



Guía del usuario

AWS License Manager



AWS License Manager: Guía del usuario

Copyright © 2024 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
Configuración	8
Inscríbase en una Cuenta de AWS	8
Creación de un usuario con acceso administrativo	9
Introducción a License Manager	10
Uso de License Manager	11
Licencias autoadministradas	12
Parámetros y reglas	13
Creación de reglas de a partir de las licencias de los proveedores	15
Cree una licencia autoadministrada	17
Comparta una licencia autoadministrada	19
Edite una licencia autoadministrada	23
Desactive una licencia autoadministrada	23
Elimine una licencia autoadministrada	24
Reglas de asignación de licencias	25
Asociación de licencias autoadministradas a las AMI	26
Desasociación de licencias autoadministradas de las AMI	27
Informes de uso	28
Creación de un informe de uso	28
Edición de informes de uso	29
Eliminación de un informe de uso	30
Conversiones de tipos de licencia	31
Tipos de licencia aptos	32
Requisitos previos	44
Conversión de un tipo de licencia	46
Conversión de tenencias	56
Resolución de problemas	58
Grupos de recursos de host	60
Cree un grupo de recursos de host	61

Comparta un grupo de recursos de host	62
Cómo añadir host dedicados a un grupo de recursos de host	62
Lance una instancia en un grupo de recursos de host	63
Modifique un grupo de recursos de host	63
Cómo eliminar hosts dedicados de un grupo de recursos de host	64
Elimine un grupo de recursos de host	64
Búsqueda en el inventario	65
Cómo trabajar con la búsqueda en el inventario	66
Detección automatizada en el inventario	72
Licencias concedidas	74
Visualización de las licencias concedidas	75
Administre las licencias concedidas	76
Distribuya los derechos	79
Aceptación y activación de concesiones	81
Estado de las licencias	83
Métricas para las cuentas de compradores	85
Licencias emitidas por el vendedor	86
Concesiones de derechos	87
Uso de licencias	87
Requisitos	88
Cómo crear licencias emitidas por el vendedor	90
Concesión de licencias a los clientes	91
Cómo obtener credenciales temporales para clientes sin cuenta de AWS	92
Consumo de licencias	93
Cómo eliminar licencias emitidas por el vendedor	94
Suscripciones basadas en usuarios	94
Requisitos previos	96
Consideraciones	99
Software compatible	100
Introducción	103
Modificación de la configuración del directorio	114
Modificación de la configuración de la VPC	115
Desasociación de usuarios	116
Cancelación de la suscripción de usuarios	116
Interrupción de instancias	117
Eliminación de un directorio	118

Resolución de problemas	118
Suscripciones de Linux	120
Administración de la detección	122
Visualización de las instancias	126
Información de facturación	128
Métricas de uso y alarmas	130
Configuración	133
Licencias administradas	134
Suscripciones de Linux	136
Suscripciones basadas en usuarios	136
Administradores delegados	137
Panel	142
Monitoreo de License Manager	144
Monitoreo con CloudWatch	144
Creación de alarmas de CloudWatch	146
Registro de llamadas a la API con CloudTrail	146
Información de License Manager en CloudTrail	147
Descripción de las entradas del archivo de registros de License Manager	148
Seguridad	150
Protección de los datos	151
Cifrado en reposo	152
Administración de identidades y accesos	152
Creación de usuarios, grupos y roles	152
Estructura de la política de IAM	153
Cree políticas de IAM para License Manager	153
Concesión de permisos a usuarios, grupos y roles	155
Roles vinculados al servicio	156
Rol principal	157
Rol de cuenta de administración	159
Rol de cuenta miembro	162
Rol de suscripción basada en usuarios	164
Rol de suscripciones de Linux	166
Políticas administradas de AWS	167
AWSLicenseManagerServiceRolePolicy	168
AWSLicenseManagerMasterAccountRolePolicy	170
AWSLicenseManagerMemberAccountRolePolicy	174

AWSLicenseManagerConsumptionPolicy	175
AWSLicenseManagerUserSubscriptionsServiceRolePolicy	175
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	177
Actualizaciones de políticas	178
Firma de licencias	181
Validación de conformidad	182
Resiliencia	184
Seguridad de la infraestructura	184
Puntos de conexión de VPC (AWS PrivateLink)	185
Creación de un punto de conexión de VPC de interfaz para License Manager	185
Cree una política de punto de conexión de VPC para License Manager	186
Resolución de problemas	187
Error de detección entre cuentas	187
La cuenta de administración no puede disociar los recursos de una licencia autogestionada ...	187
Systems Manager Inventory no está actualizado	187
Persistencia aparente de una AMI con registro anulado	188
Las nuevas instancias de cuentas secundarias tardan en aparecer en el inventario de recursos	188
Después de habilitar el modo entre cuentas, las instancias de las cuentas secundarias tardan en aparecer	188
La detección entre cuentas no se puede deshabilitar	188
El usuario de la cuenta secundaria no puede asociar la licencia autoadministrada compartida con una instancia	189
Se produce un error al vincular AWS Organizations cuentas	189
Historial de documentos	190
.....	cxcvi

¿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 realizar el seguimiento de cualquier software cuyas licencias se basen en el número de núcleos virtuales (vCPU), núcleos físicos, sockets o máquinas. Esto incluye diversos productos de software de Microsoft, IBM, SAP, Oracle y otros proveedores.

Con AWS License Managerél, puede realizar un seguimiento centralizado de las licencias y hacer cumplir los límites en varias regiones, manteniendo un registro 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. Los ISV pueden 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 (ISV) pueden utilizarlos AWS License Manager para gestionar y distribuir las licencias de software y los 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 License Manager. Los ISV que se venden de forma automática AWS Marketplace se benefician de la creación y distribución automáticas de licencias como parte del flujo de trabajo de las transacciones. Los ISV también pueden 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.
- [Suscripciones basadas en usuarios en License Manager](#): se utiliza para adquirir licencias de software compatible proporcionadas por Amazon, plenamente conformes, con una cuota de suscripción por usuario.
- [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 AWS Marketplace, AWS Systems Manager Amazon RDS y. AWS Organizations

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

- [Instancias de Amazon EC2](#)
- [Instancias dedicadas](#)
- [Hosts dedicados](#)
- [Instancias de spot y flotas de spot](#)
- [Nodos administrados](#)

Si utiliza License Manager junto con el 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 un vendedor que haya integrado su software o directamente a él AWS License Manager. AWS Data Exchange 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](#)

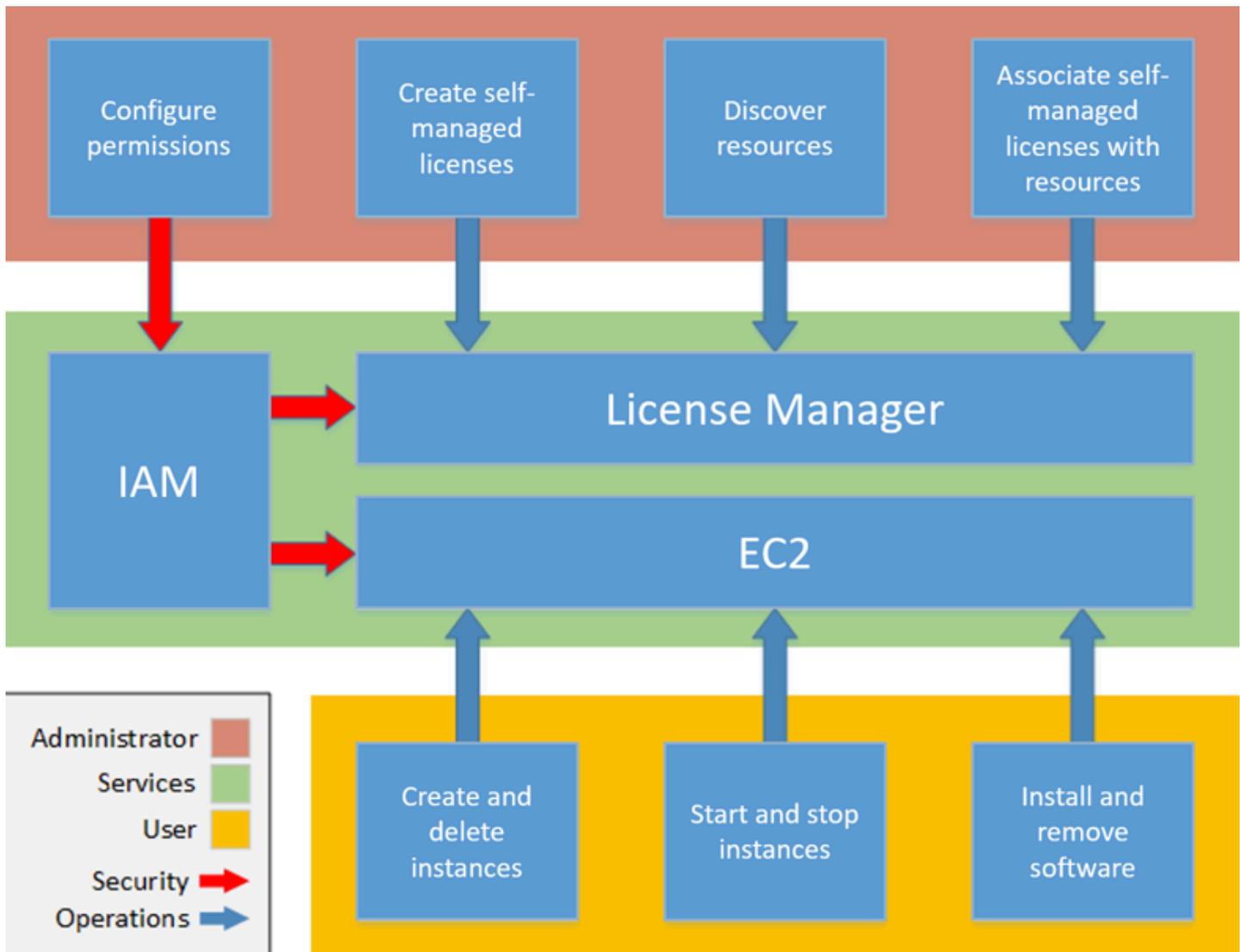
Cómo funciona License Manager

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. Y lo que es más importante, también se integra de manera nativa con los servicios de AWS, por ejemplo, con el plano de control de Amazon EC2, en el que se crean y se 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 tareas, distintas pero coordinadas, de los administradores de licencias, que administran los permisos y configuran License Manager, y los usuarios, que crean, administran y eliminan recursos a través de la consola Amazon EC2.



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 suponer la asociación de una licencia autoadministrada a una imagen de máquina de Amazon (AMI) aprobada,

que el personal de TI utiliza como plantilla para todas las implementaciones de instancias de Amazon EC2.

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.

Empezar con AWS License Manager

Las siguientes secciones lo guían en la configuración de sus usuarios Cuenta de AWS y en cómo empezar a utilizar License Manager. Para obtener más información sobre cómo administrar los permisos de los usuarios, grupos y roles para utilizar License Manager siguiendo las prácticas AWS recomendadas, consulte [Administración de identidades y accesos en AWS License Manager](#). Para obtener más información sobre la configuración de los recursos de Amazon EC2 que se integran con License Manager, consulte [Configuración para usar Amazon EC2](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

Temas

- [Configuración](#)
- [Incorporado para usar License Manager en el AWS Management Console](#)

Configuración

En la siguiente sección se detalla la configuración Cuenta de AWS de sus usuarios.

Inscríbase en una Cuenta de AWS

Si no tiene una Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWS se crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar [tareas que requieren acceso de usuario raíz](#).

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en <https://aws.amazon.com/> y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión [AWS Management Console](#) como propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte [Signing in as the root user](#) en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

Para obtener instrucciones, consulte [Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz \(consola\)](#) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Consulte las instrucciones en [Activar AWS IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte [Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la](#) Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte [Iniciar sesión en el portal de AWS acceso](#) en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte [Create a permission set](#) en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte [Add groups](#) en la Guía del usuario de AWS IAM Identity Center .

Incorporado para usar License Manager en el AWS Management Console

Para empezar a utilizar License Manager, es necesario seguir el siguiente procedimiento. Una vez completados los requisitos iniciales, puede continuar con el uso de License Manager para el caso de uso que desee.

Procedimiento para empezar a utilizar License Manager

1. Abra la consola 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.

Trabajar con AWS 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 para los productos de AWS Marketplace

License Manager ahora le permite asociar reglas de asignación de licencias a los productos de imágenes de máquinas de Amazon (AMI) con modelo Bring Your Own License (BYOL) de AWS Marketplace a través de las plantillas de lanzamiento de Amazon EC2, las plantillas de AWS CloudFormation o los productos de Service Catalog. En cada caso, podrá beneficiarse del seguimiento de licencias centralizado y se asegurará del cumplimiento.

Note

License Manager no cambia la forma en que se obtienen y activan las AMI BYOL de 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

License Manager le permite detectar las aplicaciones que se ejecutan fuera de AWS con [Systems Manager inventory](#) y, a continuación, asociar reglas de asignación de licencias a dichas aplicaciones. 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 cuentas de AWS

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

en todas las cuentas mediante AWS Resource Access Manager o al vincular cuentas de AWS Organizations con configuraciones de License Manager. Esto también le permite llevar a cabo la detección entre cuentas para buscar en el inventario de las cuentas de AWS.

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](#)
- [Grupos de recursos de host en AWS License Manager](#)
- [Búsqueda en el inventario en License Manager](#)
- [Licencias concedidas en License Manager](#)
- [Licencias emitidas por el vendedor en License Manager](#)
- [Suscripciones basadas en usuarios en License Manager](#)
- [Suscripciones de Linux en License Manager](#)
- [Configuración de AWS License Manager](#)
- [Panel en AWS License Manager](#)

Licencias autoadministradas en License Manager

Las licencias autoadministradas son el núcleo de License Manager. Las licencias autoadministradas se denominaban antes configuraciones de licencias. 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.

Límites

- Número de licencias autoadministradas por recurso: 10
- Número total de licencias autoadministradas: 25
- Las instancias administradas por Systems Manager deben estar asociadas a licencias autoadministradas tipo vCPU e instancia.

Contenido

- [Parámetros y reglas de las licencias autoadministradas](#)
- [Cree reglas de License Manager a partir de licencias de los proveedores](#)
- [Cree una licencia autoadministrada](#)
- [Comparta una licencia autoadministrada](#)
- [Edite una licencia autoadministrada](#)
- [Desactive una licencia autoadministrada](#)
- [Elimine una licencia autoadministrada](#)

Parámetros y reglas de las licencias autoadministradas

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 las vCPU, los núcleos, los sockets y las 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.
- Cantidad máxima de CPU virtuales: número máximo de vCPU 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.
- Cantidad mínima de CPU virtuales: número mínimo de vCPU para un recurso.
- Tenencia: restringe el uso de la licencia a la tenencia de EC2 especificada. Si el tipo de recuento es de núcleos o sockets, se requieren hosts dedicados. Si el tipo de recuento es instancias o vCPU, se admiten la tenencia compartida, los hosts dedicados y las instancias dedicadas. Los nombres de la consola (y las 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 permite personalizar el número de vCPU de una instancia. Si la regla se establece como Verdadera, las vCPU se contabilizan según el recuento personalizado de núcleos y subprocesos. De lo contrario, License Manager cuenta el número predeterminado de vCPU 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	vCPU
Afinidad de licencia con el alojamiento (en días)	licenseAffinityToHost	✓		✓	
Cantidad máxima de núcleos	maximumCores	✓	✓		
Cantidad máxima de sockets	maximumSockets		✓	✓	
Cantidad máxima de CPU virtuales	maximumVcpus		✓		✓

Nombre de la consola	Nombre de API	Núcleos	Instancias	Sockets	vCPU
Cantidad mínima de núcleos	<code>minimumCores</code>	✓	✓		
Cantidad mínima de sockets	<code>minimumSockets</code>		✓	✓	
Cantidad mínima de CPU virtuales	<code>minimumVcpus</code>		✓		✓
Propiedad	<code>allowedTenancy</code>	✓	✓	✓	✓
Optimización de vCPU	<code>honorVcpuOptimization</code>				✓

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 los 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	El número de núcleos se establece en 96 .
Cantidad mínima o máxima de vCPU o núcleos	La cantidad mínima de núcleos se establece en 8 . La cantidad máxima de núcleos se establece en 16 .

Regla de License Manager	Configuración
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 autoadministrada

Una licencia autoadministrada representa los términos de licencia del acuerdo con su proveedor de software. La licencia autoadministrada especifica cómo deben contarse las licencias (por ejemplo, por vCPU 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 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 (vCPU, 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 (se admiten los ID de AWS cuenta y las etiquetas de 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)

- [New-LICM \(LicenseConfiguration\)](#) AWS Tools for PowerShell

Comparta una licencia autoadministrada

Puede utilizarlas 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.

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 la 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. Utilice el [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"
      }
    ]
  }
}
```

- Utilice el [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. Utilice el [enable-sharing-with-aws-organization](#) AWS CLI comando para habilitar el uso compartido de recursos con AWS RAM:

```
aws ram enable-sharing-with-aws-organization  
  
{  
  "returnValue": true  
}
```

Puede usar el [list-aws-service-access-for-organization](#) AWS CLI comando para comprobar que las entidades principales de servicio de Organizations lists estén habilitadas 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. Utilice el [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 usar el [get-resource-share-associations](#) AWS CLI comando para validar que la asociación de recursos compartidos status sea 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
  }
]
}
```

Edite una licencia autoadministrada

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 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)
- [Update-licm LicenseConfiguration](#) ()AWS Tools for PowerShell

Desactive una licencia autoadministrada

Si desactiva una licencia autoadministrada, los recursos existentes que utilizan la licencia no se ven afectados y las imágenes de máquina de Amazon (AMI) que utilizan la licencia se pueden seguir lanzando. 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 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)
- [Update-licm \(\) LicenseConfiguration](#) AWS Tools for PowerShell

Elimine una licencia autoadministrada

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 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 licm \(\) LicenseConfiguration](#) AWS Tools for 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 la organización pueden lanzar sin problemas instancias de EC2 desde las imágenes de máquina de Amazon (AMI) designadas y los administradores pueden realizar un seguimiento del inventario de licencias a través del panel 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 administradas con las AMI: para realizar un seguimiento de las licencias del sistema operativo u otro software, puede adjuntar reglas de asignación de licencias a las AMI antes de publicarlas para un uso más amplio en su organización. Cualquier implementación desde estas AMI se controla automáticamente mediante License Manager sin que los usuarios tengan que 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 lanzamiento de Amazon EC2 y AWS CloudFormation: [si adjuntar reglas de licencia a las AMI no es una opción preferida, puede especificarlas como parámetros opcionales en las plantillas o plantillas de lanzamiento de EC2.AWS CloudFormation](#) Las implementaciones con estas plantillas se controlan mediante License Manager. Puede hacer cumplir las normas sobre las plantillas o AWS CloudFormation plantillas de lanzamiento de EC2 especificando uno o más identificadores de licencia autogestionados 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.

Asociación de licencias autoadministradas a las AMI

El siguiente procedimiento muestra cómo asociar licencias autoadministradas a las AMI mediante 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 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 las AMI asociadas actualmente, seleccione AMI asociadas.
4. Seleccione AMI asociadas.
5. Para AMI disponibles, seleccione una o más AMI y Asociar.
 - Si su cuenta es propietaria de al menos una de las AMI, se le solicitará que elija un ámbito de asociación de AMI para las AMI de su propiedad. Las AMI que se hayan compartido desde otra cuenta se asocian únicamente a su cuenta. Elija Confirmar.
 - Si las AMI se compartieron con usted desde otra cuenta se asocian únicamente a su cuenta.

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

Desasociación de licencias autoadministradas de las AMI

El siguiente procedimiento muestra cómo desasociar licencias autoadministradas de las AMI mediante la consola License Manager. No se puede desasociar una AMI que se haya dado de baja. License Manager comprueba si hay AMI cuyo registro se haya anulado cada 8 horas y las desasocia automáticamente.

Procedimiento para desasociar una licencia autoadministrada y una AMI

1. Abra la consola 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 AMI asociadas.
5. Seleccione la AMI y elija Desasociar AMI.

Informes de uso en License Manager

Con AWS License Manager, puede realizar un seguimiento del historial de sus licencias autoadministradas 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 los 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.

Creación de un informe de uso

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 que utiliza el tipo de licencia

autoadministrada especificado aparece con detalles como el ID de licencia, el estado del recurso y el ID de la cuenta de AWS propietaria del recurso.

Procedimiento para crear un informe de uso

1. Abra la consola 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 identificador uniforme de recursos (URI) de Amazon S3:

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

Edición de informes de uso

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 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.

Eliminación de un informe de uso

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 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:

Migración de cargas de trabajo en las instalaciones a Amazon EC2

Durante la migración, puede implementar su carga de trabajo en Amazon Elastic Compute Cloud (Amazon EC2) y AWS utilizar las licencias 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 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](#)
- [Requisitos previos de la conversión](#)
- [Conversión de un tipo de licencia](#)
- [Conversión de tenencias](#)
- [Solución de problemas de conversión de tipos de licencia](#)

Tipos de licencia aptos para la conversión de tipos de licencia

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](#)
 - [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](#)

Tipos de licencia aptos para Windows y SQL Server

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
Windows Server como BYOL	RunInstances:0800 ----SEP----:0800
SQL Server (cualquier edición) como BYOL	
Windows Server como modelo con licencia incluida	RunInstances:0800 ----SEP----:0002
Windows Server como modelo con licencia incluida	RunInstances:0002 ----SEP----:0002
SQL Server (cualquier edición) como BYOL	
Windows Server como modelo con licencia incluida	RunInstances:0002 ----sep----:0202
SQL Server Web como modelo con licencia incluida	
Windows Server como modelo con licencia incluida	RunInstances:0202 ----SEP----:0006
SQL Server Standard como modelo con licencia incluida	
Windows Server como modelo con licencia incluida	RunInstances:0006 ----Sept----:0102

Detalles del sistema operativo	Operación de uso
SQL Server Enterprise como modelo con licencia incluida	

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 [Conversión de un tipo de licencia](#).

⚠ 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	Windows Server como BYOL	Windows Server como BYOL	Windows 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	Sí ²	No es necesario	Sí ^{1, 2}	No se necesitan ³	No se admite	Sí ¹

Origen	Destino					
con licencia incluida (su propio medio)						
Windows Server como licencia incluida (imagen AWS proporcionada)	No <i>X</i>	No es necesario	No <i>X</i>	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 <i>x</i>	No se necesitan ⁴	No <i>x</i>	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					
SQL Server como modelo con licencia incluida						

Origen	Destino					
Windows Server como licencia incluida (imagen AWS proporcionada o contenido multimedia)	No <i>x</i>	No <i>x</i>	No <i>x</i>	No <i>x</i>	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 \times	Sí ⁵	No \times	Sí	No se admite	No es necesario
SQL Server como modelo con licencia incluida (su propio medio)						

\times 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

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	RunInstancesNo es necesario ----sep----:0g00

Rutas de conversión para Linux

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 AWS Support. Para obtener más información, consulte [Creación de un caso de soporte](#).

Requisitos previos de la conversión

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 [Empezar con AWS License Manager](#).
- La instancia de destino debe estar detenida antes de convertir el tipo de licencia. Para obtener más información, consulte [Detener e iniciar la instancia](#) en la Guía del usuario de Amazon EC2.
- 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](#).
- La instancia de destino debe configurarse con AWS Systems Manager Inventory. Para obtener más información, consulte [Configuración de Systems Manager para instancias EC2](#) e [AWS Systems Manager Inventory](#) en la Guía del usuario de AWS Systems Manager .
- 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 instancia de Amazon EC2 original debe lanzarse desde la imagen de su propia máquina virtual (VM). Para obtener más información sobre la conversión de una VM 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 usa para descargar de redes de desarrollo de contenido (CDN).
 - `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.

Conversión de un tipo de licencia

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, utilice la API [DescribeInstances](#) de Amazon EC2. Además, si tiene flujos de trabajo existentes que buscan información de facturación de las AMI, actualice esos flujos de trabajo para utilizar `DescribeInstances`.

Contenido

- [Cómo convertir un tipo de licencia para Windows y SQL Server](#)
 - [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](#)
- [Conversión de un tipo de licencia para Linux](#)
 - [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](#)

Cómo convertir un tipo de licencia para Windows y SQL Server

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 instancia de Amazon EC2 debe lanzarse desde la imagen de su propia 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 vCPU.

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 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:
 1. Ubuntu LTS
 2. Windows BYOL
 3. 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, consulte [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 [DescribeInstances](#) en Referencia de la API de Amazon EC2.

```
"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 convertir una licencia como modelo con licencia incluida en un modelo BYOL, la instancia de Amazon EC2 original debe lanzarse desde la imagen de su propia máquina virtual (VM). Para obtener más información sobre la conversión de una VM 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
```

Conversión de un tipo de licencia para Linux

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.

- 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 usuario de Amazon EC2 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 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:
 1. Ubuntu LTS
 2. Windows BYOL
 3. 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](#).

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 `UsageOperation` valor 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 [DescribeInstances](#) en Referencia de la API de Amazon EC2.

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

Haga la conversión a Ubuntu Pro

Al convertir una instancia de Ubuntu LTS a Ubuntu Pro, se debe disponer de acceso de salida a Internet desde la instancia para recuperar un token de licencia de los servidores de Canonical, así como tener instalado Ubuntu Pro Client. Para obtener más información, consulte [Requisitos previos de la conversión](#).

Para convertir Ubuntu LTS a Ubuntu Pro:

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 AWS Support. Para obtener más información, consulte [Creación de un caso de soporte](#).

Conversión de tenencias

Puede cambiar la tenencia de una instancia para que se adapte mejor a su caso de uso.

Puedes usar el AWS CLI comando [modify-instance-placement](#) 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 [Grupos de recursos de host en AWS 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.
- Todos los códigos de facturación de las ediciones compatibles de SQL Server, Red Hat (RHEL) y SUSE (SLES) con modelos con licencia incluida están permitidos en las tenencias compartidas y las instancias dedicadas. 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

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 - \[instancia\] se encuentra en un estado no válido para cambiar el tipo de licencia.](#)
- [La instancia \[instance\] de EC2 no se pudo detener. Asegúrese de tener permisos para StopInstances. de EC2.](#)

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 [¿Cómo puedo solucionar un mensaje de error de activación de Windows en mi instancia de Windows de Amazon EC2?](#) y active Windows con el manual de procedimientos de automatización de Systems Manager [AWSsupport-ActivateWindowsWithAmazonLicense](#), o bien inicie sesión en la instancia y cambie manualmente al servidor de 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 para Windows desde una AMI que haya importado para realizar una conversión 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 la conversión](#).

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 la conversión](#) y [Solucionar problemas de detención de la instancia](#) de la Guía del usuario de Amazon Elastic Compute Cloud.

La instancia [instance] de EC2 no se pudo detener. Asegúrese de tener permisos para **StopInstances** de EC2.

Debe tener permisos para realizar la acción de la API StopInstances de EC2 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.

Grupos de recursos de host en AWS License Manager

Un host dedicado de Amazon EC2 es un servidor físico con capacidad de instancias EC2 totalmente dedicado 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, consulte [Hosts dedicados](#) en la Guía del usuario de Amazon EC2.

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 por usted en caso de que el lanzamiento de una instancia en este grupo de recursos de host supere su capacidad disponible.
- **Liberar hosts automáticamente:** indica si Amazon EC2 puede liberar por usted los hosts no utilizados. Un host no utilizado no tiene ninguna instancia en ejecución.
- **Recuperar hosts automáticamente:** indica si Amazon EC2 puede trasladar instancias de un host que ha fallado inesperadamente a un host nuevo.
- **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

- [Cree un grupo de recursos de host](#)
- [Comparta un grupo de recursos de host](#)
- [Cómo añadir host dedicados a un grupo de recursos de host](#)
- [Lance una instancia en un grupo de recursos de host](#)
- [Modifique un grupo de recursos de host](#)
- [Cómo eliminar hosts dedicados de un grupo de recursos de host](#)
- [Elimine un grupo de recursos de host](#)

Cree un grupo de recursos de host

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 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 Configuración de administración de hosts dedicados de EC2, habilite o deshabilite las siguientes opciones 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.

Comparta un grupo de recursos de host

Puede usar 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 [Guía del usuario de AWS RAM](#).

Cómo añadir host dedicados a un grupo de recursos de host

Puede añadir hosts existentes a un grupo de recursos de host desde AWS Management Console, AWS CLI, o la API de AWS. Para agregar sus hosts, debe ser el propietario de la cuenta de AWS 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

Supongamos que detiene las instancias y desea reiniciarlas. Debe hacer lo siguiente:

- [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.

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 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

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 imagen de máquina de Amazon (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 puede usar la consola Amazon EC2. Para obtener más información, consulte [Lanzar instancias en un grupo de recursos de host](#) en la Guía del usuario de Amazon EC2.

Modifique un grupo de recursos de host

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 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.

Cómo eliminar hosts dedicados de un grupo de recursos de host

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 de host con otras cuentas de AWS, License Manager elimina automáticamente el host compartido y los consumidores reciben una notificación de expulsión para que trasladen sus instancias desde el host en un plazo de 15 días. Para usar un host dedicado que se ha eliminado de un grupo de recursos de host, consulte [Utilizar hosts dedicados](#) en la Guía del usuario de Amazon EC2.

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

1. Inicie sesión en la consola 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.

Elimine un grupo de recursos de host

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 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 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 roles vinculados a servicios de AWS 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 imágenes de máquina de Amazon (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 asociar reglas a estos recursos detectados y realizarles un seguimiento y validarlos igual que hace con las instancias creadas a partir de las AMI administradas.

Contenido

- [Cómo trabajar con la búsqueda en el inventario](#)
- [Detección automatizada en el inventario](#)

Cómo trabajar con la búsqueda en el inventario

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

- [Configuración para la búsqueda en el inventario](#)
- [Uso de la búsqueda en el inventario](#)
- [Cómo añadir reglas de detección automatizada a una licencia autoadministrada](#)
- [Cómo asociar una licencia autoadministrada a la búsqueda en el inventario](#)
- [Cómo desasociar una licencia autoadministrada de un recurso](#)

Configuración para la búsqueda en el 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 de AWS 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.

Uso de la búsqueda en el 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 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.

Recursos de Amazon EC2

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	<ul style="list-style-type: none"> • SQL Server Enterprise • SQL Server Standard • SQL Server Web •

Nombre del filtro	Descripción	Logical operators (Operadores lógicos)	Valores admitidos
			Windows Server Datacenter
Etiqueta	<p>Una clave de etiqueta de metadatos y un valor opcional que se asigna al recurso.</p> <p>Tenga en cuenta que el operador <code>Not equals</code> lógico solo está disponible si está habilitada la detección entre cuentas.</p>	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	<ul style="list-style-type: none">oracle-eeoracle-seoracle-se1oracle-se2db2-sedb2-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	<ul style="list-style-type: none"> • Spatial and Graph • Active Data Guard • Label Security • Oracle On-Line Analytical Processing (OLAP) • Diagnostic Pack and Tuning Pack

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.

Cómo añadir reglas de detección automatizada a una licencia autoadministrada

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 [Detección automatizada en el inventario](#).

Procedimiento para añadir reglas de detección automatizada a una licencia autoadministrada

1. Abra la consola 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 Añadir 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. Seleccione Agregar.

Cómo asociar una licencia autoadministrada a la búsqueda en el 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 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.

Cómo desasociar una licencia autoadministrada 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 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.

Detección automatizada en el inventario

License Manager utiliza [Systems Manager Inventory](#) para detectar el uso de software en las instancias de Amazon EC2 y en las instalaciones. 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 los ID de cuenta de AWS o estén asociadas a etiquetas de recursos para que no se tengan en cuenta para la detección automatizada.

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 [UpdateLicenseConfiguration](#)API. 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 de AWS 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 autoadministrada](#).

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 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.

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 utilizar AWS License Manager para regular el uso de estas licencias y distribuir los derechos de uso, o simplemente derechos, a cuentas específicas de AWS.

Las licencias de datos distribuidas a los productos de AWS Data Exchange están disponibles en la cuenta de AWS a través de AWS 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](#).

Cuando un administrador de licencias distribuye el derecho de una licencia de AWS Marketplace a una cuenta de AWS y el destinatario acepta y activa la licencia concedida, la cuenta de AWS podrá acceder a la suscripción a través de AWS Marketplace. La cuenta también tiene acceso al producto.

Por ejemplo, si un administrador de licencias compra una imagen de máquina de Amazon (AMI) en AWS Marketplace y distribuye un derecho a su cuenta de AWS, puede lanzar instancias de Amazon EC2 desde la AMI mediante AWS Marketplace y Amazon EC2.

Temas

- [Visualización de las licencias concedidas](#)
- [Administre las licencias concedidas](#)
- [Distribuya los derechos](#)
- [Aceptación y activación de concesiones](#)
- [Estado de las licencias](#)
- [Métricas para las cuentas de compradores](#)

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 las licencias concedidas

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 proviene de AWS Marketplace, de si su cuenta es una cuenta miembro de una organización para AWS Organizations y de si todas las características están habilitadas para su organización.

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 de 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 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. Una misma SKU puede existir en varios ISV.
 - Destinatario: el nombre de recurso de Amazon (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 de AWS Marketplace, el estado inicial de la concesión es Aceptación pendiente. Haga 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 utilizar la visión global de la organización para las licencias concedidas, primero debe vincular AWS Organizations mediante la configuración de la consola AWS License Manager. Para obtener más información, consulte [Configuración de AWS License Manager](#).

Procedimiento para administrar las licencias concedidas de todas las cuentas en AWS Organizations

1. Abra la consola 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. Una misma SKU puede existir en varios ISV.
 - 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 que no sea 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 utilizar 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

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 acerca de AWS Organizations, consulte [Terminología y conceptos de AWS Organizations](#).

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

- Una 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) no anidada, que incluye todas las cuentas de la OU especificada y las OU anidadas en la OU especificada.

Note

Puede crear hasta 2000 concesiones por licencia.

Puede utilizar la consola AWS License Manager o 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, los ARN serán similares a los siguientes:

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 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 ID de Cuenta de AWS, el ID o el ARN de la OU de AWS Organizations, o el ID o ARN de AWS Organizations 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 AWS CLI para distribuir un derecho. Debe especificar un ID u OU de la organización en formato ARN cuando utilice la API de AWS License Manager.

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 concesiones

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 Deshabilitado. Las concesiones aceptadas y activadas tienen el estado Activo.

Tip

Puede aceptar automáticamente concesiones que procedan de la cuenta de administración de su organización. Para habilitar la aceptación automática de las concesiones, vincule las cuentas de su organización en la página [Configuración](#) de la consola AWS License Manager desde la cuenta de administración.

No puede activar dos licencias para el mismo producto de 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 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 concesión procedente de AWS Marketplace, es posible que se le presente la opción de sustituir las concesiones 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 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. Una Cuenta de AWS especificada
 - 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 utilizar AWS CLI para trabajar con las licencias concedidas.

Procedimiento para trabajar con concesiones distribuidas utilizando AWS CLI

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

Estado de las licencias

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
AVAILABLE	La licencia está disponible para su uso y uso compartido.

Estado	Descripción
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 desactivado.
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.
FAILED_WORKFLOW	No se pudo distribuir la concesión.
DELETED	El concedente ha eliminado la concesión.

Estado	Descripción
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.

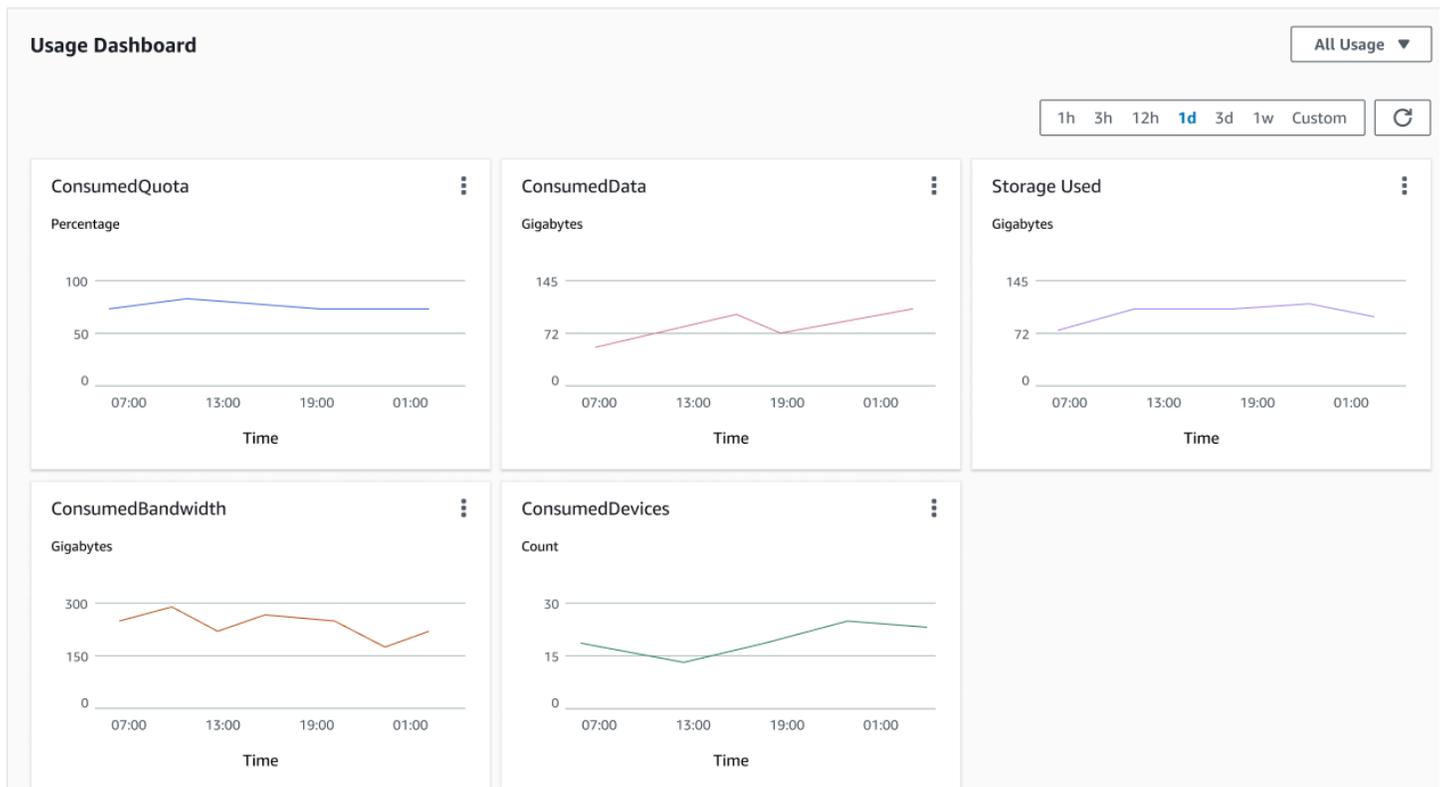
Métricas para las cuentas de compradores

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 métrica de CloudWatch en la cuenta del vendedor, la cuenta del comprador raíz y la cuenta en la que se está registrando el uso. Las cuentas de comprador son las Cuentas de AWS que han adquirido o a las que se les ha concedido una licencia emitida 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 relación con una licencia de una cuenta de comprador, la cuenta en la que se registra el uso y la cuenta del comprador raíz ven un widget de CloudWatch con registros de uso en la página Panel de uso de la consola 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 (ISV) pueden utilizar AWS License Manager para administrar y distribuir licencias de software a los usuarios finales. Como emisor, puede realizar un seguimiento centralizado del uso de las licencias emitidas por el vendedor mediante el panel 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 claves asimétricas de AWS KMS 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 los clientes mediante una identidad de AWS IAM o mediante tokens al portador generados por License Manager. Los clientes que dispongan de una cuenta de AWS pueden redistribuir las concesiones de derechos de las licencias entre las identidades de AWS de sus respectivas organizaciones. 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.

Concesiones de derechos

License Manager recoge las capacidades de la licencia como concesiones de derechos de 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

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 serie temporal a través de CloudWatch Events.

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.

Requisitos

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 cuenta de AWS puedan consumir licencias vendidas fuera de AWS Marketplace, debe crear un rol que permita a su aplicación de software llamar a la API de License Manager. Por ejemplo, puede utilizar AWS CLI. En primer lugar, utilice el comando [create-role](#) para crear un rol denominado `AWSLicenseManagerConsumptionRole`.

```
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
```

Lo siguiente es `trust-policy-document.json`.

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

A continuación, utilice el comando [attach-role-policy](#) para agregar la política administrada `AWSLicenseManagerConsumptionPolicy` de AWS al rol `AWSLicenseManagerConsumptionRole`.

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

Cómo crear licencias emitidas por el vendedor

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 API [CreateLicense](#).

Procedimiento para crear una licencia mediante la consola

1. Abra la consola 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 principal: la AWS Region 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:
 - Ingresar una clave de AWS KMS: License Manager utiliza esta clave para firmar y verificar al emisor. Para obtener más información, consulte [Firma criptográfica de licencias](#).
 - 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.

Concesión de licencias a los clientes

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 cuenta de AWS, 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 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.
 - ID de cuenta de AWS: el número de cuenta de AWS 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 cuentas de AWS.
 - Seleccione Permitir la generación de tokens en las instalaciones para autenticar las licencias compartidas sin utilizar ni credenciales ni identidades de AWS.
 - 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 principal: la Región de AWS de la licencia.
6. Seleccione Crear concesión.

Cómo obtener credenciales temporales para clientes sin cuenta de AWS

En el caso de los clientes que no tienen cuenta de AWS, puede utilizar los derechos de la misma manera que lo hace con los clientes que sí tienen cuenta de AWS. Utilice el siguiente procedimiento para obtener credenciales temporales de AWS para sus clientes sin cuenta de AWS. 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. Llame a la acción [CreateToken](#) de la API para obtener un token actualizado y cifrado como token JWT.
2. Llame a la acción [GetAccessToken](#) de la API y especifique el token actualizado que recibió de CreateToken en el paso anterior para recibir un token de acceso temporal.
3. Llame a la acción [AssumeRoleWithWebIdentity](#) de la API y especifique el token de acceso que recibió de GetAccessToken en el paso anterior, así como el rol AWSLicenseManagerConsumptionRole que creó, para obtener credenciales temporales de AWS.

Procedimiento para crear un token desde la consola AWS License Manager

1. Desde la [consola License Manager](#), vaya a la página de detalles de la licencia correspondiente al derecho de licencia específico que desee utilizar sin una cuenta de AWS.
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.

Consumo de licencias

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. Una misma SKU puede existir en varios ISV. Por lo tanto, las huellas digitales clave de confianza desempeñan un papel importante.

`1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0daEJEMPLO`, 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:** los ISV de software como servicio (SaaS) pueden retirar licencias en nombre de un cliente si incluyen 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.

Cómo eliminar licencias emitidas por el vendedor

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. Si lo desea, también puede eliminar la licencia mediante la acción [DeleteLicense](#) de la API.

Procedimiento para eliminar una licencia mediante la consola

1. Abra la consola 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.

Suscripciones basadas en usuarios en License Manager

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 imágenes de máquina de Amazon (AMI) 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, debe asociar los usuarios de [AWS Directory Service for Microsoft Active Directory](#) (AWS Managed Microsoft AD), bien de su dominio autoadministrado (en las instalaciones), a las instancias de EC2 que proporcionan el software. Para que el software con licencia esté disponible, debe crear suscripciones basadas en usuarios y asociarlas a instancias lanzadas desde AMI preconfiguradas. [AWS Systems Manager](#) configurará y endurecerá 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 para instancias reservadas de Amazon EC2 y Savings Plan pueden ayudarle a optimizar los costos de Amazon EC2. 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.

Contenido

- [Requisitos previos](#)
- [Consideraciones](#)
- [Software para suscripciones basadas en usuarios](#)
 - [Software compatible para suscripciones basadas en usuarios](#)
 - [Microsoft Visual Studio](#)
 - [Microsoft Office](#)
 - [Lanzamiento desde una AMI compatible](#)
 - [Software adicional](#)
- [Introducción a las suscripciones basadas en usuarios](#)
 - [Paso 1: Configure AWS Directory Service for Microsoft Active Directory y su nube privada virtual \(VPC\)](#)
 - [Paso 2: Suscríbase a un producto](#)
 - [Paso 3: Lance una instancia para proporcionar suscripciones basadas en usuarios](#)
 - [Paso 4: Asocie los usuarios a una instancia de suscripción basada en usuarios](#)
 - [Paso 5: Conéctese a una instancia de suscripción basada en usuarios](#)
- [Modificación de la configuración del directorio para las suscripciones basadas en usuarios](#)

- [Modificación de la configuración de la VPC para las suscripciones basadas en usuarios](#)
- [Desasociación de usuarios a suscripciones basadas en usuarios](#)
- [Cancelación de la suscripción de los usuarios a las suscripciones basadas en usuarios](#)
- [Interrupción de las instancias de EC2 que proporcionan suscripciones basadas en usuarios](#)
- [Procedimiento para eliminar un directorio de suscripciones basadas en usuarios](#)
- [Solución de problemas de suscripciones basadas en usuarios](#)
 - [Solución de problemas de conformidad de instancias](#)
 - [Solución de problemas de conformidad de licencias](#)
 - [Solución de problemas de conectividad de instancias](#)
 - [Solución de problemas a la hora de unirse al dominio](#)
 - [Solución de problemas de conectividad de Systems Manager](#)
 - [Solución de problemas de Systems Manager Run Command](#)

Requisitos previos

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

- 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 sección Suscripciones basadas en usuarios de la consola License Manager aparecerá un mensaje único en el que podrá aceptar conceder permiso a License Manager para crear el rol vinculado al servicio requerido. Tras conceder permiso a License Manager, elija Crear para crear el rol vinculado al servicio. Para obtener más información, consulte [Uso de roles vinculados a servicios de AWS License Manager](#).
- Debe haber creado un AWS Managed Microsoft AD directorio. AWS Managed Microsoft AD no se admiten los directorios que se han compartido. 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.
- Debe asociar los usuarios a su AWS Managed Microsoft AD directorio o a un Active Directory autogestionado para utilizar las suscripciones basadas en usuarios.
 - Para asociar usuarios AWS Managed Microsoft AD, debe aprovisionar los usuarios de 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 .

- Para asociar usuarios en el directorio autogestionado, debe establecer una relación de confianza bidireccional entre bosques entre el directorio autogestionado y el directorio de 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 autogestionado de Active Directory](#) en la Guía de AWS Directory Service administración.
- Las subredes que están configuradas para su directorio deben ser todas de la misma VPC que la suya. Cuenta de AWS
- El acceso de salida a Internet desde las instancias que proporcionan suscripciones basadas en usuarios, o [puntos de conexión de VPC](#), debe estar configurado para que las instancias se comuniquen con AWS Systems Manager. Para obtener más información, consulte [Configuración de Systems Manager para instancias de EC2](#) en la Guía del usuario de AWS Systems Manager .
- 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 de salida a la dirección IPv4 de la interfaz de red de cada controlador de dominio, o bien al grupo de seguridad utilizado por los controladores de dominio. Para obtener más información, consulte [Paso 1: Configure AWS Directory Service for Microsoft Active Directory y su nube privada virtual \(VPC\)](#) 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. El grupo de seguridad que seleccione también debe permitir el tráfico necesario a la dirección IPv4 o al grupo de seguridad de la interfaz de red 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.

- Debe configurar el reenvío de DNS para cualquier VPC adicional a la AWS Managed Microsoft AD que registre para las suscripciones basadas en usuarios. Puede utilizar Amazon Route 53 o cualquier otro servicio 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”](#).
- Si se suscribe a Microsoft Office con suscripciones basadas en usuarios, debe hacer lo siguiente:
 - 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](#).

- 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.
- Identifique o cree un grupo de seguridad para los puntos de conexión de VPC que permita la conectividad de entrada del puerto TCP 1688. Este grupo de seguridad se especificará al configurar los ajustes de la nube privada virtual. Para obtener más información, consulte [Trabajar con grupos de seguridad](#). License Manager asociará este grupo de seguridad a los puntos de conexión de VPC que cree por usted 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 .
- Identifique o cree un grupo de seguridad para las instancias lanzadas a fin de proporcionar suscripciones basadas en usuarios que permitan la conectividad de entrada del puerto TCP 3389 desde las fuentes de conexión aprobadas. El grupo de seguridad también debe permitir que la conectividad de salida del puerto TCP 1688 llegue a los puntos de conexión de VPC. Para obtener más información, consulte [Trabajar con grupos de seguridad](#).

Si se está preparando para usar suscripciones basadas en usuarios por primera vez, complete los requisitos previos enumerados y consulte [Introducción a las suscripciones basadas en usuarios](#). Si ya ha configurado las suscripciones basadas en usuarios y desea añadir estos productos a AWS Managed Microsoft AD y configurar la VPC para los productos de Microsoft Office, complete los requisitos previos enumerados y consulte [Modificación de la configuración del directorio para las suscripciones basadas en usuarios](#).

- 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 .

Warning

Las instancias que proporcionan suscripciones basadas en usuarios deben gestionarse por sí mismas para que estén AWS Systems Manager en buen estado. Además, las instancias deben poder activar sus licencias de suscripción basadas en usuarios y garantizar la conformidad tras la activación de las licencias. 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 [Solución de problemas de suscripciones basadas en usuarios](#) de esta guía.

- Para crear suscripciones basadas en usuarios, su usuario o rol debe tener los siguientes permisos:
 - `ec2:CreateNetworkInterface`
 - `ec2>DeleteNetworkInterface`
 - `ec2:DescribeNetworkInterfaces`
 - `ec2:CreateNetworkInterfacePermission`
 - `ec2:DescribeSubnets`
 - `ds:DescribeDirectories`
 - `ds:AuthorizeApplication`
 - `ds:UnauthorizeApplication`
 - `ds:GetAuthorizedApplicationDetails`
 - `ds:DescribeDomainControllers`
- 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`

Consideraciones

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

- Las licencias Win Remote Desktop Services SAL no se pueden utilizar por separado de los productos de suscripción basada en usuarios compatibles.
- Las instancias que ofrecen suscripciones basadas en usuarios admiten hasta dos sesiones de usuario activas a la vez.
- Al crear usuarios locales con privilegios de administrador en instancias que proporcionan suscripciones basadas en usuarios, es posible que la instancia pase a estar 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](#).

- 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. Para obtener más información, consulte [Desasociación de usuarios a suscripciones basadas en usuarios](#).
- Al configurar el directorio con productos de Microsoft Office, la VPC debe tener [puntos de conexión de VPC](#) aprovisionados en al menos una subred. Si desea eliminar todos los recursos de puntos de conexión de VPC creados por License Manager, debe realizar lo siguiente:
 - Desasocie a todos los usuarios de sus suscripciones basadas en usuarios. Para obtener más información, consulte [Desasociación de usuarios a suscripciones basadas en usuarios](#).
 - Elimine cualquier directorio que se haya configurado desde los ajustes de License Manager. Para obtener más información, consulte [Procedimiento para eliminar un directorio de suscripciones basadas en usuarios](#).
 - Termine todas las instancias que proporcionen productos de suscripción basada en usuarios. Para obtener más información, consulte [Interrupción de las instancias de EC2 que proporcionan suscripciones basadas en usuarios](#).
- La clave de la etiqueta `AWSLicenseManager` con el valor `UserSubscriptions` asignado por License Manager a sus instancias no debe modificarse ni eliminarse.
- Las dos interfaces de redes elásticas (ENI) creadas para License Manager no deben modificarse ni eliminarse para que el servicio funcione.
- 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 [Solución de problemas de suscripciones basadas en usuarios](#) de esta guía.

Software para suscripciones basadas en usuarios

AWS License Manager admite suscripciones basadas en usuarios para Microsoft Visual Studio y Microsoft Office. 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. License Manager

hará un seguimiento del uso del software compatible. Para obtener más información, consulte [Introducción a las suscripciones basadas en usuarios](#).

Plataformas de sistema operativo (SO) compatibles con Windows

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

- 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 Visual Studio es un entorno de desarrollo integrado (IDE) que permite a los desarrolladores crear, editar, depurar y publicar aplicaciones. Las AMI de Microsoft Visual Studio proporcionadas incluyen [AWS Toolkit for .NET Refactoring](#) y [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

Lanzamiento desde una AMI compatible

Al lanzar una instancia desde una AMI compatible con Office LTSC Professional Plus Microsoft Visual Studio, el lanzamiento 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 lanzarlo con una versión anterior de la plataforma del sistema operativo, siga estos pasos.

1. Abre la AWS Marketplace consola en <https://console.aws.amazon.com/marketplace>.
2. Elija Administrar suscripciones del panel de navegación.
3. Para optimizar los resultados de la suscripción, puedes buscar todo el nombre de la suscripción o parte de él. 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.

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 de administrador que se crea de forma predeterminada en su AWS Managed Microsoft AD 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 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 [Introducción a las suscripciones basadas en usuarios](#).

Introducción a las suscripciones basadas en usuarios

En los siguientes pasos 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 [Requisitos previos](#).

Si ya ha configurado el AWS Managed Microsoft AD directorio para las suscripciones basadas en usuarios y también desea utilizar Microsoft Office, consulte [Modificación de la configuración de la VPC para las suscripciones basadas en usuarios](#).

Pasos

- [Paso 1: Configure AWS Directory Service for Microsoft Active Directory y su nube privada virtual \(VPC\)](#)
- [Paso 2: Suscríbase a un producto](#)

- [Paso 3: Lance una instancia para proporcionar suscripciones basadas en usuarios](#)
- [Paso 4: Asocie los usuarios a una instancia de suscripción basada en usuarios](#)
- [Paso 5: Conéctese a una instancia de suscripción basada en usuarios](#)

Paso 1: Configure AWS Directory Service for Microsoft Active Directory y su nube privada virtual (VPC)

License Manager es necesario AWS Managed Microsoft AD para asociar los usuarios a las suscripciones basadas en usuarios. Debe seleccionar todos los productos que necesite para las suscripciones basadas en usuarios al configurar su directorio, ya que los usuarios solo pueden suscribirse a los productos configurados. <directory_id>Cuando registre su AWS Managed Microsoft AD directorio, License Manager creará dos interfaces de red elásticas (ENI) para que el servicio se comunique con su directorio con una descripción similar a la interfaz de red para LicenseManager la que AWS se creó.

Important

Debe permitir que License Manager cree el [rol vinculado al servicio](#) requerido para poder continuar. Para obtener más información, consulte [Requisitos previos](#).

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 cualquier VPC adicional a la que AWS Managed Microsoft AD registre para las suscripciones basadas en usuarios. Si tiene varias suscripciones basadas en usuarios Regiones de AWS, cada región debe tener la suya propia, AWS Managed Microsoft AD con el reenvío de DNS configurado de la siguiente manera.

Puede utilizar uno de los métodos siguientes para configurar el entorno para las suscripciones basadas en usuarios.

Console (Active Directory)

AWS Managed Microsoft AD Para configurar las suscripciones basadas en usuarios (consola)

1. Abra la consola License Manager en <https://console.aws.amazon.com/license-manager/>.
2. Vaya a la página de Configuración seleccionando Configuración en el panel de navegación izquierdo o seleccionando Abrir configuración en el banner.
3. En la página Configuración, en la sección AWS Managed Microsoft AD, seleccione Configurar.
4. Para el nombre e ID del directorio administrado por AWS , elija el directorio que contenga los usuarios para los que desea crear suscripciones basadas en usuarios.
5. Para Nombre e ID del producto, seleccione los productos correspondientes y, a continuación, seleccione Configurar.

Después de seleccionar Configurar, la sección AWS Managed Microsoft AD de la página Configuración mostrará el ID de directorio con el Estado como Configurando. Una vez finalizado el proceso de configuración, el Estado aparecerá como Configurado y podrá continuar con los pasos restantes.

Console (Active Directory and VPC)

AWS Managed Microsoft AD Para configurar las suscripciones basadas en usuarios (consola)

1. Abra la consola License Manager en <https://console.aws.amazon.com/license-manager/>.
2. Vaya a la página de Configuración seleccionando Configuración en el panel de navegación izquierdo o seleccionando Abrir configuración en el banner.
3. En la página Configuración, en la sección AWS Managed Microsoft AD, seleccione Configurar.
4. Para el nombre e ID del directorio administrado por AWS , elija el directorio que contenga los usuarios para los que desea crear suscripciones basadas en usuarios.
5. Para Nombre e ID del producto, seleccione los productos correspondientes.
6. Para la Nube virtual privada, elija una VPC para acceder a opciones de configuración adicionales.
7. En el caso de Subredes para vpc-**x**, elija al menos una subred en la que aprovisionar los puntos de conexión de VPC.

8. En el caso de Grupos de seguridad para vpc-**x**, elija el grupo de seguridad que creó para asociarlo a los puntos de conexión de la VPC y, a continuación, seleccione Configurar.

Después de seleccionar Configurar, las secciones AWS Managed Microsoft AD y Nube virtual privada de la página Configuración mostrarán el ID de directorio y el ID de VPC con el Estado como Configurando. Una vez finalizado el proceso de configuración, cada Estado aparecerá como Configurado y podrá continuar con los pasos restantes.

AWS CLI

AWS Managed Microsoft AD Para configurar las suscripciones basadas en usuarios ()AWS CLI

Puede registrarlo AWS Managed Microsoft AD como proveedor de identidad para las suscripciones basadas en usuarios con esta operación. [RegisterIdentityProvider](#)

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

Para configurar AWS Managed Microsoft AD su VPC para suscripciones basadas en usuarios ()AWS CLI

Puede registrarlo AWS Managed Microsoft AD como proveedor de identidades y configurar su VPC para suscripciones basadas en usuarios con esta operación. [RegisterIdentityProvider](#)

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

Para obtener más información acerca de los productos de software disponibles, consulte [Software para suscripciones basadas en usuarios](#).

Paso 2: Suscríbase a un producto

Para suscribirse a los productos configurados en el AWS Marketplace

Después de configurar el directorio con los productos correspondientes, es posible que también tenga que suscribirse a los productos correspondientes. Los productos con un Estado de suscripción

de Marketplace Inactivo requieren que se suscriba antes de poder asociar usuarios a una instancia y utilizarlos.

Su cuenta debe contar con una suscripción a Windows Server Remote Desktop Services Subscriber Access License (RDS SAL). Remote Desktop Services (RDS) de Microsoft, conocido como Terminal Services en Windows Server 2008 y versiones anteriores, es uno de los componentes de Microsoft Windows que permiten al usuario tomar el control de un equipo remoto o una máquina virtual a través de una conexión de red. RDS permite a los usuarios acceder de forma remota a escritorios gráficos y aplicaciones de Windows.

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.

 Note

Las licencias RDS SAL no se pueden utilizar por separado de los productos de suscripción basada en usuarios compatibles. Para obtener más información, consulte [Consideraciones](#).

Puedes suscribirte a tus productos directamente AWS Marketplace en los siguientes enlaces:

- [Visual Studio Professional](#)
- [Visual Studio Enterprise](#)
- [Office LTSC Professional Plus 2021](#)
- [Win Remote Desktop Services SAL](#)

Procedimiento para conocer y suscribirse a productos desde la consola License Manager

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

1. Abra la consola 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. Selecciona 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 correspondientes tengan una suscripción activa, puede continuar con la suscripción de los usuarios a los productos.

Note

En el caso de los períodos de facturación que no se hayan cerrado en AWS Billing(marcados como Pendiente), la factura estimada por los cargos relacionados con el número de usuarios y los costos asociados tardará 48 horas en aparecer. Para obtener más información, consulte [Visualización de su factura](#) en la Guía del usuario de AWS Billing .

Paso 3: Lance una instancia para proporcionar 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. Una vez que lance una instancia, AWS Systems Manager intentará unirla al dominio y realizar una configuración y un endurecimiento adicionales en el 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 terminarán. Para obtener más información, consulte [Requisitos previos](#) y [Solución de problemas de suscripciones basadas en usuarios](#).

Procedimiento de lanzamiento de una instancia para proporcionar suscripciones basadas en usuarios

1. Abra la consola Amazon EC2 en <https://console.aws.amazon.com/ec2/>.

2. En Imágenes, seleccione Catálogo de AMI.
3. Seleccione AMI de AWS Marketplace .
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 entre la instancia y el AWS Managed Microsoft AD directorio.
 - 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.

Una vez que tenga las instancias en ejecución de la AWS Marketplace AMI, debe suscribir a los usuarios al producto y asociarlos a las instancias que proporcionan el producto para que puedan utilizarlo.

Paso 4: Asocie los usuarios a una instancia de suscripción basada en usuarios

Una vez que se haya suscrito a la AWS Marketplace AMI del producto correspondiente, podrá 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 creará una suscripción para cada usuario al que se suscriba al producto.

Note

Cada usuario debe contar con una suscripción a Windows Server Remote Desktop Services Subscriber Access License (RDS SAL) y al producto que vaya a utilizar. Cuando su cuenta

se haya suscrito a RDS SAL como se detalla en [Paso 2: Suscríbese a un producto](#), el usuario se suscribirá a RDS SAL por usted cuando se suscriba a un producto de suscripción basado en usuarios.

La página Productos de License Manager mostrará las suscripciones activas y el Estado de suscripción de Marketplace como Activo. En la página de detalles del producto, License Manager mostrará las suscripciones de usuario activas con el Estado Suscrito.

Important

Si su directorio no está configurado con el producto, aparecerá una barra de notificaciones en la parte superior de la consola en la que se le indicará que ajuste 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 contar con 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

Puede suscribir usuarios a un producto y asociación a una instancia con el siguiente proceso.

Procedimiento de suscripción y asociación de usuarios a una instancia

1. Abra la consola 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, seleccione Suscripción y asociación de usuarios.
4. Especifique hasta cinco nombres de usuario que existan en el directorio, incluido el Nombre de dominio si se encuentran en un dominio de confianza, y seleccione Suscribirse y asociar.

En la página Asociación de usuarios, los usuarios que haya seleccionado deben mostrarse en Usuarios con el Estado de asociación Asociado. Además, en la página Productos, puede revisar la

página de detalles del producto seleccionando el Nombre del producto. Los usuarios suscritos se mostrarán en Usuarios con el Estado Suscrito.

Suscripción de usuarios a un producto

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

Console

Procedimiento de suscripción de usuarios a un producto (consola)

1. Abra la consola 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 y seleccione Suscribir usuario.
4. Especifique hasta cinco nombres de usuario que existan en el directorio, incluido el Nombre de dominio si se encuentran en un dominio de confianza, y seleccione Suscribir.

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

AWS CLI

Procedimiento de suscripción de usuarios a un producto (AWS CLI)

Puede suscribir usuarios a un producto que esté registrado con su proveedor de identidades mediante la operación [StartProductSubscription](#).

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

Procedimiento de suscripción de usuarios a un producto con Active Directory autogestionado (AWS CLI)

Puede suscribir a los usuarios de su Active Directory autogestionado a un producto que esté registrado en su AWS Managed Microsoft AD directorio mediante esta operación.

[StartProductSubscription](#)

```
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 [Software para suscripciones basadas en usuarios](#).

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

Asociación de usuarios a una instancia

Puede asociar usuarios a una instancia mediante alguno de los métodos siguientes.

Important

Antes de asociar un producto a una instancia, primero debe suscribir a los usuarios a los productos.

Console

Procedimiento de asociación de usuarios a una instancia (consola)

1. Abra la consola 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, seleccione Asociar usuarios.
4. Especifique hasta cinco nombres de usuario que existan en el directorio, incluido el Nombre de dominio si se encuentran en un dominio de confianza, y seleccione Asociar.

En la página Asociación de usuarios, los usuarios que haya seleccionado deben mostrarse en Usuarios con el Estado de asociación Asociado.

AWS CLI

Procedimiento de asociación de usuarios a una instancia (AWS CLI)

Puede asociar usuarios a una instancia lanzada para proporcionar la suscripción basada en usuarios mediante la operación [AssociateUser](#).

```
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 usuarios de Active Directory autogestionado a una instancia lanzada para proporcionar la suscripción basada en usuarios mediante la operación [AssociateUser](#).

```
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 [Software para suscripciones basadas en usuarios](#).

En la página Asociación de usuarios, los usuarios que haya seleccionado deben mostrarse en Usuarios con el Estado de asociación Asociado.

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

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 utilizar el producto con su identidad asociada.

Important

El proceso de crear la instancia de EC2 y prepararla para los usuarios puede tardar unos 20 minutos. El Estado de la 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 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.

Modificación de la configuración del directorio para las suscripciones basadas en usuarios

Puede añadir o eliminar productos para suscripciones basadas en usuarios del directorio configurado en la página de configuración de License Manager. Los pasos serán diferentes si utiliza productos de Microsoft Office, ya que License Manager debe crear [puntos de conexión de VPC](#) para estas suscripciones.

Procedimiento de modificación de la configuración del directorio sin productos de Microsoft Office

1. Abra la consola License Manager en <https://console.aws.amazon.com/license-manager/>.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página Configuración, en la sección AWS Managed Microsoft AD, seleccione Editar.
4. Para Nombre e ID del producto, seleccione productos adicionales y borre las selecciones anteriores según sea necesario; después, seleccione Guardar cambios.

Procedimiento de modificación de la configuración del directorio con productos de Microsoft Office

1. Abra la consola License Manager en <https://console.aws.amazon.com/license-manager/>.
2. Vaya a la página de Configuración seleccionando Configuración en el panel de navegación izquierdo o seleccionando Abrir configuración en el banner.
3. En la página Configuración, en la sección AWS Managed Microsoft AD, seleccione Editar.
4. Para Nombre e ID del producto, seleccione los productos correspondientes, incluidos los de Microsoft Office.
5. Para la Nube virtual privada, elija una VPC para acceder a opciones de configuración adicionales.

6. En el caso de Subredes para vpc-**x**, elija al menos una subred en la que aprovisionar los puntos de conexión de VPC.
7. En el caso de Grupos de seguridad para vpc-**x**, elija el grupo de seguridad que creó para asociarlo a los puntos de conexión de la VPC y, a continuación, seleccione Guardar cambios.

Después de seleccionar Guardar cambios, las secciones AWS Managed Microsoft AD y Nube virtual privada de la página Configuración mostrarán el ID de directorio y el ID de VPC con el Estado como Configurando. Debe esperar a que el directorio tenga el Estado Configurado y la VPC tenga el Estado Activo antes de usar suscripciones basadas en usuarios con Microsoft Office.

Modificación de la configuración de la VPC para las suscripciones basadas en usuarios

Si ha agregado productos de Microsoft Office, puede modificar la configuración de la VPC. License Manager creará [puntos de conexión de VPC](#) por usted en las subredes que especifique para que sus recursos lleguen a los servidores de activación y garanticen su conformidad. Debe especificar al menos una subred. Para obtener más información, consulte [Requisitos previos](#).

Note

La configuración de la VPC solo se puede modificar si el directorio se ha configurado con productos de Microsoft Office. Para obtener más información, consulte [Introducción a las suscripciones basadas en usuarios](#).

Si desea eliminar todos los puntos de conexión de VPC, consulte [Consideraciones](#).

Procedimiento de modificación de la configuración del directorio

1. Abra la consola License Manager en <https://console.aws.amazon.com/license-manager/>.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página Configuración, en la sección Nube virtual privada configurada, seleccione Editar.
4. Cambie las subredes y el grupo de seguridad según sea necesario para la VPC configurada y, a continuación, seleccione Guardar cambios.

Desasociación de usuarios a suscripciones basadas en usuarios

Puede desasociar los usuarios a una instancia para eliminar el acceso al recurso.

Note

La eliminación de un usuario del directorio no alterará las asociaciones ni las suscripciones de los usuarios. Debe desasociar el usuario en License Manager, desde la página de detalles del producto, para eliminar su asociación con una instancia.

Procedimiento de desasociación de los usuarios a suscripciones basadas en usuarios

1. Abra la consola 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.

Cancelación de la suscripción de los usuarios a las suscripciones basadas en usuarios

Puede cancelar la suscripción de los usuarios a un producto para eliminar el acceso y dejar de incurrir en cargos por el producto y esos usuarios.

Important

Primero debe desasociar al usuario de las instancias a las que esté asociado actualmente para poder cancelar la suscripción.

Procedimiento de cancelación de la suscripción de los usuarios a las suscripciones basadas en usuarios

1. Abra la consola 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.

Interrupción de las instancias de EC2 que proporcionan suscripciones basadas en usuarios

Puede eliminar una instancia que proporcione una suscripción basada en usuarios si ya no la necesita. Esto se denomina terminar la instancia. En primer lugar, debe desasociar a todos los usuarios de la instancia y, a continuación, terminar la instancia desde la consola de Amazon EC2.

Note

Los usuarios deben haberse desasociado de la instancia para dejar de incurrir en cargos por la suscripción. Para obtener más información, consulte [Desasociación de usuarios a suscripciones basadas en usuarios](#).

Procedimiento para identificar y terminar las instancias que proporcionan suscripciones basadas en usuarios

1. Abra la consola 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, seleccione el ID de la instancia para acceder a la página de detalles de la instancia.
4. Anote el ID de instancia, ya que lo necesitará para terminar la instancia.
5. Desasocie a todos los usuarios de la instancia.
6. Siga los pasos que se indican en [Terminar una instancia](#).

Procedimiento para eliminar un directorio de suscripciones basadas en usuarios

Puede eliminar el directorio si ya no desea utilizarlo para suscripciones basadas en usuarios. Al eliminar la configuración del directorio de License Manager, no se elimina el directorio en sí. Al eliminar el directorio, no podrá asociar usuarios del directorio a las suscripciones basadas en usuarios.

Important

Primero debe desasociar a los usuarios y terminar las instancias que proporcionan suscripciones basadas en usuarios antes de poder eliminar el directorio de License Manager.

Procedimiento para eliminar un directorio

1. Abra la consola License Manager en <https://console.aws.amazon.com/license-manager/>.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, en la AWS Managed Microsoft AD sección, elija Eliminar.
4. Introduzca el texto necesario para confirmar que desea eliminar el directorio y seleccione Eliminar.

Después de seleccionar Eliminar, la sección AWS Managed Microsoft AD de la página Configuración mostrará el ID de directorio con el Estado como Configurando. Una vez finalizado el proceso de configuración, se debe eliminar el directorio de la sección AWS Managed Microsoft AD.

Solución de problemas de suscripciones basadas en usuarios

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

Contenido

- [Solución de problemas de conformidad de instancias](#)
- [Solución de problemas de conformidad de licencias](#)
- [Solución de problemas de conectividad de instancias](#)

- [Solución de problemas a la hora de unirse al dominio](#)
- [Solución de problemas de conectividad de Systems Manager](#)
- [Solución de problemas de Systems Manager Run Command](#)

Solución de problemas de conformidad de 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 [Requisitos previos](#).

Solución de problemas de conformidad de licencias

Si configuró su directorio para proporcionar suscripciones basadas en usuarios con Microsoft Office, debe asegurarse de que los recursos puedan conectarse a los puntos de conexión 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?](#)

Solución de problemas de conectividad de instancias

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

Solución de problemas a la hora de unirse al dominio

Los usuarios deben poder conectarse a las instancias que proporcionan los productos de suscripción basada en usuarios con sus identidades de usuario desde el directorio 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.

Solución de problemas de conectividad de Systems Manager

Las instancias que ofrecen suscripciones basadas en usuarios deben gestionarse por AWS Systems Manager , de lo 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 .

Suscripciones de Linux en License Manager

AWS License Manager le ofrece la posibilidad de ver y administrar suscripciones comerciales de Linux que posea y ejecute en AWS. Puede hacer un seguimiento del uso de las licencias en Regiones de AWS y las cuentas de AWS Organizations. Una vez que se hayan detectado y agregado los datos, dispondrá de información sobre todas las instancias que utilicen suscripciones comerciales de Linux. Además, los datos detectados sobre suscripciones se mostrarán en la consola License Manager como paneles de Amazon CloudWatch. Si sus cuentas están en Organizations, puede registrar una cuenta miembro como administrador delegado para las tareas administrativas. Para obtener más información, consulte [Administradores delegados](#).

Realiza un seguimiento del uso de varias suscripciones, como:

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

Las suscripciones de Linux utilizan 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 las suscripciones de 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 presentará en la siguiente emisión métrica. Este comportamiento puede retrasar la visualización de los recursos, como las instancias comerciales de Linux en EC2 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 detectados los recursos, las métricas de Amazon CloudWatch se emiten cada hora para los datos sobre suscripciones de Linux.

Contenido

- [Administración de la detección de suscripciones de Linux](#)
 - [Habilitación de la detección de suscripciones de Linux](#)
 - [Motivos de los distintos estados de detección de los recursos](#)
 - [Deshabilitación de la detección de suscripciones de Linux](#)
- [Visualización de los datos de las instancias detectadas](#)
 - [Visualización de los datos de todas las instancias](#)
 - [Visualización de los datos de las instancias por suscripción](#)
- [Información de facturación de las suscripciones de Linux](#)
- [Métricas de uso y alarmas de Amazon CloudWatch para suscripciones de Linux](#)
 - [Métricas de uso para suscripciones de Linux](#)

- [Creación de una alarma para las suscripciones de Linux](#)
- [Modificación de una alarma para las suscripciones de Linux](#)
- [Eliminación de una alarma para las suscripciones de Linux](#)

Administración de la detección de suscripciones de Linux

Puede administrar la detección de suscripciones de Linux mediante la consola License Manager. Si habilita la detección de suscripciones de Linux para las Regiones de AWS que especifique, si lo desea, puede extender esta detección a sus cuentas de AWS Organizations. Si ya no quiere realizar un seguimiento de la utilización de suscripciones, también puede deshabilitar la detección.

Note

De forma predeterminada, puede detectar y mostrar hasta 5000 recursos por cuenta y por Región de AWS. Para solicitar un aumento de estos límites, utilice el [formulario de aumento de límites](#).

Temas

- [Habilitación de la detección de suscripciones de Linux](#)
- [Motivos de los distintos estados de detección de los recursos](#)
- [Deshabilitación de la detección de suscripciones de Linux](#)

Habilitación de la detección de suscripciones de Linux

Para permitir la detección de suscripciones de Linux, debe configurar los ajustes necesarios en License Manager. En la página de configuración, puede crear el rol vinculado a servicios, especificar en qué Regiones de AWS desea habilitar la detección y si desea detectar los recursos en sus cuentas de AWS Organizations.

Procedimiento para habilitar la detección de las suscripciones de Linux

1. Abra la consola 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 Configurar.

4. Para Regiones de AWS de origen, elija las regiones en las que desee detectar las suscripciones de Linux.
5. Si desea agregar los datos sobre las suscripciones de sus cuentas de AWS Organizations, seleccione Vincular AWS Organizations.
6. Revise y confirme la opción que concede permisos de AWS License Manager para crear un rol vinculado a servicios para suscripciones de Linux.
7. Seleccione Guardar configuración.

Motivos de los distintos estados de detección de los recursos

AWS License Manager mostrará un estado y el motivo del estado correspondiente para cada una de las 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
- 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.
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.
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 correspondientes.

Estado	Motivo del estado	Descripción
		diente. Cree el rol e inténtelo de nuevo.
	<code>"Region": "Account-Onboard: Failed - An internal error occurred"</code>	La habilitación de las suscripciones de Linux para una sola cuenta no se completó correctamente debido a un error interno.
	<code>"Region": "Org-Onboard: Failed - Account isn't the management account"</code>	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.
	<code>"Region": "Org-Onboard: Failed - Account isn't part of an organization"</code>	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.
	<code>"Region": "Org-Onboard: Failed - Linux subscriptions can't access the organization"</code>	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.

Deshabilitación de la detección de suscripciones de Linux

Puede deshabilitar la detección de suscripciones de Linux desde la página de configuración de AWS License Manager.

Warning

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

Procedimiento para deshabilitar la detección de las suscripciones de Linux

1. Abra la consola 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 [Eliminación de un rol vinculado a servicios para 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](#).

Visualización de los datos de las instancias detectadas

Una vez que se haya completado la detección inicial de recursos, podrá ver las suscripciones de Linux detectadas en la Regiones de AWS que haya seleccionado. Si opta por vincular AWS Organizations, también se agregarán los datos de las cuentas de la organización. Puede ir a la sección Instancias de la consola AWS License Manager para ver una tabla con los datos. Puede ir a la sección Instancias de la consola AWS License Manager para ver una tabla con los datos.

Los datos de cada instancia incluyen lo siguiente:

- ID de instancia: el ID de la instancia
- Tipo de instancia: el tipo de instancia.

- ID de cuenta: el ID de la cuenta propietaria de la instancia.
- Estado: el estado de la instancia.
- Región: la Región de AWS en la que reside la instancia.
- Operación de uso: el funcionamiento de la instancia y el código de facturación asociado a la imagen de máquina de Amazon (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](#).
- ID de AMI: el ID de la AMI utilizada para lanzar la instancia.

Temas

- [Visualización de los datos de todas las instancias](#)
- [Visualización de los datos de las instancias por suscripción](#)

Visualización de los datos de todas las instancias

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 ver los datos detectados para todas las instancias

1. Abra la consola License Manager en <https://console.aws.amazon.com/license-manager/>.
2. En el panel de navegación izquierdo, en Suscripciones de Linux, seleccione Instancias.
3. 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
4. (Opcional) Seleccione Exportar vista a CSV para exportar los datos de todas sus instancias como un archivo de valores separados por comas (CSV).

Visualización de 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 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 quiere 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

Cada suscripción comercial de Linux que se ejecute en Amazon EC2 tendrá la información de facturación asociada a la imagen de máquina de Amazon (AMI). Las suscripciones comerciales de Linux tendrán una operación de uso de Amazon EC2, un código de producto de AWS Marketplace 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 uso de Amazon EC2	Código de producto de AWS Marketplace	Tipo de suscripción
Red Hat Enterprise Linux Server BYOS	RunInstances:00g0	x	Modelo Bring Your Own Subscription (BYOS)
Red Hat Enterprise Linux Server	RunInstances:0010	x	Suscripción a EC2 incluida
Red Hat Enterprise Linux con complemento de alta disponibilidad	RunInstances:1010	x	Suscripción a EC2 incluida
Red Hat Enterprise Linux con SQL Server Standard y alta disponibilidad	RunInstances:1014	x	Suscripción a EC2 incluida
Red Hat Enterprise Linux con SQL Server Enterprise y alta disponibilidad	RunInstances:1110	x	Suscripción a EC2 incluida
Red Hat Enterprise Linux con SQL Server Standard	RunInstances:0014	x	Suscripción a EC2 incluida
Red Hat Enterprise Linux con SQL Server Web	RunInstances:0210	x	Suscripción a EC2 incluida
Red Hat Enterprise Linux con SQL Server Enterprise	RunInstances:0110	x	Suscripción a EC2 incluida

Nombre de la suscripción	Operación de uso de Amazon EC2	Código de producto de AWS Marketplace	Tipo de suscripción
SUSE Linux Enterprise Server	RunInstances:000g	✗	Suscripción a EC2 incluida
Red Hat Enterprise Linux para SAP con alta disponibilidad y servicios de actualización	RunInstances:0010	✓	Suscripción de AWS Marketplace ¹
SUSE Linux Enterprise Server con SAP	✗	✓	Suscripción de AWS Marketplace
Ubuntu Pro	RunInstances:0g00	✓	Suscripción de AWS Marketplace
Red Hat Enterprise Linux Workstation	✗	✓	Suscripción de AWS Marketplace

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

Métricas de uso y alarmas de Amazon CloudWatch para suscripciones de Linux

En la sección Suscripciones de la AWS License Manager consola se enumeran las suscripciones comerciales de Linux detectadas que ha adquirido en AWS o pertenecen al modelo Bring Your Own Subscription (BYOS). En todas las suscripciones comerciales de Linux, las licencias se conceden instancia por instancia.

Los siguientes datos están disponibles para cada suscripción de Linux detectada:

- Nombre de la suscripción
- Tipo de suscripción
- Número de instancias en ejecución por suscripción

- Alarmas de Amazon CloudWatch configuradas

Al elegir una suscripción de Linux en la página de resumen, la pestaña Métricas de uso y alarmas mostrará los datos de esa suscripción. En esta pestaña, se muestran los paneles de Amazon CloudWatch para la suscripción elegida en la consola 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 Métricas de uso y alarmas, cada suscripción tiene una sección de Alarmas en la que se detalla lo siguiente:

- Nombre de alarma: el nombre de la alarma.
- Estado: el estado de la alarma.
- Dimensión: las dimensiones de la alarma. La dimensión incluirá la Región de AWS y el tipo de instancia definido.
- 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 alarmas de CloudWatch con las dimensiones y condiciones que defina a fin de 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.

A continuación se especifican los posibles estados de alarma de CloudWatch:

- 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

- [Métricas de uso para suscripciones de Linux](#)
- [Creación de una alarma para las suscripciones de Linux](#)
- [Modificación de una alarma para las suscripciones de Linux](#)
- [Eliminación de una alarma para las suscripciones de Linux](#)

Métricas de uso para suscripciones de Linux

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

Métrica	Descripción
RunningInstancesCount	<p>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.</p> <p>Unidades: recuento</p> <p>Dimensiones:</p> <p>SubscriptionName : el nombre de la suscripción.</p> <p>Region: la región en la que se detectó el recurso que utilizaba una suscripción comercial de Linux.</p>

Creación de una alarma para las suscripciones de Linux

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

Procedimiento para crear una alarma de CloudWatch para suscripciones de Linux con la consola

1. Abra la consola 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.

Modificación de una alarma para las suscripciones de Linux

Puede modificar las alarmas existentes para adaptarlas a los cambios en los requisitos desde la consola License Manager.

Procedimiento para modificar una alarma de CloudWatch para suscripciones de Linux con la consola

1. Abra la consola 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.

Eliminación de una alarma para las suscripciones de Linux

Puede eliminar las alarmas existentes para adaptarlas a los cambios en los requisitos desde la consola License Manager.

Procedimiento para eliminar una alarma de CloudWatch para suscripciones de Linux con la consola

1. Abra la consola 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 de AWS License Manager

La sección Configuración de la consola AWS License Manager muestra la configuración de la cuenta actual. Debe modificar la configuración para habilitar determinadas funciones, como la distribución de derechos administrados y licencias autoadministradas a su organización, así como para realizar la detección de recursos entre cuentas.

Procedimiento para editar la configuración de License Manager

1. Abra la consola License Manager en <https://console.aws.amazon.com/license-manager/>.
2. En el panel de navegación izquierdo, elija Configuración.
3. Seleccione la pestaña que contenga la configuración que desee aplicar o modificar. Por ejemplo, elija Licencias administradas para configurar los detalles de la cuenta.
4. Seleccione la acción correspondiente a la configuración que desee aplicar o modificar. Por ejemplo, puede elegir Editar o Activar.

Temas de la configuración

- [Licencias administradas](#)
 - [Detalles de cuenta](#)
 - [Detección de recursos entre cuentas](#)
 - [Simple Notification Service \(SNS\)](#)
- [Suscripciones de Linux](#)
- [Suscripciones basadas en usuarios](#)
 - [AWS Managed Microsoft AD](#)
 - [Nube virtual privada](#)
- [Administradores delegados](#)
 - [Regiones admitidas para administradores delegados](#)
 - [Registro de un administrador delegado](#)
 - [Anular el registro de un administrador delegado](#)

Licencias administradas

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 de AWS Organizations están vinculadas, el nombre de recurso de Amazon (ARN) del bucket de S3 de License Manager de la cuenta y el AWS Resource Access Manager ARN compartido de . Esta sección también permite enlazar las cuentas de AWS Organizations.

Para distribuir derechos administrados o licencias autoadministradas en su organización, seleccione Vincular cuentas de 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 recurso compartido de AWS Resource Access Manager en su cuenta de administración, lo que le permite compartir sin problemas las licencias autoadministradas. Para obtener más información, consulte la [Guía del usuario de AWS Resource Access Manager](#).

Para deshabilitar esta opción, llame a la API [UpdateServiceSettings](#).

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 active la detección de recursos entre cuentas, AWS Organizations se 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

Las siguientes Regiones de AWS no requieren Amazon Athena ni AWS Glue para consultar o agregar datos de inventario a fin de que Systems Manager Inventory 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.

Suscripciones de Linux

Puede configurar las suscripciones de Linux para controlar cómo se realizan la detección y la agregación de suscripciones. Puede elegir las regiones para las que desea detectar suscripciones de Linux y si desea agregar los datos de las suscripciones de sus cuentas de AWS Organizations. Para obtener más información, consulte [Suscripciones de Linux en License Manager](#).

Suscripciones basadas en usuarios

Las siguientes configuraciones están disponibles en función de los productos que necesite para las suscripciones basadas en usuarios.

AWS Managed Microsoft AD

License Manager requiere configurar AWS Managed Microsoft AD para poder trabajar con suscripciones basadas en usuarios. Para obtener más información, consulte [Suscripciones basadas en usuarios en License Manager](#).

Nube virtual privada

License Manager requiere que su nube virtual privada (VPC) y AWS Managed Microsoft AD se hayan configurado antes de hacer uso de suscripciones basadas en usuarios con Microsoft Office. Para obtener más información, consulte [Suscripciones basadas en usuarios en License Manager](#).

Administradores delegados

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. Con este enfoque, tendrá un único administrador delegado en su organización para License Manager.

Con AWS CLI o los kits de desarrollo de software (SDK), puede registrar diferentes cuentas miembro de su organización como administrador delegado para cada característica 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 cuenta de AWS a unirse a su organización](#) y [Habilitar el acceso de confianza 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 tiene y ejecuta en Regiones de AWS y sus cuentas de AWS Organizations. También puede crear y administrar alarmas de Amazon CloudWatch para las 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 instancias de EC2 que son propiedad de las cuentas de su organización.

Puede registrar y anular el registro de administradores delegados mediante la [consola AWS License Manager](#), [AWS CLI](#) o [AWS SDK](#).

Regiones admitidas para administradores 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)

Registro de un administrador delegado

Puede registrar un administrador delegado con AWS CLI o AWS Management Console.

Console

Para registrar un administrador delegado mediante la consola AWS License Manager, proceda con los siguientes pasos:

1. Inicie sesión en AWS como administrador de la cuenta de administración.
2. Abra la consola 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 licencias administradas mediante AWS CLI, proceda con los siguientes pasos:

1. Desde la línea de comandos, ejecute el comando siguiente de AWS CLI:

```
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 suscripciones de Linux mediante AWS CLI, proceda con los siguientes pasos:

1. Desde la línea de comandos, ejecute el comando siguiente de AWS CLI:

```
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 delegado

Puede anular el registro de un administrador delegado con AWS CLI o AWS Management Console.

Console

Para anular el registro de un administrador delegado mediante la consola AWS License Manager, proceda con los siguientes pasos:

1. Inicie sesión en AWS como administrador de la cuenta de administración.
2. Abra la consola 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 licencias administradas mediante AWS CLI, proceda con los siguientes pasos:

1. Desde la línea de comandos, ejecute el comando siguiente de 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 suscripciones de Linux mediante AWS CLI, proceda con los siguientes pasos:

1. Desde la línea de comandos, ejecute el comando siguiente de 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 en AWS License Manager

La sección Panel de la consola License Manager proporciona detalles de uso para realizar un seguimiento del consumo de licencias asociado a cada licencia autoadministrada, los derechos de licencia concedidos, los usuarios suscritos a suscripciones basadas en usuarios y las instancias en ejecución. El panel también muestra alertas cuando se producen infracciones de las reglas de licencias.

Información 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.

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.

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 AWS License Manager

Supervise el uso de las licencias y suscripciones controladas en AWS License Manager mediante Amazon CloudWatch. CloudWatch recopila los datos sin procesar y los procesa para convertirlos en métricas legibles casi 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 [Monitoreo del uso de licencias con Amazon CloudWatch](#).

Puede capturar las llamadas a la API y los eventos relacionados realizados por su cuenta o en nombre de su Cuenta de AWS con AWS CloudTrail. Los eventos se capturan como archivos de registros y se distribuyen a un bucket de Amazon S3 especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información, consulte [Registro de llamadas a la API de AWS License Manager mediante AWS CloudTrail](#).

Contenido

- [Monitoreo del uso de licencias con Amazon CloudWatch](#)
 - [Creación de alarmas para supervisar las métricas de Secrets Manager](#)
- [Registro de llamadas a la API de AWS License Manager mediante AWS CloudTrail](#)
 - [Información de License Manager en CloudTrail](#)
 - [Descripción de las entradas del archivo de registros de License Manager](#)

Monitoreo del uso de licencias con Amazon CloudWatch

Puede supervisar las estadísticas de métricas de License Manager mediante 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 más información, consulte la [Guía del usuario de Amazon CloudWatch](#).

License Manager emite las siguientes métricas cada hora en el espacio de nombres `AWSLicenseManager/licenseUsage`:

Métrica	Descripción
RunningInstancesCount	<p>El número total de instancias que se ejecutan en la cuenta corriente y que se agrupan por el nombre de la suscripción.</p> <p>Unidades: recuento</p> <p>Dimensiones:</p> <p><code>SubscriptionName</code> : el nombre de la suscripción.</p>
AggregateRunningInstancesCount	<p>El número total agregado de instancias que se están ejecutando en todas tus cuentas de AWS Organizations en la Región de AWS actual.</p> <p>Unidades: recuento</p> <p>Dimensiones:</p> <p><code>SubscriptionName</code> : el nombre de la suscripción.</p>
TotalLicenseConfigurationUsageCount	<p>El número total de una configuración de licencia que podría estar disponible.</p> <p>Unidades: recuento</p> <p>Dimensiones:</p> <ul style="list-style-type: none"> • <code>LicenseConfigurationArn</code> : el nombre de recurso de Amazon (ARN) de la configuración de la licencia. • <code>LicenseConfigurationType</code> : el tipo de configuraciones de licencias.
LicenseConfigurationUsageCount	<p>El número total de licencias utilizadas de esta configuración.</p> <p>Unidades: recuento</p> <p>Dimensiones:</p> <ul style="list-style-type: none"> • <code>LicenseConfigurationArn</code> : el ARN de la configuración de licencia.

Métrica	Descripción
LicenseConfigurationUsagePercentage	<ul style="list-style-type: none"> <code>LicenseConfigurationType</code> : el tipo de configuraciones de licencias. <p>Las licencias utilizadas de esta configuración de licencia expresadas como porcentaje.</p> <p>Unidades: porcentaje</p> <p>Dimensiones:</p> <ul style="list-style-type: none"> <code>LicenseConfigurationArn</code> : el ARN de la configuración de licencia. <code>LicenseConfigurationType</code> : el tipo de configuraciones de licencias.

Creación de alarmas para supervisar las métricas de Secrets Manager

Puede crear una alarma de CloudWatch que envíe un mensaje de Amazon Simple Notification Service (Amazon SNS) cuando el valor de la métrica cambie y haga que 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 tan solo por tener un estado determinado; es necesario que el estado haya cambiado y se mantenga durante un número específico de periodos. Para más información, consulte [Uso de las alarmas de CloudWatch](#).

Registro de llamadas a la API de AWS License Manager mediante AWS CloudTrail

AWS License Manager se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones que realiza un usuario, un rol o un servicio de AWS en License Manager. CloudTrail captura todas las llamadas a la API para 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 un registro de seguimiento, puede habilitar el envío continuo de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de License Manager.

Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a License Manager, la dirección IP de origen desde la que se realizó la solicitud, quién realizó la solicitud, cuándo se realizó y otros detalles adicionales.

Para obtener más información acerca de CloudTrail, consulte la [Guía del usuario de AWS CloudTrail](#).

Información de License Manager en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad en License Manager, dicha actividad se registra en un evento de CloudTrail junto con los demás eventos de servicios de AWS en Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte [Ver eventos con el historial de eventos de CloudTrail](#).

Para mantener un registro continuo de los eventos en su cuenta de AWS, incluidos los eventos de License Manager, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [Servicios e integraciones compatibles con CloudTrail](#)
- [Configuración de notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de registro de CloudTrail de varias regiones](#) y [Recibir archivos de registro de CloudTrail de varias cuentas](#)

CloudTrail registra todas las acciones de License Manager y se documentan en la [Referencia de API de License Manager](#). Por ejemplo, las llamadas a las acciones `CreateLicenseConfiguration`, `ListResourceInventory` y `DeleteLicenseConfiguration` generan entradas en los archivos de registros de CloudTrail.

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 AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el [Elemento userIdentity de CloudTrail](#).

Descripción de las entradas del archivo de registros de License Manager

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que especifique. Los archivos de registro de CloudTrail pueden contener una o más entradas de registro. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción `DeleteLicenseConfiguration`.

```
{
  "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 AWS License Manager

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre 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 los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [Programas de conformidad de AWS](#) . Para obtener información sobre los programas de conformidad que se aplican a License Manager, consulte .
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS 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 puede aprender a utilizar otros servicios de AWS que lo ayuden a monitorear y proteger los recursos de License Manager.

Contenido

- [Protección de los datos en AWS License Manager](#)
- [Administración de identidades y accesos en AWS License Manager](#)
- [Uso de roles vinculados a servicios de AWS License Manager](#)
- [Políticas administradas de AWS para AWS License Manager](#)
- [Firma criptográfica de licencias](#)
- [Validación de conformidad para AWS License Manager](#)
- [Resiliencia en AWS License Manager](#)
- [Seguridad de la infraestructura en AWS License Manager](#)
- [AWS License Manager y puntos de conexión de VPC de interfaz \(AWS PrivateLink\)](#)

Protección de los datos en AWS License Manager

El [modelo de responsabilidad compartida](#) de AWS se aplica a la protección de datos de AWS License Manager. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es 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, consulte las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog [Modelo de responsabilidad compartida y GDPR de AWS](#) en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la cuenta de Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se conceden a cada usuario los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los Servicios de AWS.
- Utilice servicios de seguridad gestionados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de la línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

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 trabaje con License Manager u otros Servicios de AWS a través de la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para nombres se pueden 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).

Administración de identidades y accesos en AWS License Manager

AWS Identity and Access Management (IAM) es un servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de AWS. IAM permite crear usuarios y grupos en su cuenta de AWS. Controle los permisos que tienen los usuarios para realizar tareas con recursos de AWS. Puede utilizar IAM sin 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 su 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 [Empezar con AWS License Manager](#).

Un [rol de IAM](#) es una identidad de IAM que puede crear en su cuenta y que tiene permisos específicos. Un rol de IAM es similar a un usuario de IAM en que se trata de una identidad de AWS con políticas de permisos que determinan lo que la identidad puede hacer y lo que no en 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 las API de License Manager disponibles, consulte las siguientes referencias de API:

- [Referencia de la API de AWS License Manager](#)
- [Referencia de la API de suscripciones de usuarios a AWS License Manager](#)
- [Referencia de la API de suscripciones de Linux de AWS License Manager](#)

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

Los proveedores de software independiente (ISV) 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 proporcionar acceso, agregue permisos a sus usuarios, grupos o roles:

- Usuarios y grupos de 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 administrados en IAM a través de un proveedor de identidades:

Cree un rol para la federación de identidades. Siga las instrucciones de [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 asumir. Siga las instrucciones de [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 agregue un usuario a un grupo de usuarios. Siga las instrucciones de [Adición de permisos a un usuario \(consola\)](#) de la Guía del usuario de IAM.

Uso de roles vinculados a servicios de AWS License Manager

AWS License Manager usa [roles vinculados a servicios](#) de AWS Identity and Access Management (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a Systems Manager. Los roles vinculados a servicios están predefinidos por License Manager e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS 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 adjuntar 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 al servicio

- [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 a servicios denominado `AWSServiceRoleForAWSLicenseManagerRole` permite a License Manager acceder a los recursos de AWS para administrar 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`, consulte [Política administrada de AWS: 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 IAM, AWS CLI o la API de IAM para crear manualmente un rol vinculado a servicios. Para obtener más información, consulte [Crear 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 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 AWS CLI o la API de AWS, utilice IAM para crear un rol vinculado a servicios con el nombre de servicio `license-manager.amazonaws.com`. Para obtener más información, consulte [Crear 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 [Modificación de 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 desasociar cualquier licencia autoadministrada de las instancias y AMI asociadas y, a continuación, eliminar las licencias autoadministradas.

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 License Manager en <https://console.aws.amazon.com/license-manager/>.
2. En el panel de navegación, seleccione Licencias autoadministradas.
3. Elija una licencia autoadministrada de la que sea propietario y desasocie todas las entradas de las pestañas AMI asociadas 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 o la API de AWS para eliminar el rol vinculado a servicios de `AWSServiceRoleForAWSLicenseManagerRole`. Si también utiliza [AWSServiceRoleForAWSLicenseManagerMasterAccountRole](#) y [AWSLicenseManagerMemberAccountRole](#), elimine primero esos roles. Para obtener más información, consulte [Eliminar un rol vinculado a un servicio](#) 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 a servicios denominado

`AWSServiceRoleForAWSLicenseManagerMasterAccountRole` permite a License Manager acceder a los recursos de AWS para llevar a cabo acciones de administración de licencias para 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`, consulte [Política administrada de AWS: 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. Cuando se configura la administración de licencias entre cuentas en AWS Management Console, License Manager crea el rol vinculado a servicios automáticamente.

Note

Para hacer uso de la administración de licencias entre cuentas de License Manager, debe estar utilizando 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 utilizar la consola IAM, AWS CLI o la API de IAM para crear manualmente un rol vinculado a servicios. Para obtener más información, consulte [Crear 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 License Manager en <https://console.aws.amazon.com/license-manager/>.
2. Elija Configuración, Editar.
3. Elija Vincular cuentas AWS Organizations.
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 AWS CLI o la API de AWS, utilice IAM para crear un rol vinculado a servicios con el nombre de servicio `license-manager.master-account.amazonaws.com`. Para obtener más información, consulte [Crear 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 [Modificación de 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 AWS CLI, AWS o la API de `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` para eliminar el rol vinculado a servicios. Para obtener más información, consulte [Eliminar un rol vinculado a un servicio](#) 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 a servicios denominado

`AWSServiceRoleForAWSLicenseManagerMemberAccountRole` permite a License Manager acceder a los recursos de AWS para llevar a cabo 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`, consulte [Política administrada de AWS: 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 con AWS Organizations desde la cuenta de administración de la consola License Manager en la página Configuración. También puede hacerlo mediante AWS CLI (ejecución de `update-service-settings`) o la API de AWS (llamada a `UpdateServiceSettings`). 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 puede utilizar la consola IAM, AWS CLI o la API de AWS para crear manualmente un rol vinculado a servicios. Para obtener más información, consulte [Crear 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 la cuenta de administración de AWS Organizations.
2. Abra la consola License Manager en <https://console.aws.amazon.com/license-manager/>.
3. En el panel de navegación izquierdo, elija Configuración y Básica.
4. Elija Vincular cuentas AWS Organizations.
5. Seleccione Aplicar. Esto crea los roles [AWSServiceRoleForAWSLicenseManagerRole](#) y [AWSServiceRoleForAWSLicenseManagerMemberAccountRole](#) en 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 AWS CLI o la API de AWS, cree un rol vinculado a servicios con el nombre de servicio `license-manager.member-account.amazonaws.com`. Para obtener más información, consulte [Crear 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 [Modificación de 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 AWS CLI, AWS o la API de `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` para eliminar el rol vinculado a servicios. Para obtener más información, consulte [Eliminar un rol vinculado a un servicio](#) en la Guía del usuario de IAM.

License Manager: rol de suscripciones basadas en usuarios

License Manager requiere un rol vinculado a servicios para administrar los recursos de AWS que proporcionarán suscripciones basadas en usuarios.

Permisos para el rol de suscripciones basadas en usuarios

El rol vinculado a servicios denominado `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` permite a License Manager utilizar AWS Systems Manager y administrar los recursos de Amazon EC2 que proporcionan suscripciones basadas en usuarios, así como describir los recursos de AWS Directory Service.

Para revisar los permisos de `AWSLicenseManagerUserSubscriptionsServiceRolePolicy`, consulte [Política administrada de AWS: 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 IAM, AWS CLI o la API de IAM para crear manualmente un rol vinculado a servicios. Para obtener más información, consulte [Crear 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 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 AWS CLI o la API de AWS, cree un rol vinculado a servicios con el nombre de servicio `license-manager-user-subscriptions.amazonaws.com`. Para obtener más información, consulte [Crear 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 [Modificación de 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 AWS CLI, AWS o la API de `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` para eliminar el rol vinculado a servicios. Para obtener más información, consulte [Eliminar un rol vinculado a un servicio](#) en la Guía del usuario de IAM.

License Manager: rol de suscripciones de Linux

License Manager requiere un rol vinculado a servicios para administrar los recursos de AWS que proporcionarán suscripciones de Linux.

Permisos para el rol de suscripciones de Linux

El rol vinculado servicios denominado

`AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` permite a License Manager detectar recursos de Amazon EC2 y AWS Organizations para agregar el uso de suscripciones de Linux.

Para revisar los permisos de `AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`, consulte [Política administrada de AWS: 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 IAM, AWS CLI o la API de IAM para crear manualmente un rol vinculado a servicios. Para obtener más información, consulte [Crear 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 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 AWS CLI o la API de

AWS, cree un rol vinculado a servicios con el nombre de servicio `license-manager-linux-subscriptions.amazonaws.com`. Para obtener más información, consulte [Crear 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 [Modificación de 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 AWS CLI, AWS o la API de `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` para eliminar el rol vinculado a servicios. Para obtener más información, consulte [Eliminar un rol vinculado a un servicio](#) en la Guía del usuario de IAM.

Políticas administradas de AWS para AWS License Manager

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar las políticas administradas de AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para [crear políticas administradas por el cliente de IAM](#) que le brinden a su equipo solo los permisos necesarios. Para comenzar a hacerlo con rapidez, puede utilizar nuestras políticas administradas de AWS. Estas políticas cubren casos de uso comunes y están disponibles en su cuenta de AWS. Para obtener más información sobre las políticas administradas por AWS, consulte [Políticas administradas por AWS](#) en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas de AWS. No puede cambiar los permisos en las políticas administradas de AWS. 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 administrada de AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan los permisos de una política administrada de AWS, por lo tanto, las actualizaciones de las políticas no deteriorarán los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` administrada por AWS proporciona acceso de solo lectura a todos los servicios y recursos de AWS. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripción de las políticas de funciones de trabajo, consulte [Políticas administradas de AWS para funciones de trabajo](#) en la Guía del usuario de IAM.

Política administrada de AWS: `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 de	ARN de recurso
<code>iam:CreateServiceLinkedRole</code>	<code>arn:aws:iam::*:role/aws-service-role/license-management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement</code>
<code>iam:CreateServiceLinkedRole</code>	<code>arn:aws:iam::*:role/aws-service-role/license-</code>

Acción de	ARN de recurso
	<code>manager.member-account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole</code>
<code>s3:GetBucketLocation</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>
<code>s3:ListBucket</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>
<code>s3:ListAllMyBuckets</code>	<code>*</code>
<code>s3:PutObject</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>
<code>sns:Publish</code>	<code>arn:aws::sns:*:*:aws-license-manager-service-*</code>
<code>sns:ListTopics</code>	<code>*</code>
<code>ec2:DescribeInstances</code>	<code>*</code>
<code>ec2:DescribeImages</code>	<code>*</code>
<code>ec2:DescribeHosts</code>	<code>*</code>
<code>ssm:ListInventoryEntries</code>	<code>*</code>
<code>ssm:GetInventory</code>	<code>*</code>
<code>ssm:CreateAssociation</code>	<code>*</code>
<code>organizations:ListAWSServiceAccessForOrganization</code>	<code>*</code>

Acción de	ARN de recurso
<code>organizations:DescribeOrganization</code>	*
<code>organizations:ListDelegatedAdministrators</code>	*
<code>license-manager:GetServiceSettings</code>	*
<code>license-manager:GetLicense*</code>	*
<code>license-manager:UpdateLicenseSpecificationsForResource</code>	*
<code>license-manager:List*</code>	*

Para ver los permisos de esta política en AWS Management Console, consulte [AWSLicenseManagerServiceRolePolicy](#).

Política administrada de AWS: 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 de	ARN de recurso
<code>s3:GetBucketLocation</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>
<code>s3:ListBucket</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>

Acción de	ARN de recurso
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-*/re source-sync/*
athena:GetQueryExecution	*
athena:GetQueryResults	*
athena:StartQueryExecution	*
glue:GetTable	*

Acción de	ARN de recurso
<code>glue:GetPartition</code>	*
<code>glue:GetPartitions</code>	*
<code>glue:CreateTable</code>	Véase la nota a pie de página. ¹
<code>glue:UpdateTable</code>	Véase la nota a pie de página. ¹
<code>glue>DeleteTable</code>	Véase la nota a pie de página. ¹
<code>glue:UpdateJob</code>	Véase la nota a pie de página. ¹
<code>glue:UpdateCrawler</code>	Véase la nota a pie de página. ¹
<code>organizations:DescribeOrganization</code>	*
<code>organizations:ListAccounts</code>	*
<code>organizations:DescribeAccount</code>	*
<code>organizations:ListChildren</code>	*
<code>organizations:ListParents</code>	*
<code>organizations:ListAccountsForParent</code>	*
<code>organizations:ListRoots</code>	*
<code>organizations:ListAWSServiceAccessForOrganization</code>	*
<code>ram:GetResourceShares</code>	*
<code>ram:GetResourceShareAssociations</code>	*
<code>ram:TagResource</code>	*
<code>ram:CreateResourceShare</code>	*
<code>ram:AssociateResourceShare</code>	*

Acción de	ARN de recurso
<code>ram:DisassociateResourceShare</code>	*
<code>ram:UpdateResourceShare</code>	*
<code>ram>DeleteResourceShare</code>	*
<code>resource-groups:PutGroupPolicy</code>	*
<code>iam:GetRole</code>	*
<code>iam:PassRole</code>	<code>arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*</code>
<code>cloudformation:UpdateStack</code>	<code>arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*</code>
<code>cloudformation:CreateStack</code>	<code>arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*</code>
<code>cloudformation>DeleteStack</code>	<code>arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*</code>
<code>cloudformation:DescribeStacks</code>	<code>arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*</code>

¹ Los siguientes son los recursos definidos para las acciones de AWS Glue.

- `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 AWS Management Console, consulte.

[AWSLicenseManagerMasterAccountRolePolicy](#)

Política administrada de AWS:

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 de	ARN de recurso
<code>license-manager:UpdateLicenseSpecificationsForResource</code>	*
<code>license-manager:GetLicenseConfiguration</code>	*
<code>ssm:ListInventoryEntries</code>	*
<code>ssm:GetInventory</code>	*

Acción de	ARN de recurso
<code>ssm:CreateAssociation</code>	*
<code>ssm:CreateResourceDataSync</code>	*
<code>ssm>DeleteResourceDataSync</code>	*
<code>ssm:ListResourceDataSync</code>	*
<code>ssm:ListAssociations</code>	*
<code>ram:AcceptResourceShareInvitation</code>	*
<code>ram:GetResourceShareInvitations</code>	*

Para ver los permisos de esta política en AWS Management Console, consulte [AWSLicenseManagerMemberAccountRolePolicy](#).

Política administrada de AWS: 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](#).

Para ver los permisos de esta política, consulte [AWSLicenseManagerConsumptionPolicy](#) en la AWS Management Console.

Política administrada de AWS:

`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 de	ARN de recurso
<code>ds:DescribeDirectories</code>	*
<code>ds:GetAuthorizedApplicationDetails</code>	*
<code>ec2:CreateTags</code>	<code>arn:aws:ec2:*:*:instance/*</code> ¹
<code>ec2:DescribeInstances</code>	*
<code>ec2:DescribeVpcPeeringConnections</code>	*
<code>ec2:TerminateInstances</code>	<code>arn:aws:ec2:*:*:instance/*</code> ¹
<code>ssm:DescribeInstanceInformation</code>	*
<code>ssm:GetCommandInvocation</code>	*
<code>ssm:GetInventory</code>	*
<code>ssm:ListCommandInvocations</code>	*
<code>ssm:SendCommand</code>	<code>arn:aws:ssm:*:*:document/AWS-² RunPowerShellScript</code> <code>arn:aws:ec2:*:*:instance/*</code> 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 los permisos de esta política en, consulte. AWS Management Console [AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)

Política administrada de AWS: 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 de	ARN de recurso
<code>ec2:DescribeInstances</code>	*
<code>ec2:DescribeRegions</code>	*
<code>organizations:DescribeOrganization</code>	*
<code>organizations:ListAccounts</code>	*
<code>organizations:DescribeAccount</code>	*
<code>organizations:ListChildren</code>	*
<code>organizations:ListParents</code>	*
<code>organizations:ListAccountsForParent</code>	*
<code>organizations:ListRoots</code>	*
<code>organizations:ListAWSServiceAccessForOrganization</code>	*
<code>organizations:ListDelegatedAdministrators</code>	*

Para ver los permisos de esta política en AWS Management Console, consulte [AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#).

Actualizaciones de License Manager para políticas administradas de AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas de AWS para License Manager debido a que este servicio comenzó a realizar el seguimiento de estos cambios.

Cambio	Descripción	Fecha
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy : política nueva	License Manager agregó un permiso para crear el rol vinculado a servicios denominado <code>AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService</code> . Este rol proporciona permiso al License Manager para publicar recursos de AWS Organizations y de Amazon EC2.	21 de diciembre de 2022
AWSLicenseManagerUserSubscriptionsServiceRolePolicy : actualización de una política actual	License Manager agregó el permiso <code>ec2:DescribeVpcPeeringConnections</code> .	28 de noviembre de 2022
AWSLicenseManagerUserSubscriptionsServiceRolePolicy : política nueva	License Manager agregó un permiso para crear el rol vinculado a servicios denominado <code>AWSLicenseManagerUserSubscriptionsServiceRolePolicy</code> . Este rol proporciona permiso a License Manager para enumerar los recursos de	18 de julio de 2022

Cambio	Descripción	Fecha
	AWS Directory Service, utilizar las características de Systems Manager y administrar los recursos de Amazon EC2 creados para las suscripciones basadas en usuarios.	
AWSLicenseManagerMasterAccountRolePolicy : actualización de una política actual	License Manager agregó el permiso <code>resource-groups:PutGroupPolicy</code> 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 el valor <code>ram:ResourceTag</code> de la clave de condición para AWS Resource Access Manager <code>AWSLicenseManagerMasterAccountRolePolicy</code> de la política de administración de AWS por el valor <code>aws:ResourceTag</code> .	16 de noviembre de 2021
AWSLicenseManagerConsumptionPolicy : política nueva	License Manager agregó una nueva política que concede permisos para consumir licencias.	11 de agosto de 2021

Cambio	Descripción	Fecha
<p>AWSLicenseManagerServiceRolePolicy: actualización de una política actual</p>	<p>License Manager agregó un permiso para enumerar los administradores delegados y un permiso para crear el rol vinculado a servicios denominado <code>AWSServiceRoleForAWSLicenseManagerMemberAccountRole</code>.</p>	<p>16 de junio de 2021</p>
<p>AWSLicenseManagerServiceRolePolicy: actualización de una política actual</p>	<p>License Manager agregó un permiso para enumerar todos los recursos de License Manager, como configuraciones de licencias, licencias y concesiones.</p>	<p>15 de junio de 2021</p>
<p>AWSLicenseManagerServiceRolePolicy: actualización de una política actual</p>	<p>License Manager agregó un permiso para crear el rol vinculado a servicios denominado <code>AWSServiceRoleForMarketplaceLicenseManagement</code>. Este rol proporciona a AWS Marketplace 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.</p>	<p>9 de marzo de 2021</p>

Cambio	Descripción	Fecha
Inicio del seguimiento de los cambios por parte de License Manager	License Manager comenzó a realizar un seguimiento de los cambios en sus políticas administradas de AWS.	9 de marzo de 2021

Firma criptográfica de licencias

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 de 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 [Signy](#) 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 CMK asimétricas](#) y [Cómo elegir la 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:1-6585590917ad46858328ff02dEXAMPLE",
  "licenseConsumptionToken": "306eb19afd354ba79c3687b9bEXAMPLE",
  "nodeId": "100.20.15.10",
  "checkoutMetadata": {
    "Mac": "ABCDEFGHI"
  }
}
```

Validación de conformidad para AWS 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:

- [Guías de inicio rápido sobre seguridad y cumplimiento](#): estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de [arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services](#): en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

 Note

No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la [Referencia de servicios compatibles con HIPAA](#).

- [AWS Recursos 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, consulte 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 AWS License Manager

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. 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 latencia. 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 centros de datos únicos o múltiples.

Para obtener más información sobre las regiones y zonas de disponibilidad de AWS, consulte [Infraestructura global de AWS](#).

Seguridad de la infraestructura en AWS License Manager

Como se trata de un servicio administrado, AWS License Manager está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte [Seguridad en la nube de AWS](#). Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte [Protección de la infraestructura](#) en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para acceder a Secrets Manager a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Se requiere el uso de 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 de seguridad de IAM. También puede utilizar [AWS](#)

[Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

AWS License Manager y puntos de conexión de VPC de interfaz (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 de conexión de tipo interfaz cuentan con tecnología de [AWS PrivateLink](#) que permite acceder de forma privada a las API de License Manager sin una puerta de enlace de Internet, un dispositivo NAT, una conexión de VPN o una conexión de AWS Direct Connect. 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.license-manager`
- `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 AWS 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 [Configuración de AWS License Manager](#).

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 paso a paso](#).

La cuenta de administración no puede disociar 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 imagen de máquina de Amazon (AMI) asociada a la licencia autoadministrada mediante Amazon EC2, puede que la AMI siga apareciendo momentáneamente en el inventario de recursos de License Manager antes de que se depure.

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.

Historial de documentos para AWS License Manager

En la siguiente tabla se describen las versiones de AWS License Manager.

Cambio	Descripción	Fecha
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 (AMI) 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 concesiones activas por una licencia concedida durante la activación de la concesión.	31 de marzo de 2023
Administración delegada para las suscripciones de Linux	License Manager agregó soporte para administradores delegados para las suscripciones de Linux.	3 de marzo de 2023
Suscripciones de Linux	License Manager agregó el seguimiento de las suscripciones 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 suscripciones 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 organización (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	Utilice productos de suscripción basada 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 las licencias AWS proporcionadas y el modelo Bring Your Own License (BYOL) sin tener que volver a distribuir las cargas de trabajo existentes. AWS CLI	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 los identificadores y etiquetas de las AWS cuentas.	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

Cambio	Descripción	Fecha
Ámbito de asociación de las AMI	Asocie sus licencias autoadministradas y las imágenes de máquinas de Amazon (AMI) compartidas con su cuenta de AWS .	23 de noviembre de 2020
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 implementaciones 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 autoadministradas 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 utiliza las licencias proporcionadas 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 versión original de inglés, prevalecerá la versión en inglés.