de la consola de License Manager.

Instancias de Red Hat Enterprise Linux 7 Extended Lifecycle Support (RHEL 7 ELS): si lanza una instancia desde una AMI incluida en una suscripción para RHEL 7 ELS, debe seguir registrando la instancia en Red Hat y consumir un derecho. En este caso, License Manager informa de una suscripción duplicada, pero ese es el comportamiento esperado.

Otras instancias de Red Hat Linux: le recomendamos que busque en el inventario de suscripciones de Red Hat Hybrid Cloud Console para averiguar qué suscripciones consume su instancia.

Temas adicionales

- Configurar la detección de suscripciones de Linux en License Manager
- Ver los datos de las instancias descubiertas en License Manager
- Información de facturación de las suscripciones de Linux en License Manager
- Gestione CloudWatch las alarmas de Amazon para las suscripciones de Linux en License Manager

Configurar la detección de suscripciones de Linux en License Manager

Puede configurar la detección de suscripciones de Linux a través de la consola de License Manager AWS CLI, la API de suscripciones de Linux de License Manager o la asociada SDKs. Al activar la detección de suscripciones de Linux para las Regiones de AWS que especifique, si lo desea, puede extender la detección a sus cuentas de AWS Organizations. Si ya no desea realizar un seguimiento del uso de las suscripciones, también puede desactivar la detección.

> **Note**
>
> De forma predeterminada, puede detectar y mostrar hasta 5000 recursos Región de AWS por cuenta. Para solicitar un aumento de estos límites, utilice el formulario de aumento de límites.

Temas

- Configure la detección de suscripciones de Linux
- Active la detección de suscripciones de Red Hat Subscription Manager
- Motivos de los distintos estados de detección de los recursos
- Desactive la detección de suscripciones a Linux

Configure la detección de suscripciones de Linux

Para configurar la detección de suscripciones de Linux desde la página de configuración de la consola de License Manager, siga estos pasos:

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación, seleccione Configuración. Se abrirá la página de configuración.
3. Abre la pestaña de suscripciones de Linux y selecciona Configurar. Esto abre el panel de configuración de las suscripciones de Linux.
4. Seleccione la fuente en la Regiones de AWS que debe ejecutarse la detección de suscripciones de Linux.
5. Para agregar los datos de suscripción de tus cuentas AWS Organizations, selecciona Vincular AWS Organizations. Esta opción solo aparece si AWS Organizations está configurada para tu cuenta.
6. Revise y confirme la opción que otorga AWS License Manager permiso para crear un rol vinculado a un servicio para las suscripciones de Linux.
7. Seleccione Guardar configuración.

Active la detección de suscripciones de Red Hat Subscription Manager

Para recuperar la información de suscripción de Red Hat Subscription Manager (RHSM) en su nombre, License Manager debe proporcionar las credenciales de API de su cuenta de cliente de Red Hat.

Requisitos previos

Antes de activar la detección de suscripciones, asegúrese de cumplir los siguientes requisitos previos.

- Para Cuenta de AWS poder configurar la detección de suscripciones de RHSM, debe estar activada la detección predeterminada para las suscripciones de Linux. Si la detección predeterminada está desactivada, consulteConfigure la detección de suscripciones de Linux.
- Si utiliza un inicio de sesión corporativo de Red Hat proporcionado por el administrador de su organización, asegúrese de que su ID de inicio de sesión tenga los siguientes roles y permisos asignados:
  - Función: Administrar sus suscripciones

- Permisos:`View All`, o `View/Edit All`

  Si su ID de inicio de sesión no tiene las funciones y los permisos necesarios, póngase en contacto con el administrador de la organización del portal Red Hat y solicite añadirlos a su nombre de usuario. Para obtener más información sobre los roles y permisos de Red Hat, consulte Roles y permisos del Portal de Clientes de Red Hat. Para obtener más información sobre cómo ponerse en contacto con el administrador de la organización de Red Hat Portal, consulte ¿Cómo sé quién es el administrador de mi organización? en la base de conocimiento del portal de clientes de Red Hat.

- Para activar la detección de suscripciones a RHSM, debe proporcionar el token offline de la API de la cuenta de cliente de Red Hat o un AWS Secrets Manager secreto que contenga el token offline. Para obtener su token sin conexión, siga los pasos descritos en Generar un nuevo token sin conexión en el sitio web de documentación de Red Hat.

  > **Important**
  >
  > Su seguridad es importante para nosotros. Su token de acceso offline de Red Hat se almacena de forma segura en Secrets Manager. License Manager usa su secreto para generar un token de acceso temporal cada vez que solicita detalles de suscripción a Red Hat.

Activación

Para activar la detección de RHSM desde la página de configuración de la consola de License Manager, siga estos pasos:

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación, seleccione Configuración.
3. En la página de configuración, abra la pestaña de suscripciones de Linux.
4. Selecciona Editar para actualizar la configuración de tu suscripción a Linux. Se abrirá la página de descubrimiento de cómo configurar las suscripciones de Linux.
5. Para iniciar el proceso de activación, seleccione la casilla Activar la detección de Red Hat Subscription Manager (RHSM). Aparece el panel de la cuenta Link RHSM.
6. Selecciona la opción Secreto (token) que corresponda a tu secreto y sigue los pasos restantes, que dependen de la opción que elijas.
7. Opción: se recomienda crear un secreto nuevo

Proporcione el token de acceso offline de Red Hat y deje que License Manager cree el secreto de acceso en Secrets Manager en su nombre.

a. Introduzca un nombre para su secreto en Nombre secreto.

b. Pegue su token de acceso sin conexión de Red Hat en la casilla del token sin conexión. Asegúrese de que no haya espacios ni saltos de línea adicionales antes o después del valor del token. Puede generar su token de acceso sin conexión a Red Hat en la página de tokens de la API de Red Hat Subscription Manager.

Opción: seleccione un secreto

Seleccione un secreto existente en Secrets Manager que contenga su token de acceso sin conexión de Red Hat.

8. (opcional) Añada etiquetas a su secreto.
9. Seleccione la casilla de verificación en la parte inferior de la página para confirmar que, al activar Red Hat Subscription Manager discovery, otorga acceso al AWS License Manager servicio para recopilar datos relacionados con las suscripciones de Red Hat utilizadas en las EC2 instancias de Amazon.
10. Seleccione Activar.

Motivos de los distintos estados de detección de los recursos

AWS License Manager mostrará un estado y el motivo de estado correspondiente para cada una de las suscripciones Región de AWS que elija para habilitar la detección de suscripciones de Linux. El motivo del estado variará si ha vinculado las suscripciones de Linux con AWS Organizations:

- En curso
- Correcto
- Con error

El motivo del estado que se muestra para cada región que elija mostrará hasta dos motivos del estado a la vez. En la siguiente tabla se proporcionan más detalles:

Acción del motivo del estado	Descripción
Incorporación de cuenta	Se está incorporando una sola cuenta.
Eliminación de cuenta	Se está eliminando una sola cuenta.
Incorporación de organización	Se está incorporando una organización entera.
Eliminación de organización	Se está eliminando una organización entera.

Puede llamar a la API `UpdateServiceSettings` y, posteriormente, llamar a la API `GetServiceSettings` para supervisar el progreso de la habilitación de las suscripciones de Linux. Cada estado y motivo del estado se pueden aplicar a varias regiones a la vez. En la siguiente tabla se proporcionan más detalles sobre el estado y el motivo del estado:

Estado	Motivo del estado	Descripción
En curso	`"Region": "Account-Onboard: Pending"`	Se están habilitando las suscripciones de Linux para una sola cuenta.
	`"Region": "Org-Onboard: Pending"`	Se están habilitando las suscripciones de Linux para una organización.
	`"Region": "Account-Offboard: Pending`	Se están deshabilitando las suscripciones de Linux para una sola cuenta.
	`"Region": "Org-Offboard: Pending`	Se están deshabilitando las suscripciones de Linux para una organización.

Estado	Motivo del estado	Descripción
Correcto	`"Region": "Account-Onboard: Successful"`	Se han habilitado correctamente las suscripciones de Linux para una sola cuenta.
	`"Region": "Org-Onboard: Successful"`	Se han habilitado correctamente las suscripciones de Linux para una organización.
	`"Region": "Account-Offboard: Successful`	Se han deshabilitado correctamente las suscripciones de Linux para una sola cuenta.
	`"Region": "Org-Offboard: Successful`	Se han deshabilitado correctamente las suscripciones de Linux para una organización.
Con error	`"Region": "Account-Onboard: Failed - Service-linked role not present"`	No se pudieron habilitar las suscripciones de Linux para una sola cuenta porque no se creó el rol vinculado a servicios correspondiente. Cree el rol e inténtelo de nuevo.
	`"Region": "Account-Onboard: Failed - An internal error occurred"`	La habilitación de las suscripciones de Linux para una sola cuenta no se completó correctamente debido a un error interno.
	`"Region": "Org-Onboard: Failed - Account isn't the management account"`	No se pudieron habilitar las suscripciones de Linux para una organización porque la cuenta que realizaba la operación no era la cuenta de administración de la organización. Inicie sesión en la cuenta de administración e inténtelo de nuevo.

Estado	Motivo del estado	Descripción
	`"Region": "Org-Onboard: Failed - Account isn't part of an organization"`	No se pudieron habilitar las suscripciones de Linux para una organización porque la cuenta que realizaba la operación no pertenecía a una organización. Intente realizar la operación desde una cuenta de la organización, o bien añada esta cuenta a la organización e inténtelo de nuevo.
	`"Region": "Org-Onboard: Failed - Linux subscriptions can't access the organization"`	No se pudieron habilitar las suscripciones de Linux para una organización porque License Manager no tiene permisos para acceder a la organización. Cree el rol vinculado a servicios para suscripciones de Linux e inténtelo de nuevo.

Desactive la detección de suscripciones a Linux

Puede desactivar la detección de suscripciones a Linux desde la página de AWS License Manager configuración. Sin embargo, si ha activado la detección para

> **Warning**
>
> Si deshabilita la detección, se eliminarán todos los datos detectados anteriormente para las suscripciones de Linux AWS License Manager.

Procedimiento para deshabilitar la detección de las suscripciones de Linux

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, elija Configuración.

3. En la página Configuración, seleccione la pestaña Suscripciones de Linux y Deshabilite la detección de suscripciones de Linux.
4. Introduzca **`Disable`** y, a continuación, seleccione Deshabilitar para confirmar la operación.
5. (Opcional) Elimine el rol vinculado a servicios utilizado para las suscripciones de Linux. Para obtener más información, consulte Delete a service-linked role for License Manager.
6. (Opcional) Deshabilite el acceso de confianza entre License Manager y su organización. Para obtener más información, consulte AWS License Manager y AWS Organizations.

Ver los datos de las instancias descubiertas en License Manager

Una vez que License Manager complete el proceso inicial de descubrimiento de recursos en su equipo seleccionado Regiones de AWS, podrá ver los resultados en la consola. Si opta por vincular AWS Organizations, License Manager agrega los datos de las cuentas de toda la organización. Para ver una lista de instancias con suscripciones que cumplen sus criterios de filtrado, vaya a la sección Instancias de la AWS License Manager consola. La lista muestra los siguientes campos clave.

- ID de instancia: el ID de la instancia.
- Estado: el estado de la instancia.
- Tipo de instancia: el tipo de instancia.
- Suscripción: el nombre de la suscripción de licencia que utiliza la instancia.
- Alerta de duplicados: indica que tiene dos suscripciones de licencia diferentes para el mismo software en su instancia.
- ID de cuenta: el ID de la cuenta propietaria de la instancia.
- Región: Región de AWS en la que reside la instancia.
- ID de AMI: el ID de la AMI utilizada para lanzar la instancia.
- Operación de uso: el funcionamiento de la instancia y el código de facturación asociado a la AMI. Para obtener más información, consulte Valores de operación de uso.
- Código de producto: el código del producto asociado a la AMI utilizada para lanzar la instancia. Para obtener más información, consulte Códigos de producto AMI.
- LastUpdatedTime— La hora en la que el último descubrimiento actualizó los detalles de la instancia.

Temas

- Ver los datos de todas las instancias
- Ver los datos de las instancias por suscripción

Ver los datos de todas las instancias

Puede ver y filtrar los datos de suscripción a Linux que License Manager descubrió para las instancias de su cuenta o AWS Organizations de la siguiente manera.

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, en Suscripciones de Linux, seleccione Instancias. Muestra una lista de instancias con datos de suscripción a Linux.
3. (Opcional) Puede usar los siguientes filtros para optimizar los resultados:
   - Cuenta
   - ID de AMI
   - Suscripción duplicada
   - ID de instancia
   - Región
   - Código de producto
   - Operación de uso
4. (Opcional) Seleccione Exportar vista a CSV para exportar los datos de todas sus instancias como un archivo de valores separados por comas (CSV).

Ver los datos de las instancias por suscripción

Puede ver los datos de todas las instancias que se han agregado a todas las cuentas de su organización dentro de las regiones elegidas.

Procedimiento para visualizar los datos detectados para instancias con una suscripción específica

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, en Suscripciones de Linux, seleccione Suscripciones.
3. En la columna Nombre de suscripción, seleccione la suscripción de la que quieres ver los datos.
4. Seleccione la pestaña Instancias y consulte los datos según sea necesario en la consola. Puede filtrar los datos por:

- ID de instancia
- Cuenta
- Región
- ID de AMI
- Operación de uso
- Código de producto

5. (Opcional) Seleccione Exportar vista a CSV para exportar los datos de todas sus instancias con esta suscripción como un archivo de valores separados por comas (CSV).

Información de facturación de las suscripciones de Linux en License Manager

Cada suscripción comercial de Linux que se ejecute en Amazon EC2 tiene información de facturación asociada a la Amazon Machine Image (AMI). Las suscripciones comerciales de Linux incluyen la operación de EC2 uso de Amazon, el código de AWS Marketplace producto o una combinación de ambos. Para obtener más información, consulte Campos de información de facturación de las AMI en la Guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux y los Códigos de producto AMI en la Guía del vendedor de AWS Marketplace .

Nombre de la suscripción	Operación de EC2 uso de Amazon	AWS Marketplace código de producto	Tipo de suscripción
Red Hat Enterprise Linux Server BYOS	RunInstancescódigo de producto ----sep----:00g0	✗	Modelo Bring Your Own Subscription (BYOS)
Red Hat Enterprise Linux Server	RunInstances:00g0 ----sep----:0010	✗	EC2 suscripción incluida
Red Hat Enterprise Linux con complemento de alta disponibilidad	RunInstancessuscripción incluida ----sep----:1010	✗	EC2 suscripción incluida

Nombre de la suscripción	Operación de EC2 uso de Amazon	AWS Marketplace código de producto	Tipo de suscripción
Red Hat Enterprise Linux con SQL Server Standard y alta disponibilidad	RunInstancessuscripción incluida ----sep----:1014	✗	EC2 suscripción incluida
Red Hat Enterprise Linux con SQL Server Enterprise y alta disponibilidad	RunInstancessuscripción incluida ----sep----:1110	✗	EC2 suscripción incluida
Red Hat Enterprise Linux con SQL Server Standard	RunInstancessuscripción incluida ----sep----:0014	✗	EC2 suscripción incluida
Red Hat Enterprise Linux con SQL Server Web	RunInstancessuscripción incluida ----sep----:0210	✗	EC2 suscripción incluida
Red Hat Enterprise Linux con SQL Server Enterprise	RunInstancessuscripción incluida ----sep----:0110	✗	EC2 suscripción incluida
SUSE Linux Enterprise Server	RunInstancessuscripción incluida ----sep----:000g	✗	EC2 suscripción incluida
Red Hat Enterprise Linux para SAP con alta disponibilidad y servicios de actualización	RunInstancessuscripción incluida ----sep----:0010	✓	AWS Marketplace suscripción [1]
SUSE Linux Enterprise Server con SAP	✗	✓	Suscripción AWS Marketplace

Nombre de la suscripción	Operación de EC2 uso de Amazon	AWS Marketplace código de producto	Tipo de suscripción
Ubuntu Pro	RunInstancessuscripción [1] ----sep----:0g00	✓	Suscripción AWS Marketplace
Red Hat Enterprise Linux Workstation	✗	✓	Suscripción AWS Marketplace

[1] Esta suscripción incluye una operación de EC2 uso de Amazon y un código de AWS Marketplace producto.

Métricas de uso para suscripciones de Linux

Las siguientes métricas y dimensiones están disponibles para las suscripciones de Linux:

Métrica	Descripción
RunningInstancesCount	El número total de instancias que se ejecutan en la cuenta corriente y que se agrupan por el nombre de la suscripción, o bien por el nombre de la suscripción y la región. Unidades: recuento Dimensiones: `SubscriptionName` : el nombre de la suscripción. `Region`: la región en la que se detectó el recurso que utilizaba una suscripción comercial de Linux.

Gestione CloudWatch las alarmas de Amazon para las suscripciones de Linux en License Manager

La página de lista de suscripciones de Linux de la consola de License Manager muestra los siguientes detalles clave, incluidas las CloudWatch alarmas de Amazon que configuró para cada suscripción de Linux que License Manager encontró en sus instancias.

- Nombre de la suscripción
- Tipo de suscripción
- Número de instancias en ejecución por suscripción
- CloudWatch Alarmas de Amazon configuradas

Cuando eliges una suscripción a Linux de la página de lista, la pestaña Alarmas y métricas de uso muestra los datos de esa suscripción. En esta pestaña, se muestran los CloudWatch paneles de Amazon para la suscripción elegida en la consola de License Manager. Puede ajustar el panel para que muestre un período de tiempo determinado, o intervalo de evaluación, a horas, días o una semana a partir de una fecha seleccionada.

En la pestaña Alarmas y métricas de uso, cada suscripción tiene una sección de alarmas con los siguientes detalles:

- Nombre de alarma: el nombre de la alarma.
- Estado: el estado de la alarma.
- Dimensión: las dimensiones de la alarma. La dimensión incluirá el tipo de instancia Región de AWS y que se definió.
- Condición: la condición de la alarma. La condición incluirá el operador de comparación y el valor del umbral que se definió para la alarma.

Puede crear CloudWatch alarmas con las dimensiones y condiciones que defina para realizar un seguimiento y emitir alertas en función del uso actual de la suscripción. La consola de suscripciones de Linux muestra un resumen de los nombres de las suscripciones en uso, los tipos de suscripción, la cantidad de instancias en ejecución para cada una y el estado de las alarmas.

Los estados de CloudWatch alarma posibles son los siguientes:

- CORRECTO: la métrica o expresión están dentro del umbral definido.

- ALARMA: la métrica o expresión están fuera del umbral definido.
- DATOS_INSUFICIENTES: la alarma acaba de iniciarse, la métrica no está disponible o no hay suficientes datos de métricas para determinar el estado de la alarma.

Temas

- Cree una CloudWatch alarma para las suscripciones de Linux
- Modifique una CloudWatch alarma para las suscripciones de Linux
- Elimine una CloudWatch alarma para las suscripciones de Linux

Cree una CloudWatch alarma para las suscripciones de Linux

Puede crear alarmas para cada suscripción comercial de Linux que encuentre en sus EC2 instancias en ejecución. Si lo necesita, puede crear varias alarmas con diferentes dimensiones y condiciones para cada suscripción.

Para crear una CloudWatch alarma para las suscripciones de Linux desde la consola

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, en Suscripciones de Linux, seleccione Suscripciones.
3. En la columna Nombre de suscripción, elija la suscripción para la que desee crear una alarma y, a continuación, Crear alarma.
4. Especifique lo siguiente para la alarma:
   - Nombre de alarma: especifique un nombre similar a `AWS-LM-LS-`*`AlarmName`*.
   - Tipo de instancia: elija el tipo de instancia que utilizará la suscripción seleccionada.
   - Región de uso: elija las regiones para las que desea crear las alarmas.
   - Operador de comparación: el operador de comparación del umbral de alarma.
   - Valor del umbral de la alarma: el valor del umbral de la alarma.
5. Seleccione Crear para crear la alarma.

Modifique una CloudWatch alarma para las suscripciones de Linux

Puede modificar las CloudWatch alarmas existentes desde la consola de License Manager para adaptarlas a los requisitos cambiantes.

Para modificar una CloudWatch alarma para las suscripciones de Linux desde la consola

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, en Suscripciones de Linux, seleccione Suscripciones.
3. En la columna Nombre de suscripción, seleccione la suscripción que desee modificar y, a continuación, Editar.
4. Modifique los valores definidos según sea necesario.
5. Seleccione Editar para modificar la alarma.

Elimine una CloudWatch alarma para las suscripciones de Linux

Puede eliminar las CloudWatch alarmas existentes de la consola de License Manager para adaptarlas a los requisitos cambiantes.

Para eliminar una CloudWatch alarma para las suscripciones de Linux de la consola

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, en Suscripciones de Linux, seleccione Suscripciones.
3. En la columna Nombre de suscripción, seleccione la suscripción que desee modificar y, a continuación, Eliminar.

Configuración en License Manager

La sección de configuración de la AWS License Manager consola muestra la configuración de la cuenta corriente. Debe configurar los ajustes para habilitar la funcionalidad asociada.

Managed licenses

Los siguientes ajustes se pueden configurar para las licencias gestionadas:

- Distribución de los derechos gestionados y las licencias autogestionadas a su organización
- Detección de recursos entre cuentas
- Notificación de Amazon SNS

Para obtener más información, consulte Configuración de licencias gestionadas en License Manager.

Linux subscriptions

Las siguientes opciones se pueden configurar para las suscripciones de Linux:

- Descubrimiento y agregación de datos de suscripción a licencias de Linux comercial
- Descubrimiento de suscripciones a Red Hat Subscription Manager (RHSM) para Linux

Para obtener más información, consulte Configuración de suscripción a Linux en License Manager.

User-based subscriptions

Los siguientes ajustes se pueden configurar para las suscripciones basadas en usuarios:

- AWS Managed Microsoft AD
- Virtual Private Cloud (VPC) (Nube virtual privada)

Para obtener más información, consulte Configuración de suscripción basada en el usuario en License Manager.

Delegated administration

Esta pestaña se muestra si su cuenta tiene acceso administrativo a su organización. Como administrador, puede registrar un administrador delegado desde el AWS CLI quirófano AWS Management Console. Para obtener más información, consulte Configuración de administrador delegado en License Manager.

Temas de la configuración

- Editar la configuración de License Manager
- Configuración de licencias gestionadas en License Manager
  - Detalles de cuenta
  - Detección de recursos entre cuentas
  - Simple Notification Service (SNS)
- Configuración de suscripción a Linux en License Manager
  - Configuración de suscripciones de Linux
  - Descubrimiento de Red Hat Subscription Manager
- Configuración de suscripción basada en el usuario en License Manager

- AWS Managed Microsoft AD
- Nube virtual privada
- Configuración de administrador delegado en License Manager
  - Regiones compatibles con los administradores de License Manager delegados
  - Registrar un administrador delegado de License Manager
  - Anular el registro de un administrador de License Manager delegado

Editar la configuración de License Manager

Para editar la configuración de License Manager, siga estos pasos:

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, elija Configuración.
3. Seleccione la pestaña que contiene los ajustes que desee configurar. Por ejemplo, elija Licencias administradas para configurar los detalles de la cuenta.
4. Después de configurar los ajustes, selecciona Guardar o Cancelar para volver atrás.

Configuración de licencias gestionadas en License Manager

Las siguientes configuraciones están disponibles para las licencias administradas.

Detalles de cuenta

Puede revisar los detalles de su cuenta para ver información como el tipo de cuenta, si las cuentas AWS Organizations están vinculadas, el ARN del bucket de License Manager S3 de la cuenta y el AWS Resource Access Manager ARN compartido. Esta sección también le permite vincular sus cuentas. AWS Organizations

Para distribuir los derechos gestionados o las licencias autogestionadas en su organización, elija Vincular cuentas. AWS Organizations Todas las cuentas miembro aceptan automáticamente las concesiones distribuidas para los derechos administrados. Si selecciona esta opción, añadimos un rol vinculado a servicio a las cuentas de administración y miembro.

> **Note**
>
> Para habilitar esta opción, debe haber iniciado sesión en su cuenta de administración y tener todas las características habilitadas en AWS Organizations. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations .
> Esta selección también crea un AWS Resource Access Manager recurso compartido en su cuenta de administración, lo que le permite compartir licencias autogestionadas sin problemas. Para obtener más información, consulte la AWS Resource Access Manager Guía del usuario de .

Para deshabilitar esta opción, llama a la UpdateServiceSettingsAPI.

Detección de recursos entre cuentas

Puede activar la detección de recursos entre cuentas para administrar el uso de las licencias de todas sus cuentas en AWS Organizations.

Para habilitar la detección de recursos entre cuentas en su organización, seleccione Activar para la detección de recursos entre cuentas. Cuando actives la detección de recursos entre cuentas, se AWS Organizations vinculará automáticamente para realizar la detección de recursos en todas tus cuentas.

License Manager utiliza Systems Manager Inventory para detectar el uso del software. Compruebe que ha configurado Systems Manager Inventory en todos los recursos. Para consultar el inventario de Systems Manager Inventory se requiere lo siguiente:

- La sincronización de datos de recursos para almacenar el inventario en un bucket de Amazon S3.
- Amazon Athena para agregar los datos de inventario de sus cuentas de AWS Organizations.
- AWS Glue para proporcionar una experiencia de consulta rápida.

> **Note**
>
> Lo siguiente Regiones de AWS no requiere consultar Amazon Athena ni AWS Glue agregar datos de inventario para que el inventario de Systems Manager detecte el uso del software:
>
> - Asia-Pacífico (Yakarta)

- Israel (Tel Aviv)

Simple Notification Service (SNS)

Puede configurar Amazon SNS para recibir notificaciones y alertas de License Manager.

Procedimiento para configurar un tema de Amazon SNS

1. Seleccione Editar junto a Simple Notification Service (SNS).
2. Especifique el ARN de un tema de SNS con el siguiente formato:

   ```
   arn:<aws_partition>:sns:<region>:<account_id>:aws-license-manager-service-*
   ```
3. Elija Guardar cambios.

Configuración de suscripción a Linux en License Manager

Durante el proceso de descubrimiento, License Manager busca en las EC2 instancias que se ejecutan en sus suscripciones Cuenta de AWS de Linux. Detecta si tiene más de una suscripción de Linux definida para alguna instancia y agrega los datos.

Configuración de suscripciones de Linux

Puede configurar los ajustes de las suscripciones de Linux para controlar la forma en que License Manager gestiona la detección y la agregación. La configuración de detección predeterminada se aplica a todos los tipos de suscripciones de Linux.

Las siguientes acciones están disponibles para configurar la detección de suscripciones de Linux.

Editar

Cambie la configuración de la detección de suscripciones de Linux.

Desactivar

Desactive la detección y la agregación de las suscripciones de Linux asociadas a sus EC2 instancias. Si también tiene activada la detección para Red Hat Subscription Manager, License Manager primero desactiva su proveedor registrado de RHSM y, a continuación, continúa con la desactivación para la detección de suscripciones de Linux.

> **Note**
>
> La desactivación no afecta al secreto de acceso a Red Hat Subscription Manager (RHSM). Para evitar que se le cobre en su AWS factura un secreto asociado que ya no necesita, consulte Eliminar un AWS Secrets Manager secreto en la Guía del AWS Secrets Manager usuario.

La siguiente configuración se muestra en la consola de License Manager para el descubrimiento de suscripciones de Linux.

Configuración de detección de suscripciones de Linux

Descubrimiento de suscripciones a Linux

Indica si has activado la detección de suscripciones de Linux en tu cuenta.

Origen Regiones de AWS

Regiones de AWS donde desea que License Manager descubra los datos de suscripción.

AWS Organizations

Si lo desea, agregue los datos de suscripción de sus cuentas en AWS Organizations.

Para obtener más información, consulte Gestione las suscripciones de Linux en License Manager.

Descubrimiento de Red Hat Subscription Manager

Si ha activado la detección de suscripciones de Linux, puede configurar el acceso para que License Manager recupere datos adicionales de las suscripciones de RHEL que se administran a través de Red Hat Subscription Manager (RHSM).

Las siguientes acciones están disponibles para configurar la detección de suscripciones a RHSM.

Edite las etiquetas

Cambia las etiquetas asociadas a tu secreto de acceso.

> **Note**
>
> Si necesita realizar otros cambios en su suscripción a RHSM, primero debe desactivar su registro actual y, a continuación, configurar uno nuevo.

Desactivar

Desactive su proveedor registrado de RHSM.

> **Note**
>
> La desactivación no afecta a su secreto de acceso a Red Hat Subscription Manager (RHSM). Para evitar que se le cobre en su AWS factura un secreto asociado que ya no necesita, consulte Eliminar un AWS Secrets Manager secreto en la Guía del AWS Secrets Manager usuario.

La siguiente configuración se muestra en la consola de License Manager para la detección de RHSM.

Configuración de detección de Red Hat Subscription Manager

Estado de descubrimiento

Indica si ha activado la detección para las suscripciones a RHSM.

Nombre secreto

Se vincula al secreto de acceso al RHSM AWS Secrets Manager que contiene su token offline de Red Hat. License Manager utiliza este secreto para generar un nuevo token de acceso temporal para solicitar los datos de suscripción de Red Hat Subscription Manager (RHSM).

Puedes realizar cambios en un secreto existente a través de Secrets Manager. Para actualizar las etiquetas u otros metadatos de tu secreto, consulta Modificar un AWS Secrets Manager secreto en la Guía del AWS Secrets Manager usuario. Para actualizar el valor secreto, consulte Actualizar el valor de un AWS Secrets Manager secreto.

Últimos datos sincronizados el

La marca de tiempo de la última actualización correcta de los datos de suscripción de la cuenta registrada de Red Hat Subscription Manager (RHSM).

Etiquetas

Puede definir pares de valores clave para las etiquetas que License Manager asigna a su secreto de acceso RHSM en Secrets Manager. Para recuperar y descifrar su secreto de acceso a RHSM, la política de roles vinculados al servicio de License Manager exige que el secreto y todos los que estén asociados tengan AWS KMS key asignada la siguiente etiqueta:

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

La etiqueta se asigna automáticamente si License Manager creó su secreto durante el proceso de registro. Si crea su propio secreto para el token sin conexión, asegúrese de asignar esa etiqueta al secreto y a la clave KMS asociada, si está cifrada. Para añadir la etiqueta, consulta Modificar un AWS Secrets Manager secreto en la Guía del AWS Secrets Manager usuario.

Configuración de suscripción basada en el usuario en License Manager

Las siguientes configuraciones están disponibles en función de los productos que necesite para las suscripciones basadas en usuarios.

AWS Managed Microsoft AD

Es necesario configurar License Manager AWS Managed Microsoft AD para poder trabajar con suscripciones basadas en usuarios. Para obtener más información, consulte Utilice las suscripciones basadas en usuarios de License Manager para los productos de software compatibles.

Nube virtual privada

License Manager requiere que su VPC esté configurada, además de la suya AWS Managed Microsoft AD, cuando utilice suscripciones basadas en usuarios con Microsoft Office. Para obtener más información, consulte Utilice las suscripciones basadas en usuarios de License Manager para los productos de software compatibles.

Configuración de administrador delegado en License Manager

Puede registrar a un administrador delegado para que se encargue de las licencias administradas y las suscripciones de Linux en License Manager. Para simplificar la administración, recomendamos utilizar la consola License Manager para registrar un único administrador delegado para cada característica de License Manager. Cuando utilice este enfoque, tendrá un único administrador delegado en su organización para License Manager.

Con AWS CLI o SDKs, puede registrar diferentes cuentas de miembros en su organización como administrador delegado para cada función compatible de License Manager. Esto permite que diferentes cuentas miembro de su organización puedan realizar tareas administrativas para las licencias administradas y las suscripciones de Linux.

> **Important**
>
> Para utilizar las características de administración delegada de la consola License Manager, debe tener la misma cuenta miembro registrada como administrador delegado para cada característica de License Manager. Si ha registrado más de una cuenta miembro como administrador delegado, primero debe anular el registro de las cuentas miembro existentes y, a continuación, registrar la misma cuenta para cada característica de License Manager.

Antes de registrar a un administrador delegado, debe habilitar el acceso de confianza con Organizations. Para obtener más información, consulte Invitar a una AWS cuenta a unirse a su organización y Habilitar el acceso confiable con AWS Organizations.

Las siguientes son las características para las que puede registrar un administrador delegado:

Licencias administradas

Puede realizar tareas administrativas, como compartir las licencias autoadministradas con otras cuentas miembro, detectar recursos entre cuentas y distribuir derechos administrados a otras cuentas miembro.

Suscripciones de Linux

Puede realizar tareas administrativas, como ver y administrar las suscripciones comerciales de Linux que posee y que gestiona, Regiones de AWS así como sus cuentas AWS Organizations. También puedes crear y gestionar CloudWatch las alarmas de Amazon para tus suscripciones de Linux. Los

datos primero deben detectarse y agregarse antes de que aparezcan visibles en la consola License Manager y de que cualquier alarma pueda funcionar si se ha configurado.

> **Important**
>
> Una vez registrado, el administrador delegado podrá ver las EC2 instancias que son propiedad de las cuentas de su organización.

Puede registrar y anular el registro de los administradores delegados mediante la AWS License Manager consola, o. AWS CLIAWS SDKs

Regiones compatibles con los administradores de License Manager delegados

Las siguientes regiones admiten administradores delegados de License Manager:

- Este de EE. UU. (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Asia-Pacífico (Hong Kong)
- Medio Oriente (Baréin)
- Canadá (centro)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Londres)
- Europa (París)
- Europa (Estocolmo)

- Europa (Milán)
- África (Ciudad del Cabo)
- América del Sur (São Paulo)

Registrar un administrador delegado de License Manager

Puede registrar un administrador delegado mediante o. AWS CLI AWS Management Console

Console

Para registrar un administrador delegado mediante la AWS License Manager consola, lleve a cabo los siguientes pasos:

1. Inicie sesión AWS como administrador de la cuenta de administración.
2. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
3. En el panel de navegación izquierdo, seleccione Configuración.
4. Seleccione la pestaña Administración delegada.
5. Elija Registrar administrador delegado.
6. Introduzca el ID de la cuenta miembro para registrarla como administrador delegado, confirme que desea conceder a License Manager los permisos necesarios y, a continuación, seleccione Registrarse.
7. Un mensaje indica si la cuenta especificada se ha registrado correctamente como administrador delegado de License Manager.

AWS CLI

Para registrar un administrador delegado para las licencias gestionadas mediante el AWS CLI, lleve a cabo los siguientes pasos:

1. Desde la línea de comandos, ejecute el siguiente AWS CLI comando:

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

2. Ejecute el siguiente comando para comprobar que la cuenta especificada se registra correctamente como administrador delegado:

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

Para registrar un administrador delegado para las suscripciones de Linux mediante el AWS CLI, lleve a cabo los siguientes pasos:

1. Desde la línea de comandos, ejecute el siguiente AWS CLI comando:

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

2. Ejecute el siguiente comando para comprobar que la cuenta especificada se registra correctamente como administrador delegado:

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

Anular el registro de un administrador de License Manager delegado

Puede anular el registro de un administrador delegado mediante la tecla o. AWS CLI AWS Management Console

Console

Para anular el registro de un administrador delegado mediante la AWS License Manager consola, lleve a cabo los siguientes pasos:

1. Inicie sesión AWS como administrador de la cuenta de administración.
2. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
3. En el panel de navegación izquierdo, seleccione Configuración.
4. Seleccione la pestaña Administración delegada.
5. Elija Eliminar.
6. Introduzca el texto **`remove`** para confirmar que desea eliminar al administrador delegado de License Manager y seleccione Eliminar.
7. Un mensaje indica si se ha eliminado correctamente el registro de la cuenta especificada como administrador delegado de License Manager.

AWS CLI

Para anular el registro de un administrador delegado para las licencias gestionadas mediante el AWS CLI, lleve a cabo los siguientes pasos:

1. Desde la línea de comandos, ejecute el siguiente comando: AWS CLI

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

2. Ejecute el siguiente comando para comprobar que se ha anulado correctamente el registro de la cuenta especificada como administrador delegado.

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

Para anular el registro de un administrador delegado para las suscripciones de Linux mediante el AWS CLI, lleve a cabo los siguientes pasos:

1. Desde la línea de comandos, ejecute el siguiente comando: AWS CLI

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

2. Ejecute el siguiente comando para comprobar que se ha anulado correctamente el registro de la cuenta especificada como administrador delegado.

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

Puede volver a registrar o anular una cuenta en cualquier momento.

Panel de control en License Manager

La sección Panel de control de la consola de License Manager proporciona detalles de uso que puede utilizar para realizar un seguimiento del consumo de licencias asociado a lo siguiente:

- Licencias autoadministradas
- Derechos de licencia concedidos
- Usuarios suscritos a suscripciones basadas en usuarios
- Instancias en ejecución

El panel también muestra alertas cuando se producen infracciones de las reglas de licencias.

Descripción general

La sección de información general proporciona los siguientes detalles sobre sus licencias:

Licencias concedidas

El número total de licencias concedidas en esta cuenta y en esta región.

Licencias autoadministradas

El número total de licencias autoadministradas en esta cuenta y en esta región.

Licencias emitidas por el vendedor

El número total de licencias emitidas por el vendedor en esta cuenta y en esta región.

Productos

La sección de productos proporciona los siguientes detalles para las suscripciones basadas en usuarios.

Nombre del producto

El nombre del producto de la suscripción basada en usuarios.

Usuarios suscritos

La cantidad de usuarios suscritos al producto.

Derechos de licencia concedidos

La sección de derechos de licencia concedidos proporciona los siguientes detalles.

Nombre del producto

El nombre del producto de la licencia concedida.

Concesión de derechos

El nombre del derecho.

Uso

El uso del derecho.

Licencias autoadministradas

La sección de licencias autoadministradas proporciona los siguientes detalles.

Nombre de la licencia

El nombre de la licencia autoadministrada.

Concesión de derechos

El nombre del derecho.

Uso

El uso del derecho.

Uso de instancia

La sección de uso de instancia proporciona los siguientes detalles.

Recuento de instancias en ejecución

La cantidad total de instancias en ejecución en esta cuenta y en esta región.

Recuento agregado de instancias en ejecución

La cantidad total de instancias en ejecución agregadas a todas sus cuentas de AWS Organizations en esta región. Este gráfico solo es visible desde la cuenta de administración y desde la cuenta de administrador delegado.

Monitoreo de License Manager

Puedes monitorizar el uso de las licencias y suscripciones rastreadas a AWS License Manager través de Amazon CloudWatch. CloudWatch recopila datos sin procesar y los procesa para convertirlos en métricas legibles y prácticamente en tiempo real. Puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se alcancen dichos umbrales. Para obtener más información, consulte Supervisión del uso de licencias de License Manager con Amazon CloudWatch.

Puede capturar las llamadas a la API y los eventos relacionados realizados por su usuario o en su Cuenta de AWS nombre AWS CloudTrail. Los eventos se capturan como archivos de registros y se distribuyen a un bucket de Amazon S3 especificado. Puedes identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte Registro de llamadas a la AWS License Manager API mediante AWS CloudTrail.

Contenido

- Supervisión del uso de licencias de License Manager con Amazon CloudWatch
  - Creación de alarmas para supervisar las métricas de License Manager
- Registro de llamadas a la AWS License Manager API mediante AWS CloudTrail
  - Información sobre License Manager en CloudTrail
  - Descripción de las entradas del archivo de registros de License Manager

Supervisión del uso de licencias de License Manager con Amazon CloudWatch

Puede supervisar las estadísticas de las métricas de License Manager a través de Amazon CloudWatch. Estas estadísticas se mantienen durante 15 meses, de forma que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio. Puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se alcancen dichos umbrales. Por ejemplo, puede comprobar el porcentaje de licencias que utilizan la métrica `LicenseConfigurationUsagePercentage` y tomar medidas antes de que se superen los límites. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

License Manager emite las siguientes métricas cada hora en el espacio de nombres `AWSLicenseManager/licenseUsage`:

Métrica	Descripción
RunningInstancesCount	El número total de instancias que se ejecutan en la cuenta corriente y que se agrupan por el nombre de la suscripción. Unidades: recuento Dimensiones: `SubscriptionName` : el nombre de la suscripción.
AggregateRunningInstancesCount	El número total agregado de instancias que se están ejecutando en todas tus cuentas de AWS Organizations en la Región de AWS actual. Unidades: recuento Dimensiones: `SubscriptionName` : el nombre de la suscripción.
TotalLicenseConfigurationUsageCount	El número total de una configuración de licencia que podría estar disponible. Unidades: recuento Dimensiones: • `LicenseConfigurationArn` : el nombre de recurso de Amazon (ARN) de la configuración de la licencia. • `LicenseConfigurationType` : el tipo de configuraciones de licencias.
LicenseConfigurationUsageCount	El número total de licencias utilizadas de esta configuración. Unidades: recuento Dimensiones:

Métrica	Descripción
	• `LicenseConfigurationArn` : el ARN de la configuración de licencia. • `LicenseConfigurationType` : el tipo de configuraciones de licencias.
LicenseConfigurationUsagePercentage	Las licencias utilizadas de esta configuración de licencia expresadas como porcentaje. Unidad: porcentaje Dimensiones: • `LicenseConfigurationArn` : el ARN de la configuración de licencia. • `LicenseConfigurationType` : el tipo de configuraciones de licencias.

Creación de alarmas para supervisar las métricas de License Manager

Puede crear una CloudWatch alarma que envíe un mensaje de Amazon Simple Notification Service (Amazon SNS) cuando el valor de la métrica cambie y la alarma cambie de estado. Una alarma vigila una métrica durante el periodo especificado y realiza acciones en función del valor de la métrica relativo a un determinado umbral durante una serie de periodos de tiempo. Las alarmas invocan acciones únicamente para los cambios de estado prolongados. Las alarmas de CloudWatch no invocan acciones simplemente por tener un estado determinado. Es necesario que el estado haya cambiado y se mantenga durante un número especificado de períodos. Para obtener más información, consulte Uso de CloudWatch alarmas.

Registro de llamadas a la AWS License Manager API mediante AWS CloudTrail

AWS License Manager está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en License Manager. CloudTrail captura todas las llamadas a la API de License Manager como eventos. Las llamadas que se capturan incluyen llamadas desde la consola License Manager y llamadas de código a las

operaciones de la API de License Manager. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de License Manager. Si no configura una ruta, podrá ver los eventos más recientes de la CloudTrail consola en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a License Manager, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Temas

- Información sobre License Manager en CloudTrail
- Descripción de las entradas del archivo de registros de License Manager

Información sobre License Manager en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en License Manager, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos en su Cuenta de AWS entorno, incluidos los eventos de License Manager, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de License Manager se registran CloudTrail y se documentan en la Referencia de la AWS License Manager API. Por ejemplo, las llamadas a las llamadas a las `CreateLicenseConfiguration` `DeleteLicenseConfiguration` acciones `ListResourceInventory` y las llamadas generan entradas en los archivos de CloudTrail registro.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas del archivo de registros de License Manager

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `DeleteLicenseConfiguration` acción.

```
{
   "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"
}
```

Seguridad en License Manager

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a License Manager, consulte AWS Services in Scope by Compliance Program AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables

Esta documentación le permite comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza License Manager. Le mostrará cómo configurar License Manager para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos de License Manager.

Contenido

- Protección de datos en License Manager
- Gestión de identidad y acceso para License Manager
- Uso de funciones vinculadas a servicios para License Manager
- AWS políticas gestionadas para License Manager
- Firma criptográfica de licencias en License Manager
- Validación de conformidad para License Manager
- Resiliencia en License Manager
- Seguridad de la infraestructura en License Manager
- License Manager e interfaz de puntos finales de VPC con AWS PrivateLink

Protección de datos en License Manager

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS License Manager. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con License Manager u otro

Servicios de AWS mediante la consola, la API o AWS SDKs. AWS CLI Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

License Manager guarda datos en un bucket de Amazon S3 en la cuenta de administración. El bucket se configura con claves de cifrado administradas por Amazon S3 (SSE-S3).

Gestión de identidad y acceso para License Manager

AWS Identity and Access Management (IAM) es un AWS servicio que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Con IAM, puede crear usuarios y grupos en su cuenta. AWS Usted controla los permisos que tienen los usuarios para realizar tareas utilizando AWS los recursos. El uso de IAM no está sujeto a ningún cargo adicional.

De forma predeterminada, los usuarios no tienen permisos para los recursos y las operaciones de License Manager. Para permitir a los usuarios administrar recursos de License Manager, se crea una política de IAM que les concede permisos explícitamente.

Cuando se asocia una política a un usuario o grupo de usuarios, les otorga o deniega el permiso para realizar las tareas especificadas en los recursos indicados. Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

Creación de usuarios, grupos y roles

Puede crear usuarios y grupos para usted Cuenta de AWS y, a continuación, asignarles los permisos que necesiten. Como práctica recomendada, los usuarios deben adquirir los permisos al asumir roles de IAM. Para obtener más información sobre cómo configurar usuarios y grupos para su Cuenta de AWS, consulte Comience a utilizar License Manager.

Un rol de IAM es una identidad de IAM que puede crear en su cuenta y que tiene permisos específicos. Una función de IAM es similar a la de un usuario de IAM en el sentido de que es una AWS identidad con políticas de permisos que determinan lo que la identidad puede y no puede hacer

en ella. AWS No obstante, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Además, un rol no tiene asociadas credenciales a largo plazo estándar, como una contraseña o claves de acceso. En su lugar, cuando se asume un rol, este proporciona credenciales de seguridad temporales para la sesión de rol.

Estructura de la política de IAM

Una política de IAM es un documento JSON que contiene una o varias instrucciones. Cada instrucción tiene la estructura siguiente.

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

Una instrucción está compuesta por varios elementos:

- Effect: el valor de effect puede ser `Allow` o `Deny`. De forma predeterminada, los usuarios no tienen permiso para utilizar los recursos y las operaciones de API; y se deniegan todas las solicitudes. La concesión (allow) de un permiso explícito anula el valor predeterminado. Una denegación explícita (deny) anula cualquier permiso concedido.
- Action: el valor de action es la operación de la API para la que concede o deniega permisos.
- Resource: el recurso al que afecta la acción. Algunas operaciones de la API de License Manager permiten incluir en la política recursos específicos que la operación puede crear o modificar. Para especificar un recurso en la instrucción, debe usar el nombre de recurso de Amazon (ARN). Para obtener más información, consulte Acciones definidas por. AWS License Manager
- Condition: las condiciones son opcionales. Se pueden usar para controlar cuándo está en vigor la política. Para obtener más información, consulte Claves de condición para AWS License Manager.

Cree políticas de IAM para License Manager

En una instrucción de política de IAM puede especificar cualquier operación de API de cualquier servicio que sea compatible con IAM. License Manager usa los siguientes prefijos con el nombre de la operación de API:

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

Por ejemplo:

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

Para obtener más información sobre el License Manager disponible APIs, consulte las siguientes referencias de API:

- AWS License Manager Referencia de la API
- AWS License Manager Referencia de la API de suscripciones de usuarios
- AWS License Manager Referencia de la API de suscripciones de Linux

Para especificar varias operaciones en una única instrucción, sepárelas con comas del siguiente modo:

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

También puede utilizar caracteres comodín para especificar varias operaciones. Por ejemplo, puede especificar todas las operaciones de la API de License Manager cuyo nombre comience por la palabra List del siguiente modo:

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

Para especificar todas las operaciones de la API de License Manager, use el carácter comodín * del siguiente modo:

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

Ejemplo de política para un ISV con License Manager

ISVs que distribuyen licencias a través de License Manager requieren los siguientes permisos:

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

Concesión de permisos a usuarios, grupos y roles

Una vez creadas las políticas de IAM necesarias, tendrá que conceder estos permisos a los usuarios, grupos y roles.

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .

- Usuarios gestionados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Uso de funciones vinculadas a servicios para License Manager

AWS License Manager utiliza funciones vinculadas al AWS Identity and Access Management servicio (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a License Manager. Las funciones vinculadas al servicio están predefinidas por License Manager e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado al servicio simplifica la configuración de License Manager porque ya no tendrá que agregar manualmente los permisos requeridos. License Manager define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo License Manager puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar los recursos relacionados. De esta forma se protegen los recursos de License Manager, ya que evita que se puedan quitar accidentalmente permisos de acceso a los recursos.

Las acciones de License Manager dependen de tres roles vinculados al servicio, que se describe en las secciones siguientes.

Roles vinculados a servicios

- License Manager: rol principal
- License Manager: rol de cuenta de administración
- License Manager: rol de cuenta miembro
- License Manager: rol de suscripciones basadas en usuarios

- License Manager: rol de suscripciones de Linux

License Manager: rol principal

License Manager requiere un rol vinculado a servicios para administrar las licencias por usted.

Permisos del rol principal

El rol vinculado al servicio denominado `AWSServiceRoleForAWSLicenseManagerRole` permite que License Manager acceda a AWS los recursos para administrar las licencias en su nombre.

El rol vinculado a servicios `AWSServiceRoleForAWSLicenseManagerRole` confía en el servicio `license-manager.amazonaws.com` para asumir el rol.

Para revisar los permisos de AWSLicenseManagerServiceRolePolicy, consulteAWS política gestionada: AWSLicenseManagerServiceRolePolicy. Para obtener más información sobre cómo configurar los permisos para un rol vinculado a servicios, consulte Permisos de rol vinculado a servicios en la Guía del usuario de IAM.

Cree un rol vinculado a servicios para License Manager

No necesita crear manualmente un rol vinculado a servicios. Cuando rellene el formulario de la experiencia de primer uso de License Manager la primera vez que visite la consola License Manager, el rol vinculado a servicios se creará automáticamente.

También puede utilizar la consola de IAM o la API de IAM para crear manualmente un rol vinculado a un servicio. AWS CLI Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Además, si utilizaba License Manager antes del 1 de enero de 2017, cuando comenzó a admitir los roles vinculados a servicios, License Manager creó el rol `AWSServiceRoleForAWSLicenseManagerRole` en su cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en la cuenta de IAM.

Puede utilizar la consola License Manager para crear un rol vinculado a servicios.

Para crear el rol vinculado al servicio de

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Seleccione Comenzar a usar AWS License Manager.
3. En el formulario Permisos de IAM (one-time-setup), seleccione Otorgo AWS License Manager los permisos necesarios y, a continuación, elija Continuar.

También puede utilizar la consola IAM para crear un rol vinculado a servicios con el caso de uso de License Manager. Como alternativa, en la API AWS CLI o en la AWS API, usa IAM para crear un rol vinculado a un servicio con el nombre del servicio. `license-manager.amazonaws.com` Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM.

Si elimina este rol vinculado a servicios, puede utilizar el mismo proceso de IAM para volver a crear el rol.

Edite un rol vinculado a servicios para License Manager

License Manager no le permite modificar el rol vinculado a servicios `AWSServiceRoleForAWSLicenseManagerRole`. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Elimine un rol vinculado a servicios para License Manager

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, solo dispondrá de entidades que se monitorizan o mantienen de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpie un rol vinculado a servicios

Para poder utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar todos los recursos que utiliza el rol. Esto significa disociar las licencias autogestionadas de las instancias asociadas y AMIs, a continuación, eliminar las licencias autogestionadas.

> **Note**
>
> Si License Manager está utilizando el rol cuando se intentan eliminar los recursos, es posible que se produzcan errores en la operación de eliminación. Si eso sucede, espere unos minutos e inténtelo de nuevo.

Procedimiento para eliminar los recursos de License Manager que utilizan los roles vinculados a servicios

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación, seleccione Licencias autoadministradas.
3. Elija una licencia autogestionada de la que sea propietario y desasocie todas las entradas de las pestañas Asociadas AMIs y Recursos. Repita este proceso para la configuración de cada licencia.
4. En la página de la licencia autoadministrada, seleccione Acciones y, a continuación, Eliminar.
5. Repita los pasos anteriores hasta que se hayan eliminado todas las licencias autoadministradas.

Elimine manualmente el rol vinculado a servicios

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al `AWSServiceRoleForAWSLicenseManagerRole` servicio. Si también está utilizando AWSServiceRoleForAWSLicenseManagerMasterAccountRoley AWSLicenseManagerMemberAccountRole, primero elimine esos roles. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

License Manager: rol de cuenta de administración

License Manager requiere un rol vinculado a servicios para administrar las licencias.

Permisos para el rol de cuenta de administración

El rol vinculado al servicio denominado `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` permite que License Manager acceda a AWS los recursos para gestionar las acciones de administración de licencias de una cuenta de administración central en su nombre.

El rol vinculado a servicios `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` confía en el servicio `license-manager.master-account.amazonaws.com` para asumir el rol.

Para revisar los permisos de AWSLicenseManagerMasterAccountRolePolicy, consulteAWS política gestionada: AWSLicenseManagerMasterAccountRolePolicy. Para obtener más información sobre cómo configurar los permisos para un rol vinculado a servicios, consulte Permisos de rol vinculado a servicios en la Guía del usuario de IAM.

Cree un rol de cuenta de administración vinculado a servicios

No es necesario crear manualmente este rol vinculado a servicios. Al configurar la administración de licencias multicuenta en AWS Management Console, License Manager crea el rol vinculado al servicio automáticamente.

> **Note**
>
> Para utilizar el soporte multicuenta en License Manager, debe utilizar AWS Organizations.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta.

También puede usar la consola de IAM o la API de IAM para crear manualmente un rol vinculado a un servicio. AWS CLI Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Además, si utilizaba License Manager antes del 1 de enero de 2017, cuando comenzó a admitir los roles vinculados a servicios, License Manager creó `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` en su cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en la cuenta de IAM.

Puede utilizar la consola License Manager para crear este rol vinculado a servicios.

Para crear el rol vinculado al servicio de

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. Elija Configuración, Editar.
3. Seleccione Vincular AWS Organizations cuentas.
4. Seleccione Aplicar.

También puede utilizar la consola IAM para crear un rol vinculado a servicios con el caso de uso de cuenta de administración de License Manager. Como alternativa, en la API AWS CLI o en la AWS API, usa IAM para crear un rol vinculado a un servicio con el nombre del `license-manager.master-account.amazonaws.com` servicio. Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM.

Si elimina este rol vinculado a servicios, puede utilizar el mismo proceso de IAM para volver a crear el rol.

Edite un rol vinculado a servicios para License Manager

License Manager no le permite modificar el rol vinculado a servicios `AWSServiceRoleForAWSLicenseManagerMasterAccountRole`. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Elimine un rol vinculado a servicios para License Manager

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, solo dispondrá de entidades que se monitorizan o mantienen de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Eliminación manual de un rol vinculado a servicios

Utilice la consola de IAM o la AWS API para eliminar el rol vinculado al servicio. AWS CLI`AWSServiceRoleForAWSLicenseManagerMasterAccountRole` Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

License Manager: rol de cuenta miembro

License Manager requiere un rol vinculado a servicios que permita a la cuenta de administración administrar las licencias.

Permisos para el rol de cuenta miembro

El rol vinculado al servicio denominado `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` permite a License Manager acceder a AWS los recursos para realizar acciones de administración de licencias desde una cuenta de administración configurada en su nombre.

El rol vinculado a servicios `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` confía en el servicio `license-manager.member-account.amazonaws.com` para asumir el rol.

Para revisar los permisos de AWSLicenseManagerMemberAccountRolePolicy, consulteAWS política gestionada: AWSLicenseManagerMemberAccountRolePolicy. Para obtener más información sobre cómo configurar los permisos para un rol vinculado a servicios, consulte Permisos de rol vinculado a servicios en la Guía del usuario de IAM.

Cree el rol vinculado a servicios para License Manager

No necesita crear manualmente el rol vinculado a servicios. Puede habilitar la integración AWS Organizations desde la cuenta de administración de la consola de License Manager en la página de configuración. También puede hacerlo mediante la AWS CLI (ejecuciónupdate-service-settings) o la AWS API (llamadaUpdateServiceSettings). Cuando lo haga, License Manager creará el rol vinculado a servicios por usted en las cuentas miembro de Organizations.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta.

También puedes usar la consola de IAM o la AWS API para crear un rol vinculado a un servicio de forma manual. AWS CLI Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Además, si utilizaba el servicio License Manager antes del 1 de enero de 2017,

cuando comenzó a admitir los roles vinculados a servicios, License Manager creó el rol `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` en su cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en la cuenta de IAM.

Puede utilizar la consola License Manager para crear un rol vinculado a servicios.

Para crear el rol vinculado al servicio de

1. Inicie sesión en su cuenta de administración. AWS Organizations
2. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
3. En el panel de navegación izquierdo, elija Configuración y Básica.
4. Seleccione Vincular AWS Organizations cuentas.
5. Seleccione Aplicar. Esto crea los roles AWSServiceRoleForAWSLicenseManagerRole y AWSServiceRoleForAWSLicenseManagerMemberAccountRoleen todas las cuentas secundarias.

También puede utilizar la consola IAM para crear un rol vinculado a servicios con el caso de uso `License Manager - Member account`. Como alternativa, en la AWS API AWS CLI o, cree un rol vinculado al servicio con el nombre del `license-manager.member-account.amazonaws.com` servicio. Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM.

Si elimina este rol vinculado a servicios, puede utilizar el mismo proceso de IAM para volver a crear el rol.

Edite un rol vinculado a servicios para License Manager

License Manager no le permite modificar el rol vinculado a servicios `AWSServiceRoleForAWSLicenseManagerMemberAccountRole`. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Elimine un rol vinculado a servicios para License Manager

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, solo dispondrá de entidades que se monitorizan

o mantienen de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Eliminación manual de un rol vinculado a servicios

Utilice la consola de IAM o la AWS API para eliminar el `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` rol vinculado al servicio. AWS CLI Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

License Manager: rol de suscripciones basadas en usuarios

License Manager requiere una función vinculada a un servicio para administrar AWS los recursos que proporcionarán suscripciones basadas en los usuarios.

Permisos para el rol de suscripciones basadas en usuarios

El rol vinculado al servicio denominado `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` permite a License Manager utilizar AWS Systems Manager y gestionar EC2 los recursos de Amazon que proporcionan suscripciones basadas en los usuarios, así como describir los recursos. AWS Directory Service

Para revisar los permisos de AWSLicenseManagerUserSubscriptionsServiceRolePolicy, consulteAWS política gestionada: AWSLicenseManagerUserSubscriptionsServiceRolePolicy. Para obtener más información sobre cómo configurar los permisos para un rol vinculado a servicios, consulte Permisos de rol vinculado a servicios en la Guía del usuario de IAM.

Cree el rol vinculado a servicios para License Manager

No necesita crear manualmente el rol vinculado a servicios, ya que se le solicitará crear el rol en las páginas de Suscripciones basadas en usuarios de la consola License Manager.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta.

También puede utilizar la consola de IAM o la API de IAM para crear manualmente un rol vinculado a un servicio. AWS CLI Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM.

Puede utilizar la consola License Manager para crear un rol vinculado a servicios.

Para crear el rol vinculado al servicio de

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.
2. En el panel de navegación izquierdo, seleccione Asociación de usuarios o Productos.
3. Acepte las condiciones de License Manager para crear el rol de suscripciones basadas en usuarios.
4. Seleccione Crear. Así, se creará el rol.

También puede utilizar la consola IAM para crear un rol vinculado a servicios con el caso de uso `License Manager - User-based subscriptions`. Como alternativa, en la AWS API AWS CLI o API, cree un rol vinculado a un servicio con el nombre del `license-manager-user-subscriptions.amazonaws.com` servicio. Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM.

Si elimina este rol vinculado a servicios, puede utilizar el mismo proceso de IAM para volver a crear el rol.

Edite un rol vinculado a servicios para License Manager

License Manager no le permite modificar el rol vinculado a servicios `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService`. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Elimine un rol vinculado a servicios para License Manager

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, solo dispondrá de entidades que se monitorizan o mantienen de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Eliminación manual de un rol vinculado a servicios

Utilice la consola de IAM o la AWS API para eliminar el `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` rol vinculado al servicio. AWS CLI Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

License Manager: rol de suscripciones de Linux

License Manager requiere una función vinculada a un servicio para administrar AWS los recursos que proporcionan suscripciones de Linux.

Permisos para el rol de suscripciones de Linux

El rol vinculado al servicio denominado `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` permite a License Manager realizar las siguientes acciones para las suscripciones de Linux.

- Descubra Amazon Elastic Compute Cloud y AWS Organizations sus recursos.
- Obtenga información confidencial etiquetada con AWS Secrets Manager para acceder a proveedores `"LicenseManagerLinuxSubscriptions": "enabled"` de suscripciones de Linux de terceros y obtener información sobre las suscripciones.
- Utilice las claves de KMS etiquetadas con `"LicenseManagerLinuxSubscriptions": "enabled"` esta etiqueta para descifrar los secretos.

Para revisar los permisos del AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy, consulteAWS política gestionada: AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy. Para obtener más información sobre cómo configurar los permisos para un rol vinculado a servicios, consulte Permisos de rol vinculado a servicios en la Guía del usuario de IAM.

Cree el rol vinculado a servicios para License Manager

No necesita crear manualmente el rol vinculado a servicios, ya que se le solicitará crear el rol en las páginas de Suscripciones de Linux de la consola License Manager.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta.

También puede utilizar la consola de IAM o la API de IAM para crear manualmente un rol vinculado a un servicio. AWS CLI Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM.

Puede utilizar la consola License Manager para crear un rol vinculado a servicios.

Para crear el rol vinculado al servicio de

1. Abra la consola de License Manager en https://console.aws.amazon.com/license-manager/.

2. En el panel de navegación izquierdo, seleccione Suscripciones o Instancias.
3. Acepte las condiciones de License Manager para crear el rol de suscripciones de Linux.
4. Seleccione Crear. Así, se creará el rol.

También puede utilizar la consola IAM para crear un rol vinculado a servicios con el caso de uso `License Manager - Linux subscriptions`. Como alternativa, en la AWS API AWS CLI o API, cree un rol vinculado a un servicio con el nombre del `license-manager-linux-subscriptions.amazonaws.com` servicio. Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM.

Si elimina este rol vinculado a servicios, puede utilizar el mismo proceso de IAM para volver a crear el rol.

Edite un rol vinculado a servicios para License Manager

License Manager no le permite modificar el rol vinculado a servicios `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Elimine un rol vinculado a servicios para License Manager

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, solo dispondrá de entidades que se monitorizan o mantienen de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Eliminación manual de un rol vinculado a servicios

Utilice la consola de IAM o la AWS API para eliminar el `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` rol vinculado al servicio. AWS CLI Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

AWS políticas gestionadas para License Manager

Para añadir permisos a los usuarios, grupos y funciones, es más fácil utilizar políticas AWS gestionadas que escribirlas usted mismo. Se necesita tiempo y experiencia para crear políticas

administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en tu AWS cuenta. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política gestionada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: AWSLicenseManagerServiceRolePolicy

Esta política se asocia al rol vinculado a servicios denominado `AWSServiceRoleForAWSLicenseManagerRole` para permitir a License Manager llamar a las acciones de API con el objetivo de administrar las licencias en su nombre. Para obtener más información sobre el rol vinculado a servicios, consulte Permisos del rol principal.

La política de permisos del rol permite que License Manager realice las siguientes acciones en los recursos especificados.

Acción	ARN de recurso
`iam:CreateServiceLinkedRole`	`arn:aws:iam::*:role/aws-service-role/license-management.marketplace.amazonaws.com`

Acción	ARN de recurso
	/AWSServiceRoleFor MarketplaceLicense Management
iam:CreateServiceLinkedRole	arn:aws:iam::*:role/aws-service-role/license-manager.member-account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:ListAllMyBuckets	*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
sns:Publish	arn:aws::sns:*:*:aws-license-manager-service-*
sns:ListTopics	*
ec2:DescribeInstances	*
ec2:DescribeImages	*
ec2:DescribeHosts	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*

Acción	ARN de recurso
ssm:CreateAssociation	*
organizations:ListAWSServiceAccessForOrganization	*
organizations:DescribeOrganization	*
organizations:ListDelegatedAdministrators	*
license-manager:GetServiceSettings	*
license-manager:GetLicense*	*
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:List*	*

Para ver los permisos de esta política en AWS Management Console, consulte AWSLicenseManagerServiceRolePolicy.

AWS política gestionada: AWSLicenseManagerMasterAccountRolePolicy

Esta política se adjunta a la función vinculada al servicio denominada AWSServiceRoleForAWSLicenseManagerMasterAccountRole para permitir que License Manager llame a las acciones de la API que realizan la administración de licencias para una cuenta de administración central en su nombre. Para obtener más información sobre el rol vinculado a servicios, consulte License Manager: rol de cuenta de administración.

La política de permisos del rol permite que License Manager realice las siguientes acciones en los recursos especificados.

Acción	ARN de recurso
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*

Acción	ARN de recurso
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:GetLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*
s3:PutLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*
s3:GetBucketPolicy	arn:aws:s3:::aws-license-manager-service-*
s3:PutBucketPolicy	arn:aws:s3:::aws-license-manager-service-*
s3:AbortMultipartUpload	arn:aws:s3:::aws-license-manager-service-*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
s3:GetObject	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucketMultipartUploads	arn:aws:s3:::aws-license-manager-service-*
s3:ListMultipartUploadParts	arn:aws:s3:::aws-license-manager-service-*
s3:DeleteObject	arn:aws:s3:::aws-license-manager-service-*/resource-sync/*
athena:GetQueryExecution	*
athena:GetQueryResults	*

Acción	ARN de recurso
athena:StartQueryExecution	*
glue:GetTable	*
glue:GetPartition	*
glue:GetPartitions	*
glue:CreateTable	Véase la nota [1] a pie de página
glue:UpdateTable	Véase la nota [1] a pie de página
glue:DeleteTable	Véase la nota [1] a pie de página
glue:UpdateJob	Véase la nota [1] a pie de página
glue:UpdateCrawler	Véase la nota [1] a pie de página
organizations:DescribeOrganization	*
organizations:ListAccounts	*
organizations:DescribeAccount	*
organizations:ListChildren	*
organizations:ListParents	*
organizations:ListAccountsForParent	*
organizations:ListRoots	*
organizations:ListAWSServiceAccessForOrganization	*
ram:GetResourceShares	*
ram:GetResourceShareAssociations	*
ram:TagResource	*

Acción	ARN de recurso
ram:CreateResourceShare	*
ram:AssociateResourceShare	*
ram:DisassociateResourceShare	*
ram:UpdateResourceShare	*
ram:DeleteResourceShare	*
resource-groups:PutGroupPolicy	*
iam:GetRole	*
iam:PassRole	arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*
cloudformation:UpdateStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:CreateStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:DeleteStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*

Acción	ARN de recurso
`cloudformation:DescribeStacks`	`arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*`

[1] Los siguientes son los recursos definidos para las AWS Glue acciones:

- `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`

Para ver los permisos de esta política en el AWS Management Console, consulte AWSLicenseManagerMasterAccountRolePolicy.

AWS política gestionada: AWSLicenseManagerMemberAccountRolePolicy

Esta política se asocia al rol vinculado a servicios denominado `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` para permitir a License Manager llamar a las acciones de API con el objetivo de administrar las licencias en su nombre desde una cuenta de administración configurada. Para obtener más información, consulte License Manager: rol de cuenta miembro.

La política de permisos del rol permite que License Manager realice las siguientes acciones en los recursos especificados.

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

Para ver los permisos de esta política en AWS Management Console, consulte AWSLicenseManagerMemberAccountRolePolicy.

AWS política gestionada: AWSLicenseManagerConsumptionPolicy

Puede asociar la política `AWSLicenseManagerConsumptionPolicy` a las identidades de IAM. Esta política concede permisos que permiten el acceso a las acciones de la API de License Manager necesarias para consumir licencias. Para obtener más información, consulte Uso de licencias emitidas por el vendedor en License Manager.

Para ver los permisos de esta política, consulte AWSLicenseManagerConsumptionPolicyen el AWS Management Console.

AWS política gestionada: AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Esta política se asocia a la política del rol vinculado a servicios denominado `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` para permitir a License Manager llamar a las acciones de API con el objetivo de administrar recursos de suscripciones basadas en usuarios. Para obtener más información, consulte License Manager: rol de suscripciones basadas en usuarios.

La política de permisos del rol permite que License Manager realice las siguientes acciones en los recursos especificados.

Acción	ARN de recurso
anuncios: DescribeDirectories	*
ds: GetAuthorizedApplicationDetails	*
ec2: CreateTags	arn:aws:ec2:*:*:instance/* [1]
ec2: DescribeInstances	*
ec2: DescribeNetworkInterfaces	*
ec2: DescribeSecurityGroupRules	*
ec2: DescribeSubnets	*
ec2: DescribeVpcPeeringConnections	*
ec2: TerminateInstances	arn:aws:ec2:*:*:instance/* [1]
ruta 53: GetHostedZone	*
ruta 53: ListResourceRecordSets	*
administrador de secretos: GetSecretValue	arn:aws:secretsmanager: *:*:secret: -* license-manager-user
sms: DescribeInstanceInformation	*

Acción	ARN de recurso
ssm: GetCommandInvocation	*
ssm: GetInventory	*
ssm: ListCommandInvocations	*
ssm: SendCommand	arn:aws:ssm: *::document/AWS- ² RunPowerShellScript arn:aws:ec2:*:*:instance/* ²

¹ License Manager solo puede crear etiquetas y terminar instancias que tengan los códigos de producto bz0vcy31ooqlzk5tsash4r1ik, 77yzkpa7kvee1y1tt7wnsdwoc o d44g89hc0gp9jdzm99rznthpw.

² License Manager solo puede ejecutar un comando SSM Run Command con el documento `AWS-RunPowerShellScript` en instancias con el nombre de etiqueta `AWSLicenseManager` y un valor `UserSubscriptions`.

Para ver AWS Management Console los permisos de esta política en el, consulte AWSLicenseManagerUserSubscriptionsServiceRolePolicy.

AWS política gestionada: AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Esta política se asocia a la política del rol vinculado a servicios denominado `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` para permitir a License Manager llamar a las acciones de API con el objetivo de administrar recursos de suscripciones de Linux. Para obtener más información, consulte License Manager: rol de suscripciones de Linux.

La política de permisos del rol permite que License Manager realice las siguientes acciones en los recursos especificados.

Acción	Condiciones	Recurso
`ec2:DescribeInstances`	N/A	*

Acción	Condiciones	Recurso
ec2:DescribeRegions	N/A	*
organizations:DescribeOrganization	N/A	*
organizations:ListAccounts	N/A	*
organizations:DescribeAccount	N/A	*
organizations:ListChildren	N/A	*
organizations:ListParents	N/A	*
organizations:ListAccountsForParent	N/A	*
organizations:ListRoots	N/A	*
organizations:ListAWSServiceAccessForOrganization	N/A	*
organizations:ListDelegatedAdministrators	N/A	*
administrador de secretos: GetSecretValue	StringEquals: «aws:ResourceTag/LicenseManagerLinuxSubscriptions«: «habilitado» «aws: ResourceAccount «: «${aws:PrincipalAccount}»	arn:aws:secretsmanager:*:*:secret:*

Acción	Condiciones	Recurso
kms:Decrypt	StringEquals: «aws:ResourceTag/LicenseManagerLinuxSubscriptions«: «habilitado», «aws: ResourceAccount «: «${aws:PrincipalAccount}» StringLike: «kms: «: [ViaService«secretsmanager.*.amazonaws.com»]	`arn:aws:kms:*:*:key/*`

Para ver los permisos de esta política en el, consulte AWS Management ConsoleAWSLicenseManagerLinuxSubscriptionsServiceRolePolicy.

License Manager actualiza las políticas AWS gestionadas

Vea los detalles sobre las actualizaciones de las políticas AWS administradas de License Manager desde que este servicio comenzó a rastrear estos cambios.

Cambio	Descripción	Fecha
AWSLicenseManagerUserSubscriptionsServiceRolePolicy: actualización de una política actual	License Manager agregó los siguientes permisos para administrar las licencias y los datos de Active Directory : obtener información de rutas de Route 53, obtener información de redes y reglas de grupos de seguridad de Amazon EC2 y obtener secretos de Secrets Manager.	7 de noviembre de 2024

Cambio	Descripción	Fecha
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy: actualización de una política actual	License Manager agregó permisos para almacenar y recuperar secretos y usar AWS KMS claves para descifrar los secretos de AWS Secrets Manager los tokens de acceso para las suscripciones de Bring Your Own License (BYOL).	22 de mayo de 2024
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy: política nueva	License Manager agregó un permiso para crear el rol vinculado a servicios denominado `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` . Esta función proporciona permiso al License Manager para publicar AWS Organizations y publicar EC2 recursos de Amazon.	21 de diciembre de 2022
AWSLicenseManagerUserSubscriptionsServiceRolePolicy: actualización de una política actual	License Manager agregó el permiso `ec2:DescribeVpcPeeringConnections` .	28 de noviembre de 2022

Cambio	Descripción	Fecha
AWSLicenseManagerUserSubscriptionsServiceRolePolicy: política nueva	License Manager agregó un permiso para crear el rol vinculado a servicios denominado `AWSLicenseManagerUserSubscriptionsServiceRolePolicy` . Esta función proporciona permiso al License Manager para enumerar AWS Directory Service los recursos, utilizar las funciones de Systems Manager y gestionar EC2 los recursos de Amazon creados para las suscripciones basadas en usuarios.	18 de julio de 2022
AWSLicenseManagerMasterAccountRolePolicy: actualización de una política actual	License Manager agregó el `resource-groups:PutGroupPolicy` permiso para los grupos de recursos administrados por AWS Resource Access Manager.	27 de junio de 2022
AWSLicenseManagerMasterAccountRolePolicy: actualización de una política actual	License Manager cambió la clave de `AWSLicenseManagerMasterAccountRolePolicy` condición de la política AWS administrada AWS Resource Access Manager de usar `ram:ResourceTag` a `aws:ResourceTag` .	16 de noviembre de 2021

Cambio	Descripción	Fecha
AWSLicenseManagerConsumptionPolicy: política nueva	License Manager agregó una nueva política que concede permisos para consumir licencias.	11 de agosto de 2021
AWSLicenseManagerServiceRolePolicy: actualización de una política actual	License Manager agregó un permiso para enumerar los administradores delegados y un permiso para crear el rol vinculado a servicios denominado `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` .	16 de junio de 2021
AWSLicenseManagerServiceRolePolicy: actualización de una política actual	License Manager agregó un permiso para enumerar todos los recursos de License Manager, como configuraciones de licencias, licencias y concesiones.	15 de junio de 2021

Cambio	Descripción	Fecha
AWSLicenseManagerServiceRolePolicy: actualización de una política actual	License Manager agregó un permiso para crear el rol vinculado a servicios denominado `AWSServiceRoleForMarketplaceLicenseManagement` . Esta función AWS Marketplace proporciona permisos para crear y administrar licencias en License Manager. Para obtener más información, consulte Uso de roles vinculados a servicios en AWS Marketplace en la Guía para comprador de AWS Marketplace .	9 de marzo de 2021
Inicio del seguimiento de los cambios por parte de License Manager	License Manager comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	9 de marzo de 2021

Firma criptográfica de licencias en License Manager

License Manager puede firmar criptográficamente las licencias emitidas por un ISV o a través de ellas AWS Marketplace en nombre de un ISV. La firma permite a los proveedores validar la integridad y el origen de una licencia dentro de la propia aplicación, incluso en un entorno fuera de línea.

Para firmar las licencias, License Manager utiliza una asimétrica AWS KMS key que pertenece a un ISV y está protegida en AWS Key Management Service ()AWS KMS. Esta CMK administrada por el cliente se compone de un par de claves privadas y públicas relacionadas matemáticamente. Cuando un usuario solicita una licencia, License Manager genera un objeto JSON con los derechos de licencia y firma este objeto con la clave privada. La firma y el objeto JSON de texto no cifrado se devuelven al usuario. Cualquier persona a la que se le presenten estos objetos puede utilizar la

clave pública para validar que el texto de la licencia no se ha alterado y que la licencia la ha firmado el propietario de la clave privada. La parte privada del key pair nunca sale AWS KMS. Para obtener más información sobre la criptografía asimétrica en AWS KMS, consulte Uso de claves simétricas y asimétricas.

> **Note**
>
> License Manager llama a las operaciones AWS KMS `Sign`y a la `Verify`API al firmar y verificar las licencias. La CMK debe tener un valor de uso de clave de SIGN_VERIFY para que se pueda utilizar en estas operaciones. Esta variedad de CMK no se puede utilizar para cifrado y descifrado.

El siguiente flujo de trabajo describe la emisión de licencias firmadas criptográficamente:

1. En la AWS KMS consola, la API o el SDK, el administrador de licencias crea una CMK asimétrica gestionada por el cliente. La CMK debe tener un uso de la clave de firma y verificación, y admitir el algoritmo de firma RSASSA-PSS SHA-256. Para obtener más información, consulte Creación de una configuración de CMK asimétrica CMKs y Cómo elegir una configuración de CMK.
2. En License Manager, el administrador de licencias crea una configuración de consumo que incluye un AWS KMS ARN o un ID. La configuración puede especificar la opción Préstamo o Provisional, o bien ambas. Para obtener más información, consulte Cómo crear un bloque de licencias emitidas por el vendedor.
3. El usuario final obtiene la licencia mediante las operaciones de API `CheckoutLicense` o `CheckoutBorrowLicense`. La operación `CheckoutBorrowLicense` solo está permitida en las licencias con la opción Préstamo configurada. Devuelve una firma digital como parte de su respuesta junto con el objeto JSON que enumera los derechos. El objeto JSON de texto sin cifrar se parece al siguiente:

```
{
   "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"
   }
}
```

Validación de conformidad para License Manager

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).

- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulta la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en License Manager

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja demora. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura AWS global.

Seguridad de la infraestructura en License Manager

Como servicio gestionado, AWS License Manager está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder a License Manager a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

License Manager e interfaz de puntos finales de VPC con AWS PrivateLink

Puede establecer una conexión privada entre su nube privada virtual (VPC) y AWS License Manager creando un punto de conexión de VPC de tipo interfaz. Los puntos finales de la interfaz funcionan con una tecnología que puede utilizar para acceder de forma privada a la API de License Manager sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una AWS Direct Connect conexión. AWS PrivateLink Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con License Manager. El tráfico entre su VPC y License Manager no sale de la red de Amazon.

Cada punto de conexión de interfaz está representado por una o más interfaces de red elásticas en las subredes.

Para obtener más información, consulte Puntos de conexión de VPC de interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC.

Creación de un punto de conexión de VPC de interfaz para License Manager

Cree un punto de conexión de interfaz para License Manager utilizando uno de los siguientes nombres de servicio:

- com.amazonaws. ***region***.administrador de licencias

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

Si habilita un DNS privado para el punto de conexión, puede realizar solicitudes de API a License Manager mediante su nombre de DNS predeterminado para la región. Por ejemplo, `license-manager.`*`region`*`.amazonaws.com`.

Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Cree una política de punto de conexión de VPC para License Manager

Puede asociar una política a su punto de conexión de VPC a fin de controlar el acceso a License Manager. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones
- Las acciones que se pueden realizar
- El recurso en el que se pueden realizar las acciones

A continuación, se muestra un ejemplo de una política de punto de conexión para License Manager. Cuando se asocia con un punto de conexión, esta política concede acceso a las acciones de License Manager mostradas para todas las entidades principales en todos los recursos.

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

Para obtener más información, consulte Control del acceso a los servicios con puntos de conexión de VPC en la Guía del usuario de Amazon VPC.

Solución de problemas de License Manager

La siguiente información puede ayudarle a solucionar problemas que puedan surgir al utilizar AWS License Manager. Antes de empezar, confirme que la configuración de License Manager cumple los requisitos establecidos en the section called “Configuración”.

Error de detección entre cuentas

Al configurar la detección entre cuentas, puede encontrarse con el siguiente mensaje de error en la página Búsqueda en el inventario:

Excepción de Athena: la consulta de Athena falló: permisos insuficientes para ejecutar la consulta. Migre el catálogo para permitir el acceso a esta base de datos.

Esto puede ocurrir si el servicio de Athena utiliza el catálogo de datos administrado por Athena en lugar del de AWS Glue Data Catalog. Para obtener instrucciones de actualización, consulte Actualización al catálogo de datos de AWS Glue Step-by-Step.

La cuenta de administración no puede desasociar los recursos de una licencia autogestionada

Si una cuenta miembro de una organización elimina el rol vinculado al servicio (SLR) `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` en esta cuenta y existen recursos que pertenecen a los miembros y están asociados a una licencia autoadministrada, se evita que la cuenta principal se desasocie de dichos recursos de la cuenta miembro. Esto significa que los recursos de la cuenta miembro seguirán utilizando las licencias del grupo de la cuenta principal. Para permitir que la cuenta principal desasocie recursos, restaure el SLR.

Este comportamiento justifica los casos en los que un cliente prefiere no permitir que la cuenta de administración realice ciertas acciones que afectan a los recursos de la cuenta miembro.

Systems Manager Inventory no está actualizado

Systems Manager almacena datos en los datos de inventario durante 30 días. Durante este periodo, License Manager contabiliza una instancia administrada como activa aunque no permita hacer ping.

Una vez que los datos del inventario se hayan depurado de Systems Manager, License Manager marca la instancia como inactiva y actualiza los datos del inventario local. Para mantener la precisión de los recuentos de instancia administrados, recomendamos anular el registro de las instancias de forma manual en Systems Manager para que License Manager puede ejecutar operaciones de limpieza.

Persistencia aparente de una AMI con registro anulado

License Manager elimina las asociaciones obsoletas entre los recursos y las licencias autoadministradas cada pocas horas. Si se anula el registro de una AMI asociada a una licencia autogestionada en Amazon, es posible que EC2 la AMI siga apareciendo brevemente en el inventario de recursos de License Manager antes de ser purgada.

Las nuevas instancias de cuentas secundarias tardan en aparecer en el inventario de recursos

Cuando la compatibilidad entre cuentas se habilita, License Manager actualiza las cuentas de cliente a las 13:00 h cada día de forma predeterminada. Las instancias añadidas más tarde aparecen en el inventario de recursos de la cuenta de administración al día siguiente. Puede cambiar la frecuencia con la que se ejecuta el script de actualización editándolo `LicenseManagerResourceSynDataProcessJobTrigger` en la AWS Glue consola de la cuenta de administración.

Después de habilitar el modo entre cuentas, las instancias de las cuentas secundarias tardan en aparecer

Cuando habilita el modo entre cuentas en License Manager, las instancias de las cuentas secundarias pueden tardar desde algunos minutos hasta unas horas en aparecer en el inventario de recursos. El tiempo depende del número de cuentas secundarias y el número de instancias de cada cuenta secundaria.

La detección entre cuentas no se puede deshabilitar

Después de configurar una cuenta para la detección entre cuentas, es imposible volver a la detección en una única cuenta.

El usuario de la cuenta secundaria no puede asociar la licencia autoadministrada compartida con una instancia

Cuando esto sucede y la detección entre cuentas se encuentra habilitada, compruebe que se ha hecho lo siguiente:

- La cuenta secundaria se ha eliminado de la organización.
- La cuenta secundaria se ha eliminado del recurso compartido creado en la cuenta de administración.
- La licencia autoadministrada se ha eliminado del recurso compartido.

Se produce un error al vincular AWS Organizations cuentas

Si la página Configuración notifica este error, significa que una cuenta no es un miembro de una organización por las siguientes razones:

- Una cuenta secundaria se ha eliminado de la organización.
- Un cliente ha desactivado el acceso a License Manager desde la consola de la organización de la cuenta de administración.

Error en la configuración del producto de suscripción de usuario

Es posible que la configuración del producto esté fallando debido a problemas con el acceso a la red saliente. Para solucionar este problema, asegúrese de que el grupo de seguridad predeterminado permita el tráfico saliente a IPv4 las direcciones de la interfaz de red de cada controlador de dominio, así como al SSM.

- Compruebe que la configuración predeterminada del grupo de seguridad facilite el tráfico saliente a IPv4 las direcciones de las interfaces de red de los controladores de dominio.
  - License Manager crea dos interfaces de red que utilizan el grupo de seguridad predeterminado de la VPC en la que se aprovisiona AWS Managed Microsoft AD . Estas interfaces se utilizan para la funcionalidad de servicio requerida con su directorio. Asegúrese de que su grupo de seguridad predeterminado permita el tráfico saliente a la IPv4 dirección de la interfaz de red de cada controlador de dominio o al grupo de seguridad utilizado por los controladores de dominio.

Para obtener más información, consulte Requisitos previos para crear suscripciones basadas en usuarios y Qué se crea en la AWS Directory Service Guía de administración.

- Configure el acceso saliente a Internet desde instancias que proporcionan suscripciones basadas en usuarios o puntos de conexión de VPC.
  - El acceso saliente a Internet desde las instancias que proporcionan suscripciones basadas en usuarios, o puntos de enlace de VPC, debe configurarse para que las instancias se comuniquen con SSM. Para obtener más información, consulte Configuración de Systems Manager para EC2 instancias en la Guía del AWS Systems Manager usuario.

Una vez finalizado el proceso de aprovisionamiento, puede asociar un grupo de seguridad diferente a las interfaces creadas por License Manager. El grupo de seguridad que seleccione también debe permitir el tráfico necesario a la IPv4 dirección de la interfaz de red o al grupo de seguridad de cada controlador de dominio. Para obtener más información, consulte Trabajar con grupos de seguridad en la Guía del usuario de Amazon Virtual Private Cloud.

Las instancias de suscripción de usuario no se lanzan

Los lanzamientos de sus instancias pueden estar fallando debido a varios motivos. Estos son algunos de los problemas más comunes por los que puede fallar el lanzamiento de una instancia:

- Asegúrese de que SSM pueda detectar su instancia; consulte. the section called “Solucione los problemas de conectividad de las instancias”
- Asegúrese de que la instancia pueda unirse a su dominio, consulte. the section called “Solucione problemas al unirse al dominio”
- Asegúrese de que la regla de punto final del solucionador saliente de Route53 esté establecida. Para obtener más información, consulte la entrada del blog Integrar la resolución de DNS de su servicio de directorio con Amazon Route 53 Resolvers.
- Si va a lanzar instancias a partir de una suscripción de usuario AMIs creada a partir de una suscripción personalizada AMIs, asegúrese de utilizar Sysprep y de utilizar nombres de ordenador únicos al crear y lanzar instancias personalizadas. AMIs

La unión perfecta de dominios para EC2 instancias con productos de suscripción de usuario no funciona

License Manager debe realizar la unión de dominios en estas instancias mediante SSM para permitir el acceso autorizado únicamente a los usuarios suscritos al producto. Como resultado, se desactiva la función de unión fluida de dominios.

No se puede eliminar Active Directory

License Manager se registra como una aplicación autorizada en Directory Service durante la configuración, lo que evita que los directorios activos se eliminen una vez configurados. Como parte del procedimiento estándar, los clientes deben eliminar primero todas las instancias, asociaciones de instancias y suscripciones de usuarios. A continuación, pueden proceder a eliminar el directorio activo del License Manager y, posteriormente, eliminar el propio directorio.

El punto final de VPC se creó en mi cuenta

License Manager crea los puntos finales de la VPC necesarios para que sus recursos se conecten a los servidores de activación y cumplan la normativa al configurar la VPC.

Elimine todos los recursos de puntos finales de VPC creados por License Manager

Para eliminar los recursos de punto final de la VPC, debe realizar las siguientes acciones:

- Desasocie a todos los usuarios de sus suscripciones basadas en usuarios. Para obtener más información, consulte the section called “Desvincular a los usuarios de una instancia”.
- Elimine cualquier directorio que se haya configurado desde los ajustes de License Manager. Para obtener más información, consulte the section called “Anule el registro de Active Directory”.
- Termine todas las instancias que proporcionen productos de suscripción basada en usuarios. Para obtener más información, consulte the section called “Lance una instancia a partir de una licencia incluida (AMI)”.

No se pudo eliminar el rol vinculado al AWSService RoleFor AWSLicense ManagerUserSubscriptionsService servicio (SLR)

License Manager requiere la función "AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService" vinculada al servicio para administrar AWS los recursos que proporcionarán suscripciones basadas en los usuarios. Un rol vinculado a un servicio facilita la configuración de License Manager, ya que no es necesario añadir manualmente los permisos necesarios. License Manager define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo License Manager puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Para obtener más información, consulte the section called “Requisitos previos de una suscripción basada en el usuario” License Manager: rol de suscripción basado en el usuario y roles vinculados a servicios.

Error de suscripción no presente para el producto SAL de RDS

Su cuenta debe contar con una suscripción a Windows Server Remote Desktop Services Subscriber Access License (RDS SAL). Todos los usuarios asociados a las instancias que proporcionan productos de suscripción basada en usuarios deben disponer de una única suscripción activa a esta licencia, además de a cualquier otro producto que deseen utilizar. Su usuario se suscribirá a RDS SAL por usted cuando se suscriba a un producto de suscripción basada en usuarios.

Sin embargo, si se ha cancelado la suscripción o se ha eliminado por otros motivos de conformidad, es posible que tengas que volver a suscribirte. Si ya está suscrito, puede intentar cancelar y volver a suscribirse, lo que no afectará a las suscripciones de usuario de License Manager.

Solución de problemas de confianza

Según nuestra experiencia trabajando con muchos clientes, la gran mayoría de los problemas de configuración de la confianza se deben a errores de resolución del DNS o de conectividad de red. Estos son algunos pasos de solución de problemas que te ayudarán a resolver problemas comunes:

- Compruebe si ha permitido el tráfico de red saliente en el AWS Managed Microsoft AD.
- Si el servidor DNS o la red de su dominio local utilizan un espacio de direcciones IP público (distinto de la RFC 1918), siga estos pasos:

  - En la AWS Directory Service consola, vaya a la sección de enrutamiento IP de su directorio, elija Acciones y, a continuación, elija Agregar ruta.
  - Introduzca el bloque de direcciones IP de su servidor DNS o red local con el formato CIDR, por ejemplo, 203.0.113.0/24.
  - Este paso no es necesario si tanto el servidor DNS como la red local utilizan espacios de direcciones IP privadas según la norma RFC 1918.
- Tras comprobar el grupo de seguridad y comprobar si se requieren las rutas aplicables, lance una instancia de Windows Server y únala al AWS Managed Microsoft AD directorio. Una vez lanzada la instancia:
  - Ejecuta este PowerShell comando para probar la conectividad DNS:

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

También deberías consultar las explicaciones de los mensajes en la guía sobre los motivos del estado de creación de confianza que se encuentra en la AWS Directory Service documentación.

Problemas de facturación de las suscripciones de los usuarios

AWS le facturará mediante una suscripción mensual, en función del número de usuarios asociados a la licencia, incluidas las instancias de Microsoft Office o Visual Studio. Estos cargos por usuario se facturan por mes natural y la facturación comienza en el momento en que se suscribe al producto. Si eliminas el acceso a un usuario durante el mes actual, se te facturará por el usuario durante el resto del mes. Dejarás de incurrir en cargos para el usuario el mes siguiente.

Además:

- La facturación se basa en cada usuario dentro de las suscripciones de usuario. Solo los usuarios que estén suscritos al producto incurrirán en cargos, no todos los usuarios de Active Directory.
- La facturación se realiza en un ciclo mensual, a partir del primer día de cada mes natural. Los cargos se cobran durante todo el mes, independientemente de la fecha específica de activación de la suscripción.
- Necesita una SAL de RDS para cada usuario que necesite acceder a sus instancias de Office/VS.
- Para dejar de incurrir en cargos por las suscripciones basadas en usuarios, debe desasociar al usuario de todas las instancias a las que esté asociado. Eliminar un usuario de Active Directory no

desvincula al usuario de las instancias. Para obtener más información, consulte the section called "Desvincular a los usuarios de una instancia".

- Un usuario solo se cuenta una vez. Se cobra por usuario en el caso de Microsoft Office y Visual Studio, independientemente del número de EC2 instancias a las que se conecte el usuario. A los usuarios se les cobra la suscripción una vez, independientemente del uso que hagan de varias instancias.

Los productos de suscripción de usuario muestran el estado de suscripción de Marketplace como Inactivo

Después de configurar el directorio con los productos necesarios, tendrá que suscribirse a los productos necesarios. Los productos con un Estado de suscripción de Marketplace Inactivo requieren que se suscriba antes de poder asociar usuarios a una instancia y utilizarlos.

Cambie un nombre de usuario en Managed Active Directory

Cambiar un nombre de usuario no afecta a su capacidad de realizar RDP en las instancias asociadas. Los usuarios asociados deberían poder utilizar sus datos de inicio de sesión actualizados para realizar el RDP en las instancias de suscripción de usuario.

Disocia a los usuarios de una instancia finalizada

Cada vez que se cancela una instancia de suscripciones de usuario, se disocian todos los usuarios que están asociados a la instancia. No es necesario desasociar al usuario manualmente.

> **Note**
>
> Los usuarios no se disocian si la instancia se detiene.

Límites de usuarios por instancia

Hay un límite de 25 instancias por usuario. En caso de que necesites algún ajuste, ponte en contacto con AWS Support. A los usuarios se les cobra la suscripción una vez, independientemente del uso que hagan de varias instancias.

Instalar software adicional en las instancias de suscripción de los usuarios

Puede instalar software adicional en sus instancias que no se encuentre disponible como suscripciones basadas en usuarios. License Manager no hace ningún seguimiento de las instalaciones de software adicionales. Estas instalaciones deben realizarse con la cuenta de administrador que se crea de forma predeterminada en su AWS Managed Microsoft AD directorio. Para obtener más información, consulte la cuenta de administrador en la Guía de AWS Directory Service administración.

Para instalar software adicional con la cuenta de administrador:

- Suscriba la cuenta de administrador al producto proporcionado por la instancia.
- Asocie la cuenta de administrador a la instancia.
- Conéctese a la instancia mediante la cuenta de administrador para realizar la instalación.

Para obtener más información, consulte the section called “Introducción”.

Paquetes de idioma japonés en las instancias de suscripción de usuario

Las instancias de suscripción de usuario admiten la instalación de paquetes de idioma japonés.

Usuario administrador local en instancias de suscripción de usuario

Solo permitimos que los usuarios del dominio de Active Directory administrado por los usuarios se asocien a instancias de suscripción de usuarios para evitar el acceso no autorizado a estos productos de Microsoft. Al crear usuarios locales con privilegios de administrador en instancias que ofrecen suscripciones basadas en usuarios, el estado de la instancia cambia a estado insalubre.

Instancias en mal estado

Las instancias que proporcionan suscripciones basadas en usuarios deben mantenerse en buen estado para garantizar su conformidad. Las instancias marcadas como en mal estado ya no cumplen los requisitos previos requeridos. License Manager intenta devolver la instancia a un estado correcto, pero las instancias que no pueden volver a un estado correcto se cancelan.

Número de usuarios que pueden acceder mediante RDP a una instancia de suscripciones de usuario

Las instancias que ofrecen suscripciones basadas en usuarios admiten hasta dos sesiones de usuario activas a la vez, tal y como se indica en Use License Manager (suscripciones basadas en usuarios) para los productos de software compatibles. De forma predeterminada, Windows permite hasta 2 conexiones de escritorio remoto, incluida una conexión de administrador, en un momento dado, en todas las ediciones de Windows Server. Para utilizar más de 2 usuarios simultáneos, los clientes deben configurar un servidor de licencias de RDS.

Sistemas operativos Windows compatibles

Para obtener información sobre las plataformas de sistemas operativos Windows compatibles, consultethe section called “Suscripciones de software compatibles”.

Versiones compatibles de Office y Visual Studio

Para obtener información sobre el software compatible con las suscripciones basadas en usuarios, consultethe section called “Software compatible”.

Uso de la suscripción de usuario con versiones anteriores de Windows Server

Al lanzar una instancia desde una AMI compatible con Office LTSC Professional Plus o Microsoft Visual Studio, el inicio se realiza de forma predeterminada en la versión más reciente de la AMI para la plataforma de sistema operativo Windows (por ejemplo, Windows Server 2022). Para lanzarla con una versión anterior de la plataforma del sistema operativo, siga estos pasos:

1. Abre la AWS Marketplace consola enhttps://console.aws.amazon.com/marketplace.
2. Elija Administrar suscripciones del panel de navegación.
3. Para optimizar los resultados de la suscripción, puedes buscar todo o parte del nombre de la suscripción. Por ejemplo, Office LTSC Professional Plus 2021 o Visual Studio Enterprise.
4. Seleccione Lanzar nueva instancia en el panel de suscripción. Esto abre una página de configuración de lanzamiento.

5. Para lanzar una instancia desde una AMI basada en una versión anterior de la plataforma del sistema operativo Windows, seleccione el enlace completo al AWS Marketplace sitio web, ubicado en la versión de software. Esto le llevará a una página de configuración donde podrá seleccionar de una lista de versiones.
6. La lista muestra las últimas versiones de AMI para las plataformas de sistema operativo Windows compatibles. Seleccione la versión del sistema operativo Windows desde la que desee iniciar.

Uso de las suscripciones de usuario de License Manager en todas las cuentas o regiones

No se admiten los siguientes escenarios:

- Uso de las suscripciones de usuario de License Manager en todas las cuentas
- Uso de las suscripciones de usuario de License Manager en todas las regiones
- Uso de suscripciones de usuario de License Manager con Active Directory compartido

Gestión del token CAL durante la migración a RDS SAL

Si utiliza sus propios servidores de licencias RDS de Microsoft, cualquier token de licencia de acceso de cliente (CAL) ya emitido seguirá siendo válido hasta que caduque. Durante este período, los usuarios con fichas CAL válidas no se suscriben automáticamente al producto SAL de RDS. Las nuevas sesiones de usuario no se suscriben automáticamente a RDS SAL aunque License Manager esté configurado. License Manager no anula los tokens CAL existentes emitidos por sus propios servidores de licencias. El servidor de licencias gestionado por el servicio comienza a emitir tokens y a gestionar las nuevas solicitudes solo después de que caduquen los tokens CAL existentes. Una vez que los tokens CAL emitidos actualmente llegan a su fecha de caducidad, el servidor de licencias gestionado por el servicio gestiona las nuevas solicitudes de token y los usuarios se suscriben automáticamente al producto SAL de RDS según sea necesario.

Usuarios en mi AD autogestionado con productos de suscripción de usuario

Para asociar los usuarios a su directorio autogestionado, debe establecer una confianza bidireccional en el bosque entre el directorio autogestionado y el directorio. AWS Managed Microsoft AD Para

obtener más información, consulte el tutorial: Crear una relación de confianza entre su dominio de Active Directory AWS Managed Microsoft AD y su dominio autoadministrado en la Guía de administración. AWS Directory Service

Consejos para contactar con AWS Support

- Cuando te pongas en contacto con el servicio de AWS asistencia, crea una instancia con la misma configuración que una instancia finalizada y activa la protección contra la terminación de la instancia para obtener una respuesta rápida.
- Para cualquier problema relacionado con el RDP, necesitaríamos los registros relacionados con el RDP para ayudar a solucionar estos problemas. Utilice el «AWSSupport-RunEC2RescueForWindowsTool» para los entornos con acceso a Internet. Para obtener más información, consulte EC2Rescue for Windows Server.
- Al utilizar una instancia de Office como instancia de trabajo y montar un volumen restaurado a partir de una instantánea del volumen de la instancia original, es posible recopilar datos incluso en un entorno sin acceso a Internet.
- Solución de problemas de lanzamientos de instancias desde Backup AMIs: si lanza una instancia desde una AMI de respaldo, debe terminar la instancia original.

Historial de documentos de License Manager

En la siguiente tabla se describen las versiones de AWS License Manager.

Cambio	Descripción	Fecha
Se agregó compatibilidad con las suscripciones basadas en usuarios de las licencias de acceso de suscriptor (RDS SAL) de Microsoft Remote Desktop Services	License Manager agregó soporte para la administración y configuración de las suscripciones basadas en usuarios de RDS SAL, incluida la capacidad de configurar más de dos conexiones de escritorio remoto a la vez.	14 de noviembre de 2024
Se actualizó la política gestionada por SLR de suscripciones basadas en usuarios para obtener información sobre rutas y redes	License Manager agregó los siguientes permisos para administrar las licencias y los datos de Active Directory : obtener información de rutas de Route 53, obtener información de redes y reglas de grupos de seguridad de Amazon EC2 y obtener secretos de Secrets Manager. Para obtener más información, AWS política gestionada: AWSLicenseManagerUserSubscriptionsServiceRolePolicy.	7 de noviembre de 2024
Recupere la información de suscripción BYOL de Red Hat Subscription Manager (RHSM)	License Manager agregó soporte para recuperar información de suscripción de RHSM para licencias BYOL en instancias de Red Hat Enterprise Linux. Esto incluye	10 de julio de 2024

Cambio	Descripción	Fecha
	actualizaciones de AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy.	
Se agregó compatibilidad con Amazon RDS para licencias BYOL basadas en vCPU de Db2	License Manager agregó compatibilidad con Amazon RDS para licencias BYOL basadas en vCPU de Db2.	20 de marzo de 2024
Se ha agregado compatibilidad con Windows Server 2019 para las suscripciones basadas en usuarios de Microsoft Office	AWS se agregó soporte para Windows Server 2019 en Amazon Machine Images (AMIs) con licencias proporcionadas por Amazon para Microsoft Office LTSC Professional Plus 2021 en Amazon. EC2	4 de diciembre de 2023
Los usuarios de dominios (en las instalaciones) autoadministrados pueden utilizar suscripciones basadas en usuarios	License Manager agregó soporte para que los usuarios del dominio autoadministrado de Active Directory utilicen suscripciones basadas en usuarios cuando se haya creado una confianza en su AWS Managed Microsoft AD directorio.	6 de septiembre de 2023
Conversiones de tipos de licencias para las suscripciones a Ubuntu LTS	License Manager agregó soporte para que las instancias de Ubuntu LTS utilicen la conversión de tipos de licencias para agregar una suscripción a Ubuntu Pro.	20 de abril de 2023

Cambio	Descripción	Fecha
Sustitución de las concesiones activas	License Manager agregó una funcionalidad para sustituir opcionalmente las concesion es activas por una licencia concedida durante la activació n de la concesión.	31 de marzo de 2023
Administración delegada para las suscripciones de Linux	License Manager agregó soporte para administradores delegados para las suscripci ones de Linux.	3 de marzo de 2023
Suscripciones de Linux	License Manager agregó el seguimiento de las suscripci ones comerciales de Linux.	21 de diciembre de 2022
CloudWatch Métricas de Amazon	License Manager ahora emite CloudWatch métricas para la configuración de licencias, el uso y las suscripciones.	21 de diciembre de 2022
Microsoft Office para suscripci ones basadas en usuarios	License Manager agregó Microsoft Office como software compatible para las suscripciones basadas en usuarios.	28 de noviembre de 2022
Distribución de derechos a las unidades organizativas	Distribuya derechos a una unidad organizativa específica de su organización.	17 de noviembre de 2022
Visión general de la organizac ión (consola)	Gestione las licencias concedidas en sus cuentas AWS Organizations mediante la consola License Manager.	11 de noviembre de 2022

Cambio	Descripción	Fecha
Suscripciones basadas en usuarios	Utiliza productos de suscripción basados en usuarios compatibles en Amazon EC2.	2 de agosto de 2022
Registro y envío de datos de uso de las licencias (consola)	Registre y envíe los datos de uso de las licencias mediante la consola License Manager.	28 de marzo de 2022
Conversión de tipos de licencia (consola)	Cambie el tipo de licencia entre la licencia AWS proporcionada y el modelo Bring Your Own License (BYOL) mediante la consola License Manager sin tener que volver a implementar las cargas de trabajo existentes.	9 de noviembre de 2021
Conversión de tipos de licencia (CLI)	Cambie el tipo de licencia entre la licencia AWS proporcionada y el modelo Bring Your Own License (BYOL) AWS CLI sin tener que volver a distribuir las cargas de trabajo existentes.	22 de septiembre de 2021
Uso compartido de los derechos	Comparta los derechos de las licencias administradas con toda su organización con una sola solicitud.	16 de julio de 2021

Cambio	Descripción	Fecha
Informes de uso	Realice un seguimiento del historial de las configuraciones de sus tipos de licencia con los informes de uso de License Manager. Los informes de uso se denominaban antes generadores de informes e informes de licencias.	18 de mayo de 2021
Reglas de exclusión de la detección automatizada	Excluya las instancias de la detección automática de License Manager en función de la AWS cuenta IDs y las etiquetas.	5 de marzo de 2021
Derechos administrados	Realice un seguimiento y distribuya los derechos de licencia de los productos comprados a AWS Marketplace los vendedores que utilizan License Manager para distribuir licencias.	3 de diciembre de 2020
Contabilización automatizada del software desinstalado	Configure la detección automatizada para detener el seguimiento de las instancias cuando se desinstala el software.	3 de diciembre de 2020
Filtrado por etiquetas	Busque en su inventario de recursos utilizando etiquetas.	3 de diciembre de 2020
Ámbito de asociación de las AMI	Asocie sus licencias autogestionadas y las AMIs compartidas a su cuenta. AWS	23 de noviembre de 2020

Cambio	Descripción	Fecha
Afinidad de licencia con el alojamiento	Asigne licencias a hardware dedicado durante un determinado número de días.	12 de agosto de 2020
Seguimiento de las implement aciones de Oracle en Amazon RDS	Realice un seguimiento del uso de las ediciones y los paquetes de licencias del motor de base de datos Oracle en Amazon RDS.	23 de marzo de 2020
Grupos de recursos de host	Configure un grupo de recursos de host para permitir que License Manager administre sus hosts dedicados.	1 de diciembre de 2019
Detección automatizada de software	Configure License Manager para buscar sistemas operativos o aplicaciones recién instalados y asocie las licencias autoadmin istradas correspondientes a las instancias.	1 de diciembre de 2019
Diferenciación entre modelos con licencias incluidas y el modelo BYOL	Filtre los resultados de la búsqueda en función de si utilizas las licencias proporcio nadas por Amazon o las suyas propias.	8 de noviembre de 2019

Cambio	Descripción	Fecha
Asociación de licencias a recursos en las instalaciones	Después de asociar licencias a una instancia en las instalaciones, License Manager recopila periódicamente el inventario de software, actualiza la información de licencias e informa sobre el uso.	8 de marzo de 2019
AWS License Manager versión inicial	Lanzamiento del servicio inicial	28 de noviembre de 2018

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.