



Manual do usuário

AWS License Manager



AWS License Manager: Manual do usuário

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestígie a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

O que AWS License Manager é	1
Direitos gerenciados	2
Casos de uso do License Manager	2
Serviços relacionados	3
Como o License Manager funciona	5
Conceitos básicos	8
Configuração	8
Inscreva-se para um Conta da AWS	8
Criar um usuário com acesso administrativo	9
Conceitos básicos do License Manager	10
Trabalhar com o License Manager	11
Licenças autogerenciadas	12
Parâmetros e regras	13
Criar regras a partir de licenças de fornecedores	15
Como criar uma licença autogerenciada	17
Como compartilhar uma licença autogerenciada	18
Como editar uma licença autogerenciada	22
Como desativar uma licença autogerenciada	23
Como excluir uma licença autogerenciada	24
Regras de licença	24
Associando licenças e AMIs autogerenciadas	26
Desassociando licenças e AMIs autogerenciadas	27
Relatórios de uso	27
Criar relatórios de uso	28
Editar relatórios de uso	29
Excluir um relatório de uso	30
Conversões de tipo de licença	30
Tipos de licença elegíveis	32
Pré-requisitos	41
Como converter um tipo de licença	43
Conversão de locação	53
Solução de problemas	55
Grupos de atributos de host	57
Criar um grupo de atributos de host	58

Compartilhar um grupo de recursos de host	59
Adicionar hosts dedicados a um grupo de atributos de host	59
Como executar uma instância em um grupo de atributos de host	60
Modificar um grupo de recursos de host	60
Remover Hosts dedicados de um grupo de recursos de host	60
Excluir um grupo de atributos de host	61
Pesquisa de inventário	61
Trabalhando com a pesquisa de inventário	62
Descoberta automatizada de inventário	68
Licenças concedidas	70
Visualizar suas licenças concedidas	71
Como gerenciar suas licenças concedidas	71
Como distribuir direitos	75
Como aceitar a ativar concessões	76
Status da licença	79
Métricas para contas de compradores	80
Licenças emitidas pelo vendedor	81
Direitos	82
Uso da licença	83
Requisitos	83
Criação de licenças emitidas pelo vendedor	85
Concessão de licenças aos clientes	86
Obter credenciais temporárias para clientes sem uma conta AWS	87
Consumo de licenças	88
Exclusão de licenças emitidas pelo vendedor	89
Gerencie assinaturas baseadas no usuário	89
Pré-requisitos	91
Considerações	94
Software compatível	95
Conceitos básicos	98
Modificar as configurações do diretório	108
Modificar as configurações da VPC	109
Desassociar usuários	110
Cancelar a inscrição de usuários	110
Terminar instâncias	111
Remover um diretório	112

Solução de problemas	112
Gerenciar assinaturas Linux	114
Configurar a descoberta	116
Exibir dados da instância	123
Informações de cobrança	125
Gerenciar CloudWatch alarmes	127
Configurações	130
Editar configurações do License Manager	131
Licenças gerenciadas	131
Assinaturas Linux	133
Conversão de tipo de licença	136
Administradores delegados	136
Painel	141
Monitorar o License Manager	144
Monitoramento com CloudWatch	144
Criar alarmes do CloudWatch	146
Registrar em log chamadas de API com o CloudTrail	146
Informações sobre o License Manager no CloudTrail	147
Noções básicas sobre as entradas do arquivo de log do License Manager	148
Segurança	149
Proteção de dados	150
Criptografia em repouso	151
Gerenciamento de identidade e acesso	151
Criar usuários, grupos e perfis	151
Estrutura da política do IAM	152
Criar políticas do IAM para o License Manager	153
Conceder permissões a usuários, grupos e perfis	154
Funções vinculadas a serviço	155
Perfil principal	156
Perfil da conta de gerenciamento	158
Perfil da conta-membro	161
Perfil de assinatura baseado no usuário	163
Perfil de assinaturas Linux	165
AWS políticas gerenciadas	166
AWSLicenseManagerServiceRolePolicy	167
AWSLicenseManagerMasterAccountRolePolicy	169

AWSLicenseManagerMemberAccountRolePolicy	173
AWSLicenseManagerConsumptionPolicy	174
AWSLicenseManagerUserSubscriptionsServiceRolePolicy	174
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	176
Atualizações da política	177
Assinatura de licença	181
Validação de conformidade	182
Resiliência	184
Segurança da infraestrutura	184
VPC endpoints (AWS PrivateLink)	185
Criar um endpoint da VPC de interface para o License Manager	185
Criar uma política de endpoint da VPC para o License Manager	185
Solução de problemas	187
Erro de descoberta entre contas	187
A conta de gerenciamento não pode dissociar recursos de uma licença autogerenciada	187
O inventário do Systems Manager está desatualizado	187
Persistência aparente de uma AMI de registro cancelado	188
Nova instância de conta filho demora a ser exibida no inventário de atributos	188
Após habilitar o modo entre contas, as instâncias de contas filho demoram a ser exibidas	188
Não é possível desabilitar a descoberta entre contas	188
O usuário de uma conta filho não consegue associar a licença autogerenciada compartilhada com uma instância	189
Falha na vinculação de AWS Organizations contas	189
Histórico do documento	190
.....	cxcvi

O que AWS License Manager é

AWS License Manager é um serviço que facilita o gerenciamento centralizado de licenças de software de fornecedores de software (por exemplo, Microsoft, SAP, Oracle e IBM) em todos os ambientes locais e em seus ambientes AWS locais. Isso fornece controle e visibilidade do uso de suas licenças, permitindo que você limite os excedentes de licenciamento e reduza o risco de não conformidade e relatórios incorretos.

Ao criar sua infraestrutura de nuvem AWS, você pode economizar custos usando as oportunidades do modelo Bring Your Own License (BYOL). Ou seja, você poderá reaproveitar o inventário de licenças existente para usar com atributos de nuvem.

O License Manager reduz o risco de excedentes e penalidades de licenciamento com o rastreamento de inventário vinculado diretamente aos serviços. AWS Com controles baseados em regras no consumo de licenças, os administradores podem definir limites rígidos ou flexíveis em implantações de nuvem novas e existentes. Com base nesses limites, o License Manager ajuda a impedir o uso incompatível do servidor antes que isso aconteça.

Os painéis integrados do License Manager fornecem visibilidade contínua do uso de licenças e assistência nas auditorias de fornecedores.

O License Manager oferece suporte ao rastreamento de qualquer software licenciado com base em núcleos virtuais (vCPUs), núcleos físicos, soquetes ou número de máquinas. Isso inclui uma variedade de produtos de software da Microsoft, IBM, SAP, Oracle e outros fornecedores.

Com AWS License Manager, você pode rastrear licenças de forma centralizada e impor limites em várias regiões, mantendo uma contagem de todos os direitos retirados. O License Manager também rastreia a identidade do usuário e o identificador de atributo subjacente, se disponível, associado a cada check-out, além de quando o check-out foi feito. Esses dados de séries temporais podem ser rastreados até o ISV por meio de CloudWatch métricas e eventos. Os ISVs podem usar esses dados para análises, auditorias e outros fins semelhantes.

AWS License Manager é integrado [AWS Marketplace](#) ao [AWS Data Exchange](#) e aos seguintes AWS serviços: [AWS Identity and Access Management \(IAM\)](#) [AWS Organizations](#), Service Quotas [AWS CloudFormation](#), marcação de AWS recursos e [AWS X-Ray](#)

Direitos gerenciados

Com o License Manager, um administrador de licenças pode distribuir, ativar e rastrear licenças de software em todas as contas e em toda a organização.

Fornecedores independentes de software (ISVs) podem usar AWS License Manager para gerenciar e distribuir licenças e dados de software para usuários finais por meio de direitos gerenciados. Como emissor, você pode monitorar centralmente o uso das licenças emitidas pelo vendedor usando o painel do License Manager. Os ISVs vendidos por meio da venda AWS Marketplace se beneficiam da criação e distribuição automáticas de licenças como parte do fluxo de trabalho da transação. Os ISVs também podem usar o License Manager para criar chaves de licença e ativar licenças para clientes sem uma AWS conta.

O License Manager usa padrões abertos e seguros do setor para representar licenças e permite que os clientes verifiquem criptograficamente sua autenticidade. O License Manager oferece suporte a uma variedade de modelos de licenciamento diferentes, incluindo licenças perpétuas, licenças flutuantes, licenças por assinatura e licenças baseadas no uso. Se você tiver licenças que precisam ser bloqueadas por nó, o License Manager fornece mecanismos para consumir as licenças dessa forma.

Você pode criar licenças AWS License Manager e distribuí-las aos usuários finais usando uma identidade do IAM ou por meio de tokens assinados digitalmente gerados por AWS License Manager. Os usuários finais que usam AWS podem redistribuir ainda mais os direitos de licença às AWS identidades em suas respectivas organizações. Usuários finais com direitos distribuídos podem fazer check-out e check-in dos direitos exigidos pela licença por meio de integração de seu software com o AWS License Manager. Cada check-out de licença especifica os direitos, a quantidade associada e o período de check-out, como o check-out de 10 **admin-users** por 1 hora. Essa verificação pode ser realizada com base na identidade subjacente do IAM para a licença distribuída ou com base nos tokens de longa duração gerados por AWS License Manager meio do AWS License Manager serviço.

Casos de uso do License Manager

Veja a seguir exemplos da funcionalidade fornecida pelo License Manager para vários casos de uso:

- [Licenças autogerenciadas no License Manager](#)— Usado para definir regras de licenciamento com base nos termos de seus contratos corporativos, que determinam como AWS processa os comandos que consomem essas licenças.

- [Licenças emitidas pelo vendedor no License Manager](#): usado para gerenciar e distribuir licenças de software para usuários finais.
- [Licenças concedidas no License Manager](#)— Usado para controlar o uso de licenças adquiridas de AWS Marketplace AWS Data Exchange, ou diretamente de um vendedor que integrou seu software com direitos gerenciados.
- [Conversões de tipo de licença no License Manager](#)— Usado para alterar seu tipo de licença entre o licenciamento AWS fornecido e o modelo Bring Your Own License (BYOL) sem reimplantar suas cargas de trabalho.
- [Pesquisa de inventário no License Manager](#)— Usado para descobrir e rastrear aplicativos locais usando regras de AWS Systems Manager inventário e licenciamento.
- [Gerencie assinaturas baseadas no usuário no License Manager](#): usado para comprar licenças totalmente compatíveis fornecidas pela Amazon para software com suporte a uma taxa de assinatura por usuário.
- [Gerencie assinaturas Linux no License Manager](#): usado para visualizar e gerenciar assinaturas comerciais do Linux que você possui e executa na AWS.

Serviços relacionados

O License Manager é integrado ao Amazon EC2, Amazon RDS,, AWS Marketplace, e. AWS Systems Manager AWS Organizations

A integração com o Amazon EC2 permite que você rastreie licenças para os seguintes recursos e aplique regras de licenciamento em todo o ciclo de vida do recurso:

- [Instâncias do Amazon EC2](#)
- [Instâncias dedicadas](#)
- [Hosts dedicados](#)
- [Instâncias spot e frota spot](#)
- [Nós gerenciados](#)

Ao usar o License Manager junto com AWS Systems Manager, você pode gerenciar licenças em servidores físicos ou virtuais hospedados fora do AWS. Você pode usar o License Manager com AWS Organizations para gerenciar todas as suas contas organizacionais de forma centralizada.

Além disso, você pode controlar o uso de licenças compradas de AWS Marketplace AWS Data Exchange, ou diretamente de um vendedor que integrou seu software com AWS License Manager. Você pode usar AWS License Manager para distribuir direitos de uso, conhecidos como direitos, para pessoas específicas. Contas da AWS

O License Manager se integra ao Amazon RDS for Oracle e ao Amazon RDS para licenças BYOL baseadas em vCPUs do Db2. Com essa integração, você ganha visibilidade do uso da vCPU para suas instâncias de banco de dados RDS for Oracle e RDS for Db2. Você pode usar esses dados para calcular o número de licenças consumidas com base nos termos de licenciamento com os fornecedores do sistema de gerenciamento de banco de dados. Para obter mais informações, consulte os seguintes links associados no Guia do usuário do Amazon RDS.

- [Opções de licenciamento do RDS para Oracle](#)
- [Opções de licenciamento do RDS for Db2](#)

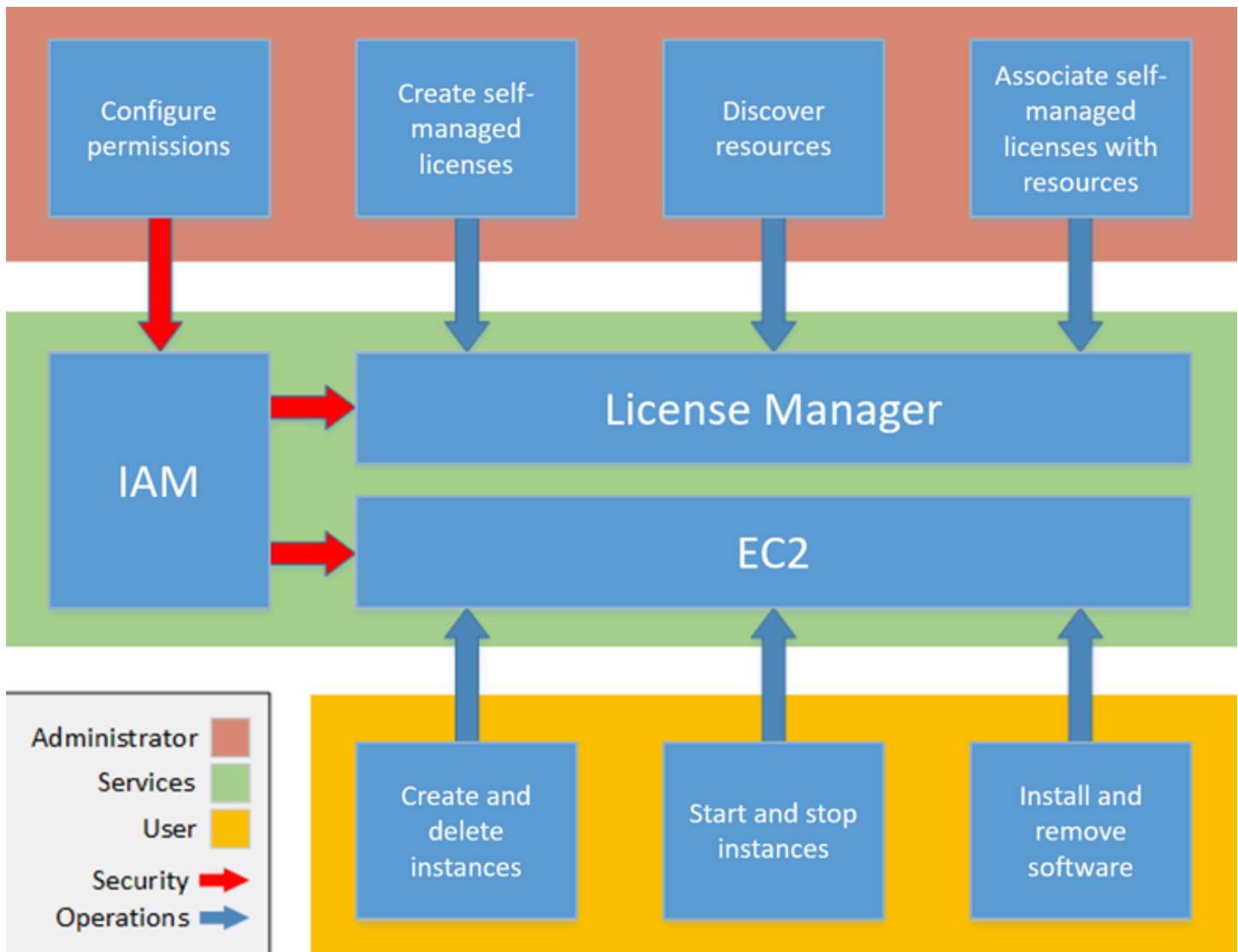
Como o License Manager funciona

O gerenciamento eficaz de licenças de software depende do seguinte:

- Uma compreensão especializada da linguagem em contratos de licenciamento corporativo
- Acesso adequadamente restrito às operações que consomem licenças
- Rastreamento preciso do inventário de licenças

É provável que as empresas tenham pessoas ou equipes dedicadas responsáveis por cada um desses domínios. Depois disso se torna um problema de comunicação eficaz, principalmente entre especialistas em licenças e administradores de sistemas. O License Manager apresenta uma forma de reunir conhecimento de vários domínios. Por esse motivo, ele também se integra nativamente aos serviços da AWS. Por exemplo, com o ambiente de gerenciamento do Amazon EC2, onde instâncias são criadas e excluídas. Isso significa que as regras e limites do License Manager capturam o conhecimento comercial e operacional e também se convertem em controles automatizados na criação de instâncias e na implantação de aplicativos.

O diagrama a seguir ilustra os deveres distintos, mas coordenados, dos administradores de licenças, que gerenciam permissões e configuram o License Manager, e os usuários, que criam, gerenciam e excluem atributos por meio do console do Amazon EC2.



Se for responsável pelo gerenciamento de licenças em sua organização, você poderá usar o License Manager para definir regras de licenciamento, anexá-las a seus lançamentos e rastrear o uso. Os usuários em sua organização podem adicionar e remover atributos que consomem licença sem trabalho adicional.

Um especialista em licenciamento gerencia licenças em toda a organização, determinando as necessidades de inventário de atributos, supervisionando a aquisição de licenças e orientando o uso de licenças em conformidade. Em uma empresa que usa o License Manager, esse trabalho é consolidado por meio do console do License Manager. Conforme mostrado no diagrama, isso envolve a definição de permissões de serviço, a criação de licenças autogerenciadas, o inventário de atributos de computação on-premises e na nuvem e a associação de licenças autogerenciadas a atributos descobertos. Na prática, isso poderia significar associar uma licença autogerenciada

a uma imagem de máquina da Amazon (AMI) aprovada que a TI usa como modelo para todas as implantações de instâncias do Amazon EC2.

O License Manager economiza custos que, de outra forma, seriam perdidos em violações de licenças. Auditorias internas revelam violações apenas após o fato, quando é tarde demais para evitar penalidades por incompatibilidade. O License Manager impede que esses incidentes caros aconteçam. O License Manager simplifica a criação de relatórios com painéis integrados que mostram o consumo de licenças e os atributos monitorados.

Começando com AWS License Manager

As seções a seguir orientam você na configuração de seus usuários Conta da AWS e em como começar a usar o License Manager. Para obter mais informações sobre como gerenciar permissões para usuários, grupos e funções utilizarem o License Manager e, ao mesmo tempo, seguir as AWS melhores práticas, consulte [Gerenciamento de identidade e acesso para o AWS License Manager](#). Para obter mais informações sobre como configurar seus atributos do Amazon EC2 que se integram ao License Manager, consulte [Configurar o Amazon EC2](#) no Guia do usuário do Amazon Elastic Compute Cloud.

Tópicos

- [Configuração](#)
- [Integrado para usar o License Manager no AWS Management Console](#)

Configuração

A seção a seguir detalha a configuração do seu Conta da AWS e dos usuários.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga as instruções on-line.

Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar [tarefas que exigem acesso de usuário-raiz](#).

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando <https://aws.amazon.com/> e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login [AWS Management Console](#) como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

Para obter ajuda ao fazer login usando o usuário-raiz, consulte [Signing in as the root user](#) (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .

2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

Para obter instruções, consulte [Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz \(console\) no Guia](#) do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

Para obter instruções, consulte [Habilitar AWS IAM Identity Center](#) no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte [Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM](#) no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte [Como fazer login no portal de AWS acesso](#) no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte [Create a permission set](#) no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

Para obter instruções, consulte [Add groups](#) no Guia do usuário do AWS IAM Identity Center .

Integrado para usar o License Manager no AWS Management Console

O procedimento a seguir é necessário para começar a usar o License Manager. Depois que os requisitos iniciais forem concluídos, você pode começar a usar o License Manager para o caso de uso desejado.

Conceitos básicos do License Manager

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Você precisará configurar as permissões para o License Manager e seus serviços compatíveis. Siga as instruções para configurar as permissões necessárias.
3. Depois que a configuração inicial for concluída, você pode começar a usar o License Manager para o [Casos de uso do License Manager](#) que quiser.

Trabalhar com AWS License Manager

O License Manager pode ser aplicado a cenários padrão de empresas com infraestrutura mista de atributos de AWS e atributos on-premises. É possível criar licenças autogerenciadas, fazer inventário dos atributos que consomem licença, associar licenças autogerenciadas a atributos e controlar o inventário e a conformidade.

Licenciamento para produtos do AWS Marketplace

Usando o License Manager, agora você pode associar regras de licenciamento aos produtos da AMI BYOL do AWS Marketplace por meio dos modelos de execução do Amazon EC2, modelos do AWS CloudFormation ou produtos do catálogo de serviços. Em cada caso, você se beneficia do controle centralizado de licenças e da aplicação de compatibilidade.

Note

O License Manager não altera a forma como você obtém e ativa as AMIs BYOL do Marketplace. Após o lançamento, você deve fornecer uma chave de licença obtida diretamente do vendedor para ativar qualquer software de terceiros.

Controle de licenças para atributos em datacenters locais

Com o License Manager, é possível descobrir aplicativos em execução fora da AWS com o serviço de [inventário do Systems Manager](#) e anexar regras de licenciamento a eles. Depois que as regras de licenciamento forem anexadas, você poderá rastrear os servidores on-premises juntamente com os atributos da AWS no console do License Manager.

Diferencie entre licença incluída e BYOL

Com o License Manager, você pode identificar quais atributos têm uma licença incluída no produto e quais usam uma licença pertencente a você. Isso permite relatar com precisão como está usando as licenças BYOL. Esse filtro requer SSM versão 2.3.722.0 ou posterior.

License Manager em todas as suas contas da AWS

O License Manager permite gerenciar licenças em todas as suas contas da AWS. Logo, é possível criar configurações de licença na sua conta de gerenciamento do AWS Organizations e compartilhá-

las pelas suas outras contas usando o AWS Resource Access Manager ou vincular as contas do AWS Organizations usando as configurações do License Manager. Também é possível executar a descoberta entre contas para pesquisar o inventário em suas contas da AWS.

Índice

- [Licenças autogerenciadas no License Manager](#)
- [Regras de licença no License Manager](#)
- [Relatórios de uso no License Manager](#)
- [Conversões de tipo de licença no License Manager](#)
- [Hospede grupos de recursos em AWS License Manager](#)
- [Pesquisa de inventário no License Manager](#)
- [Licenças concedidas no License Manager](#)
- [Licenças emitidas pelo vendedor no License Manager](#)
- [Gerencie assinaturas baseadas no usuário no License Manager](#)
- [Gerencie assinaturas Linux no License Manager](#)
- [Configurações em AWS License Manager](#)
- [Painel na AWS License Manager](#)

Licenças autogerenciadas no License Manager

As licenças autogerenciadas são a essência do License Manager. Anteriormente, elas eram como “configurações de licenças”. As licenças autogerenciadas contêm regras de licenciamento com base nos termos de seus contratos empresariais. As regras que você cria determinam como AWS processa os comandos que consomem licenças. Ao criar licenças autogerenciadas, trabalhe em conjunto com a equipe de compliance da sua organização para analisar seus contratos empresariais.

Limites

- Número de licenças autogerenciadas por atributo: 10
- Número total de licenças autogerenciadas: 25
- As instâncias gerenciadas do Systems Manager devem estar associadas às licenças autogerenciadas por vCPU e tipo de instância.

Conteúdo

- [Parâmetros e regras das licença autogerenciadas](#)
- [Como criar regras do License Manager a partir de licenças de fornecedores](#)
- [Como criar uma licença autogerenciada](#)
- [Como compartilhar uma licença autogerenciada](#)
- [Como editar uma licença autogerenciada](#)
- [Como desativar uma licença autogerenciada](#)
- [Como excluir uma licença autogerenciada](#)

Parâmetros e regras das licença autogerenciadas

Uma licença autogerenciada consiste em parâmetros básicos e regras que variam de acordo com os valores de parâmetro. Você também pode adicionar tags a licenças autogerenciadas. Depois de criar uma licença autogerenciada, um administrador pode modificar o número de licenças e o limite de uso para refletir as mudanças nas necessidades de atributos.

Os parâmetros e as regras disponíveis incluem o seguinte:

- Nome da licença autogerenciada — O nome da licença autogerenciada.
- (Opcional) Descrição — Uma descrição da licença autogerenciada.
- Tipo de licença — A métrica usada para contas licenças. Os valores compatíveis são vCPUs, Núcleos, Soquetes e Instâncias.
- (Opcional) Número de <opção>: o número de licenças usadas por um atributo.
- Status — Indica se a configuração está ativa.
- Informações do produto — Os nomes e versões dos produtos para [descoberta automatizada](#). Os produtos compatíveis são Windows Server, SQL Server, Amazon RDS for Oracle e Amazon RDS for Db2.
- (Opcional) Regras: elas incluem o seguinte. As regras disponíveis variam de acordo com o tipo de contagem.
 - Afinidade da licença com o host (em dias) — Restringe o uso da licença para o host pelo número especificado de dias. O intervalo é de 1 a 180. O tipo de contagem deve ser Núcleos ou Soquetes. Após o término do período de afinidade, a licença estará disponível para reutilização em 24 horas.
 - Máximo de núcleos — Contagem máxima de núcleos para um atributo.
 - Máximo de soquetes — Contagem máxima de soquetes para um atributo.

- Máximo de vCPUs — Contagem máxima de vCPUs para um atributo.
- Mínimo de núcleos — Contagem mínima de núcleos para um atributo.
- Mínimo de soquetes — Contagem mínima de soquetes para um atributo.
- Mínimo de vCPUs — Contagem mínima de vCPUs para um atributo.
- Locação — Restringe o uso da licença à locação do EC2 especificada. Hosts Dedicados são necessários se o tipo de contagem for Núcleos ou Soquetes. Locação compartilhada, Hosts Dedicados e Instâncias Dedicadas são compatíveis se o tipo de contagem for Instâncias ou vCPUs. Os nomes do console (e da API) são os seguintes:
 - Compartilhado (EC2-Default)
 - Instância Dedicada (EC2-DedicatedInstance)
 - Host Dedicado (EC2-DedicatedHost)
- Otimização de vCPU — O License Manager se integra ao suporte de [otimização de CPU](#) no Amazon EC2, o que permite que você personalize o número de vCPUs em uma instância. Se a regra for definida como “True”, o License Manager conta vCPUs com base no núcleo personalizado e na contagem de threads. Caso contrário, ele contabiliza o número padrão de vCPUs para o tipo de instância.

A tabela a seguir descreve quais regras de licença estão disponíveis para cada tipo de contagem.

Nome do console	Nome da API	Núcleos	Instâncias	Soquetes	vCPUs
Afinidade de licença com o host (em dias)	licenseAffinityToHost	✓		✓	
Máximo de núcleos	maximumCores	✓	✓		
Máximo de soquetes	maximumSockets		✓	✓	
Máximo de vCPUs	maximumVcpus		✓		✓
Mínimo de núcleos	minimumCores	✓	✓		
Mínimo de soquetes	minimumSockets		✓	✓	
Mínimo de vCPUs	minimumVcpus		✓		✓

Nome do console	Nome da API	Núcleos	Instâncias	Soquetes	vCPUs
Locação	allowedTenancy	✓	✓	✓	✓
Otimização de vCPU	honorVcpuOptimization				✓

Como criar regras do License Manager a partir de licenças de fornecedores

Você pode criar conjuntos de regras do License Manager com base na linguagem das licenças dos fornecedores de software. Os exemplos a seguir não são esquemas para casos de uso reais. Em qualquer aplicação real de um contrato de licença, você escolhe entre opções concorrentes, dependendo da arquitetura e do histórico de licenciamento do seu ambiente de servidor on-premises específico. Suas opções também dependem dos detalhes da migração planejada de atributos para a AWS.

Sempre que possível, esses exemplos devem ser neutros em relação a fornecedores, concentrando-se em questões de alocação de hardware e software que podem ser aplicadas de forma geral. As disposições de licenciamento do fornecedor também interagem com AWS os requisitos e limites. O número de licenças necessárias para um aplicativo varia de acordo com o tipo de instância escolhido e outros fatores.

Important

AWS não participa do processo de auditoria com fornecedores de software. Os clientes são responsáveis pela compatibilidade e assumem a responsabilidade de compreender e capturar com cuidado as regras do License Manager com base nos contratos de licenciamento.

Exemplo: implementação de uma licença de sistema operacional

Este exemplo envolve uma licença para um sistema operacional de servidor. A linguagem de licenciamento impõe restrições ao tipo de núcleo da CPU, locação e número mínimo de licenças por servidor.

Neste exemplo, os termos de licenciamento incluem as seguintes estipulações:

- Núcleos do processador físico determinam a contagem de licenças.
- O número de licenças deve ser igual ao número de núcleos.
- Um servidor deve executar no mínimo oito núcleos.
- O sistema operacional deve ser executado em um host não virtualizado.

Além disso, o cliente tomou as seguintes decisões:

- Licenças para 96 núcleos foram compradas.
- Um limite rígido é imposto para restringir o consumo de licenças à quantidade comprada.
- Cada servidor precisa de um máximo de 16 núcleos.

A tabela abaixo associa os parâmetros de criação de regras do License Manager aos requisitos de licenciamento de fornecedores que eles capturam e automatizam. Os valores de exemplo são apenas para fins ilustrativos. Você precisa especificar os valores necessários nas suas próprias licenças autogerenciadas.

Regra do License Manager	Configurações
Tipo de contagem de licenças	Tipo de licença é definido como Cores .
Contagem de licenças	Número de núcleos é definido como 96 .
Mínimo/máximo de vCPUs ou núcleos	Mínimo de núcleos é definido como 8 . Máximo de núcleos é definido como 16 .
Limite rígido de contagem de licenças	Aplicar limite de licença está selecionado.
Localização permitida	Localização está definida como Dedicated Host .

Como criar uma licença autogerenciada

Uma licença autogerenciada representa os termos de licenciamento no contrato com seu fornecedor de software. Sua licença autogerenciada especifica como suas licenças devem ser contadas (por exemplo, por vCPUs ou número de instâncias). Ela também especifica limites que previnem que o uso ultrapasse o número de licenças alocadas. Além disso, as licenças autogerenciadas também podem especificar outras restrições, como o tipo de locação.

Considerações sobre o Amazon RDS for Oracle e o Amazon RDS para bancos de dados Db2

Quando você adiciona informações do produto para configurar a descoberta automática dos bancos de dados Amazon RDS for Oracle ou Amazon RDS for Db2, os seguintes requisitos se aplicam:

- O tipo de contagem de licenças compatível é vCPU.
- Não há suporte para regras.
- Não há suporte para limites rígidos de licenças.
- Você pode monitorar uma versão do produto por licença autogerenciada.
- Você não pode rastrear bancos de dados do Amazon RDS e outros produtos usando a mesma licença autogerenciada.

Para criar uma licença autogerenciada usando o console

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Escolha Criar licença autogerenciada.
4. No painel Detalhes da configuração, forneça as seguintes informações:
 - Nome da licença autogerenciada — O nome da licença autogerenciada.
 - Descrição — Uma descrição opcional da licença autogerenciada.
 - Tipo de licença — O modelo de contagem para esta licença (vCPUs, Núcleos, Soquetes ou Instâncias).
 - Número de <opção>: a opção exibida depende do tipo de licença. Quando o limite de licenças for excedido, o License Manager notificará você (limite flexível) ou impedirá a implantação de um atributo (limite rígido).
 - Aplicar limite de licença — Quando selecionado, o limite será rígido.

- Regras — Uma ou mais regras. Para cada regra, selecione um tipo, forneça um valor e escolha Adicionar regra. Os tipos de regra exibidos dependem do tipo de licença. Por exemplo, valores mínimos, valores máximos e locação. Se você não especificar um tipo de locação, todos serão aceitos.
5. (Opcional) No painel de Regras de descoberta automatizada, faça o seguinte:
 - a. Escolha o nome do produto, o tipo de produto e o tipo de atributo para descobrir e rastrear usando a [descoberta automatizada](#).
 - b. Selecione Parar de rastrear instâncias quando o software for desinstalado para disponibilizar a licença para reutilização depois que o License Manager detectar que o software foi desinstalado e que qualquer período de afinidade de licença tenha passado.
 - c. (Opcional) Se sua conta for uma conta de gerenciamento do License Manager para uma Organizations, você tem a opção de definir atributos a serem excluídos da descoberta automática. Para fazer isso, selecione Adicionar regra de exclusão, escolha a propriedade para filtrar, IDs de AWS conta e tags de recursos são aceitos e, em seguida, insira as informações para identificar essa propriedade.
 6. (Opcional) Expanda o painel Tags para adicionar uma ou mais tags à sua licença autogerenciada. As tags são pares de chave-valor. Forneça as seguintes informações para cada tag:
 - Chave - O nome pesquisável da chave.
 - Valor - O valor da chave.
 7. Selecione Enviar.

Para criar uma licença autogerenciada usando a linha de comando

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

Como compartilhar uma licença autogerenciada

Você pode usar AWS Resource Access Manager para compartilhar suas licenças autogerenciadas com qualquer AWS conta ou por meio de. AWS Organizations Para obter mais informações, consulte [Compartilhando seus AWS recursos](#) no Guia AWS RAM do usuário.

Cota de contas compatíveis

Se você habilitou o compartilhamento de licenças AWS License Manager antes de 14 de outubro de 2023, sua cota para o número máximo de contas que o License Manager suporta em sua organização será menor do que o novo máximo padrão. Você pode aumentar essa cota usando as operações de AWS RAM API fornecidas na seção a seguir. Para obter mais informações sobre as cotas padrão no License Manager, consulte [Cotas para trabalhar com licenças](#) no Guia Referência geral da AWS .

Pré-requisitos

Para concluir o procedimento seguinte, você deve fazer login como entidade principal na conta de gerenciamento da organização que tem as seguintes permissões:

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

Como aumentar a cota de contas compatíveis

O procedimento a seguir aumentará sua cota atual de `Number of accounts per organization for License Manager` até o atual padrão máximo.

Para aumentar a cota de contas compatíveis no License Manager

1. Use o [describe-organization](#) AWS CLI comando para determinar o ARN da sua organização usando a operação:

```
aws organizations describe-organization

{
  "Organization": {
    "Id": "o-abcde12345",
    "Arn": "arn:aws:organizations::111122223333:organization/o-abcde12345",
    "FeatureSet": "ALL",
    "MasterAccountArn": "arn:aws:organizations::111122223333:account/o-abcde12345/111122223333",
    "MasterAccountId": "111122223333",
    "MasterAccountEmail": "name+orgsidentifier@example.com",
```

```
"AvailablePolicyTypes": [  
  {  
    "Type": "SERVICE_CONTROL_POLICY",  
    "Status": "ENABLED"  
  }  
]  
}  
}
```

2. Use o [get-resource-shares](#) AWS CLI comando para determinar o ARN da sua organização usando a operação:

```
aws ram get-resource-shares --resource-owner SELF --tag-filters  
tagKey=Service,tagValues=LicenseManager --region us-east-1  
  
{  
  "resourceShares": [  
    {  
      "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",  
      "name": "licenseManagerResourceShare-111122223333",  
      "owningAccountId": "111122223333",  
      "allowExternalPrincipals": true,  
      "status": "ACTIVE",  
      "tags": [  
        {  
          "key": "Service",  
          "value": "LicenseManager"  
        }  
      ],  
      "creationTime": "2023-10-04T12:52:10.021000-07:00",  
      "lastUpdatedTime": "2023-10-04T12:52:10.021000-07:00",  
      "featureSet": "STANDARD"  
    }  
  ]  
}
```

3. Use o [enable-sharing-with-aws-organization](#) AWS CLI comando para ativar o compartilhamento de recursos com AWS RAM:

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

```
"returnValue": true
}
```

Você pode usar o [list-aws-service-access-for-organization](#) AWS CLI comando para verificar se os diretores de serviço das listas de Organizations estão habilitados para o License Manager e 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

Pode levar até seis horas AWS RAM para concluir essa operação em sua organização. Esse processo precisa estar concluído antes que você possa continuar.

- Use o [associate-resource-share](#) AWS CLI comando para associar seu compartilhamento de recursos do License Manager à sua organização:

```
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
}
]
```

Você pode usar o [get-resource-share-associations](#) AWS CLI comando para validar se a associação de compartilhamento de recursos status é 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
    }
  ]
}
```

Como editar uma licença autogerenciada

É possível editar os valores dos seguintes campos em uma licença autogerenciada:

- Nome da licença autogerenciada
- Descrição
- Número de <opção>
- Aplicar o limite do tipo de licença

Para editar uma licença autogerenciada

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Selecione a licença autogerenciada.
4. Selecione Ações, Editar.
5. Edite os detalhes conforme necessário e escolha Atualizar.

Para editar uma licença autogerenciada usando a linha de comando

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

Como desativar uma licença autogerenciada

Quando você desativa uma licença autogerenciada, os atributos existentes que usam a licença não são afetados e as AMIs que usam a licença ainda podem ser executadas. No entanto, o consumo da licença não é mais rastreado.

Quando uma licença autogerenciada é desativada, ela não deve estar anexada a nenhuma instância em execução. Após a desativação, execuções não poderão ser realizadas com a licença autogerenciada.

Para desativar uma licença autogerenciada

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Selecione a licença autogerenciada.
4. Escolha Ações, Desativar. Quando a confirmação for solicitada, escolha Desativar.

Para desativar uma licença autogerenciada usando a linha de comando

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

Como excluir uma licença autogerenciada

Antes de excluir uma licença autogerenciada, é preciso desassociar todos os atributos. Você pode excluir uma licença autogerenciada se precisar recomeçar com novas regras de licenciamento. Se os termos de licenciamento de seus fornecedores de software mudarem, você poderá desassociar os atributos existentes, excluir a licença autogerenciada, criar uma nova licença autogerenciada para refletir os termos atualizados e associá-la aos atributos existentes.

Para excluir uma licença autogerenciada usando o console

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Escolha o nome para abrir a página de detalhes da licença.
4. Selecione cada um dos atributos (individualmente ou em lote) e escolha Desassociar atributo. Repita até a lista estar vazia.
5. Escolha Ações, Excluir. Quando a confirmação for solicitada, escolha Excluir.

Para excluir uma licença autogerenciada usando a linha de comando

- [delete-license-configuration](#) (AWS CLI)
- [Remover - Licm LicenseConfiguration](#) (AWS Tools for PowerShell)

Regras de licença no License Manager

Depois que as regras de licença autogerenciada estiverem em vigor, elas podem ser anexadas aos mecanismos de inicialização relevantes, que podem impedir diretamente a implantação de novos atributos que não sejam compatíveis. Os usuários de sua organização podem inicializar facilmente instâncias do EC2 a partir de AMIs designadas, e os administradores podem monitorar o inventário de licenças pelo painel integrado do License Manager. Os controles de execução e os alertas do painel permitem uma aplicação mais fácil da conformidade.

⚠ Important

AWS não participa do processo de auditoria com fornecedores de software. Os clientes são responsáveis pela compatibilidade e assumem a responsabilidade de compreender e capturar com cuidado as regras do License Manager com base nos contratos de licenciamento.

O controle de licenças funciona a partir das regras de tempo anexadas a uma instância até seu encerramento. Você define seus limites de uso e regras de licenciamento, e o rastrea implantações e, ao mesmo tempo, alerta você sobre violações de regra. Se você tiver configurado limites rígidos, o License Manager poderá evitar que atributos sejam iniciados.

Quando um servidor rastreado é interrompido ou encerrado, sua licença é liberada e retornada ao grupo de licenças disponíveis.

Como as organizações têm diferentes abordagens para operações e compatibilidade, o License Manager oferece suporte a vários mecanismos de execução:

- Associação manual de configurações de licença com AMIs – para controle de licenças do sistema operacional ou outro software, você pode anexar regras de licenciamento às AMIs antes de publicá-las para uso mais amplo em sua organização. Qualquer implantação dessas AMIs será rastreada automaticamente com o sem a necessidade de ações adicionais por parte dos usuários. Você também pode anexar regras de licenciamento aos seus mecanismos de criação de AMI atuais, como [Systems Manager Automation](#), [VM Import/Export](#) e [Packer](#).
- Modelos de lançamento do Amazon EC2 e AWS CloudFormation — [Se anexar regras de licenciamento às AMIs não for uma opção preferida, você pode especificá-las como parâmetros opcionais nos modelos ou modelos de lançamento do EC2.](#) [AWS CloudFormation](#) Implantações com esses modelos são rastreadas usando o License Manager. Você pode aplicar regras em modelos ou AWS CloudFormation modelos de execução do EC2 especificando uma ou mais IDs de licença autogerenciadas no campo de licenças autogerenciadas.

AWS trata os dados de rastreamento de licenças como dados confidenciais do cliente, acessíveis somente por meio da AWS conta proprietária. AWS não tem acesso aos seus dados de rastreamento de licenças. Você controla seus dados de controle de licenças e pode excluí-los a qualquer momento.

Associando licenças e AMIs autogerenciadas

O procedimento a seguir demonstra como associar licenças autogerenciadas a AMIs usando o console do License Manager. O procedimento pressupõe que você tenha pelo menos uma licença autogerenciada existente. Você pode associar configurações de licença a qualquer AMI a que você tenha acesso, seja de propriedade ou compartilhada. Se uma AMI foi compartilhada com você, poderá associá-la à licença autogerenciada na conta atual. Caso contrário, você pode especificar se a AMI está associada à licença autogerenciada em todas as contas ou somente na conta atual.

Se você associar uma AMI a uma licença autogerenciada em todas as contas, poderá acompanhar as execuções de instâncias da AMI em todas as contas. Quando um limite rígido é atingido, o License Manager bloqueia a execução de instâncias adicionais. Quando um limite suave é atingido, o License Manager notifica sobre a execução de instâncias adicionais.

Se você copiar uma AMI dentro da mesma região e essa AMI tiver configurações de licença associadas, essas configurações de licença serão automaticamente associadas à nova AMI. Quando você executa uma instância a partir da nova AMI, o License Manager a rastreia. Da mesma forma, se você criar uma nova AMI a partir de uma instância em execução que tenha configurações de licença associadas, essas configurações de licença serão automaticamente associadas à nova AMI, e o License Manager rastreará as instâncias que você executa a partir da nova AMI.

Warning

O License Manager não oferece suporte ao rastreamento de instâncias entre regiões. Se você copiar uma AMI que tenha configurações de licença associadas para uma região diferente, o License Manager bloqueia todas as execuções de instância da nova AMI.

Para associar uma licença autogerenciada e uma AMI

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Escolha o nome para abrir a página de detalhes da licença. Para visualizar as AMIs atualmente associadas, escolha AMIs associadas.
4. Escolha Associar AMI.
5. Para AMIs disponíveis, selecione uma ou mais AMIs e escolha Associar.

- Se sua conta possuir pelo menos uma das AMIs, você será solicitado a escolher um escopo de associação de AMI para as AMIs que você possui. Todas as AMIs que foram compartilhadas com outra conta são associadas somente à sua conta. Selecione a opção Confirmar.
- Todas as AMIs que foram compartilhadas com outra conta são associadas somente à sua conta.

As AMIs recém-associadas agora aparecem na guia AMIs associadas na página de detalhes da licença.

Desassociando licenças e AMIs autogerenciadas

O procedimento a seguir demonstra como desassociar licenças autogerenciadas a AMIs usando o console do License Manager. Você não pode desassociar uma AMI com o registro cancelado. O License Manager verifica as AMIs canceladas a cada 8 horas e as desassocia automaticamente.

Para desassociar uma licença autogerenciada e uma AMI

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Escolha o nome para abrir a página de detalhes da licença.
4. Escolha AMIs associadas.
5. Selecione o link e escolha Desassociar AMI.

Relatórios de uso no License Manager

Com o AWS License Manager é possível acompanhar o histórico das licenças autogerenciadas agendando instantâneos periódicos do uso de licença. Ao configurar relatórios de uso, o License Manager carregará automaticamente relatórios de suas licenças autogerenciadas em um bucket do S3 com base nas especificações. Anteriormente, os relatórios de uso eram chamados de geradores de relatórios. É possível configurar vários relatórios de uso para monitorar com eficácia as configurações de diferentes tipos de licença no ambiente.

Note

O AWS License Manager não armazena seus relatórios. Os relatórios do License Manager são publicados diretamente no bucket do S3. Quando um relatório de uso é excluído, os relatórios não são mais publicados no bucket do S3.

Criar relatórios de uso

Ao criar um relatório de uso, você especifica um tipo de licença autogerenciada a ser monitorada pelo License Manager, um intervalo de frequência, que define a frequência com que os relatórios devem ser gerados, e um tipo de relatório. Todos os relatórios são gerados no formato CSV e publicados em um bucket do S3. Um relatório de uso pode produzir um ou mais tipos de relatório, descritos a seguir.

Relatório resumo de licenças autogerenciadas

Esse tipo de relatório contém informações sobre o número de licenças consumidas e detalhes sobre a licença autogerenciada. O tipo de licença autogerenciada monitorada lista detalhes como a contagem de licenças, as regras de licença e a distribuição de licenças nos diferentes tipos de atributos.

Relatório de uso de atributos

Esse tipo de relatório fornece detalhes sobre seus atributos monitorados e o consumo de licenças. Cada atributo rastreado que usa o tipo de licença autogerenciada especificado é listado com detalhes como o ID da licença, o status do atributo e o ID da conta da AWS que possui o atributo.

Como criar um relatório de uso

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação, escolha Relatórios de uso.
3. Escolha Criar relatório de uso e, no painel Criar relatório de uso, defina os parâmetros do relatório:
 - a. Insira um nome e uma descrição opcional para o relatório.
 - b. Selecione um tipo de licença autogerenciada na lista suspensa. É o tipo de licença sobre o qual o relatório de uso gerará dados.

- c. Escolha os tipos de relatório a serem gerados.
 - d. Escolha a frequência com que o License Manager publicará os relatórios. Você pode escolher A cada 24 horas, A cada 7 dias ou A cada 30 dias.
 - e. (Opcional) Adicione tags para rastrear o atributo relatório de uso.
4. Selecione Criar relatório de uso.

Um novo relatório de uso começará a publicar relatórios em até 60 minutos.

Se ainda não tiver um bucket do S3 associado à sua conta, o License Manager criará um novo bucket do Amazon S3 em sua conta quando você criar um relatório de uso. Caso a Pesquisa de inventário entre contas já tenha sido ativada, os relatórios serão enviados para o bucket do S3 criado pelo License Manager quando a Pesquisa de inventário entre contas for ativada.

Os relatórios são armazenados no bucket com o seguinte padrão de URI do Amazon S3:

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

Editar relatórios de uso

É possível visualizar e fazer alterações nos relatórios de uso no console do License Manager a qualquer momento. A tabela relatórios de uso lista todos os relatórios de uso criados para sua conta. A partir da tabela, você tem uma visão geral dos diferentes relatórios, pode ir para o bucket do Amazon S3 associado aos seus relatórios de uso e visualizar o status da geração de relatórios.

Para editar um relatório de uso

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação, escolha Relatórios de uso.
3. Escolha o relatório de uso que deseja editar na tabela e selecione Exibir detalhes.
4. Selecione Editar para fazer alterações no relatório de uso.
5. Faça as alterações desejadas no relatório de uso e escolha Salvar alterações.

Após a atualização, será gerado um novo relatório de uso em até uma hora.

Note

Se alterar o nome do relatório de uso, os futuros relatórios serão enviados para uma nova pasta no bucket do License Manager S3, refletindo o novo nome.

Excluir um relatório de uso

A exclusão de um relatório de uso interrompe a geração de novos relatórios. No entanto, o bucket do Amazon S3 e todos os relatórios anteriores não são afetados.

Note

Não será possível excluir uma licença autogerenciada da conta que tiver um relatório de uso associado. Primeiro você deve excluir o relatório de uso.

Para editar um relatório de uso

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação, escolha Relatórios de uso.
3. Escolha o relatório de uso que deseja editar na tabela e selecione Exibir detalhes.
4. Selecione Excluir. Essa ação exclui permanentemente o relatório de uso.

Conversões de tipo de licença no License Manager

Com o License Manager, você pode alterar o tipo de licença entre o licenciamento AWS fornecido e o modelo Bring Your Own License (BYOL) ou o modelo Bring your Own Subscription (BYOS), conforme as necessidades de sua empresa mudarem. É possível fazer isso sem reimplantar suas workloads existentes.

Você pode otimizar seu inventário de licenças para os seguintes cenários usando a conversão:

Migrar workloads on-premises para o Amazon EC2

Durante a migração, você pode implantar sua carga de trabalho no Amazon Elastic Compute Cloud (Amazon AWS EC2) e usar as licenças fornecidas. Quando a migração estiver concluída,

use a Conversão de tipo de licença do License Manager para alterar o tipo de licença de suas instâncias. Você pode mudar para BYOL ou BYOS para poder usar as licenças que foram liberadas durante a migração.

Continue executando workloads com contratos de licença expirados

Você pode usar a conversão do tipo de licença do License Manager para mudar de BYOL ou BYOS para licenças AWS fornecidas. Essa opção permite que você continue executando suas cargas de trabalho com licenças de software totalmente compatíveis, fornecidas por um modelo flexível de licenciamento AWS go. pay-as-you Você pode fazer isso caso seu contrato de licença com o fornecedor do software do sistema operacional (A Microsoft ou a Canonical, por exemplo) estiver prestes a expirar e você não planejar renová-lo.

Otimize custos

Para cargas de trabalho pequenas ou irregulares, as instâncias com licenças AWS fornecidas (licença incluída) podem ser mais econômicas. Quando você opta por usar BYOL ou BYOS, essas opções podem exigir um compromisso de longo prazo. Nesse caso, você pode usar a Para obter mais informações do License Manager para mudar suas instâncias para licença incluída, otimizando os custos relacionados ao licenciamento. Se suas instâncias foram iniciadas a partir de sua própria imagem de máquina virtual (VM), você pode voltar para BYOL ou BYOS. Isso pode ser feito quando a workload for mais estável ou previsível.

Manutenção estendida

Se o seu sistema operacional Ubuntu chegou ao fim do suporte padrão, você pode adicionar uma assinatura paga do Ubuntu Pro. Assinar o Ubuntu Pro fornece atualizações de segurança durante um longo período de tempo. Para obter mais informações, consulte [Ubuntu Pro](#) na documentação da Canonical.

Tópicos

- [Tipos de licença elegíveis para a conversão de tipo de licença](#)
- [Pré-requisitos da conversão](#)
- [Como converter um tipo de licença](#)
- [Conversão de locação](#)
- [Solução de problemas de conversão de tipo de licença](#)

Tipos de licença elegíveis para a conversão de tipo de licença

Você pode usar a conversão de tipo de licença do License Manager com versões compatíveis e combinações de licenças do Windows Server e do Microsoft SQL Server. Você também pode usar a conversão de tipo de licença com assinaturas do Ubuntu Linux.

Sumário

- [Tipos de licença elegíveis para Windows e SQL Server](#)
 - [Edições do SQL Server](#)
 - [Versão do SQL Server](#)
 - [Valores da operação de uso](#)
 - [Compatibilidade de mídia](#)
 - [Caminhos de conversão](#)
- [Tipos de assinatura elegíveis para Linux](#)

Tipos de licença elegíveis para Windows e SQL Server

Important

Instâncias originalmente lançadas a partir de uma imagem de máquina da Amazon (AMI) fornecida pela Amazon não estão qualificadas para conversão para BYOL.

O Windows e o SQL Server devem atender a determinados requisitos para se qualificarem para a conversão de tipo de licença.

Tópicos

- [Edições do SQL Server](#)
- [Versão do SQL Server](#)
- [Valores da operação de uso](#)
- [Compatibilidade de mídia](#)
- [Caminhos de conversão](#)

Edições do SQL Server

O License Manager oferece suporte às seguintes edições do SQL Server:

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

Versão do SQL Server

O License Manager oferece suporte às seguintes versões do 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 da operação de uso

Uma conversão de tipo de licença altera o valor da operação de uso associado à sua instância. Os valores da operação de uso para cada sistema operacional compatível são fornecidos na tabela a seguir. Para obter mais informações, consulte os [campos de informações de faturamento da AMI](#).

Detalhes do sistema operacional	Operação de uso
Windows Server como BYOL	RunInstances0800
Windows Server como BYOL	RunInstances0800
SQL Server (qualquer edição) como BYOL	RunInstances0800
Windows Server como licença incluída	RunInstances:002

Detalhes do sistema operacional	Operação de uso
Windows Server como licença incluída SQL Server (qualquer edição) como BYOL	RunInstances:002
Windows Server como licença incluída SQL Server Web como licença incluída	RunInstances0:02
Windows Server como licença incluída SQL Server Standard como licença incluída	RunInstances0:006
Windows Server como licença incluída SQL Server Enterprise como licença incluída	RunInstances0:012

Compatibilidade de mídia

A tabela a seguir confirma quais mídias podem ser usadas em quais modelos de licenciamento de instância.

Origem	Destino	
	BYOL	Licença incluída
AWS imagem fornecida do Windows Server	Não	Sim
AWS imagem fornecida do SQL Server	Não	Sim
Sua mídia do Windows Server ¹	Sim	Sim
Sua mídia do SQL Server ²	Sim	Sim

¹ Indica que a instância foi originalmente iniciada a partir de sua própria máquina virtual (VM) importada. Você pode importar sua VM usando um serviço como o [VM Import/Export](#) ou o [AWS Application Migration Service](#).

² Indica que você adquiriu sua própria mídia de instalação do SQL Server (.iso, .exe).

Caminhos de conversão

A tabela a seguir confirma se o modelo de licença de origem pode ser convertido para outro modelo, entre BYOL e licença incluída. Para ter mais informações, consulte [Como converter um tipo de licença](#).

Important

- O Windows Server como BYOL com o SQL Server como licença incluída é uma configuração incompatível.
- As conversões especificadas como “Não necessárias” não alterarão o valor da operação de uso.

Origem	Destino					
	Windows Server como BYOL	Windows Server como licença incluída	Windows Server como BYOL	Windows Server como BYOL	Windows Server como licença incluída	Windows Server como licença incluída
			SQL Server como BYOL	SQL Server como BYOL	SQL Server como licença incluída	SQL Server como licença incluída
Windows Server como	Não é necessário	Sim	Não é necessário	Sim ¹	Sem suporte	Sim ¹

Origem	Destino					
BYOL (sua mídia)						
Windows Server como licença incluída (sua mídia)	Sim ²	Não é necessário	Sim ^{1, 2}	Não é necessário ³	Sem suporte	Sim ¹
Windows Server como licença incluída (imagem AWS fornecida)	Não x	Não é necessário	Não x	Não é necessário ³	Sem suporte	Sim ¹
Windows Server como BYOL (sua mídia)	Não é necessário ⁴	Sim	Não é necessário	Sim	Sem suporte	Sim
SQL Server como BYOL (sua mídia)						

Origem	Destino					
Windows Server como licença incluída (sua mídia)	Sim ²	Não é necessário ⁴	Sim ²	Não é necessário	Sem suporte	Sim
SQL Server como BYOL (sua mídia)						
Windows Server como licença incluída (imagem AWS fornecida)	Não <i>x</i>	Não é necessário ⁴	Não <i>x</i>	Não é necessário	Sem suporte	Sim
SQL Server como BYOL (sua mídia)						

Origem	Destino					
Windows Server como BYOL (sua mídia)	Sem suporte	Sem suporte	Sem suporte	Sem suporte	Sem suporte	Sem suporte
SQL Server como licença incluída						
Windows Server como licença incluída (imagem AWS fornecida ou sua mídia)	Não x	Não x	Não x	Não x	Sem suporte	Não é necessário
SQL Server como licença incluída (imagem AWS fornecida)						

Origem	Destino					
Windows Server como licença incluída (sua mídia)	Sim ^{2, 5, 6}	Sim ⁵	Sim ²	Sim	Sem suporte	Não é necessário
SQL Server como licença incluída (sua mídia)						
Windows Server como licença incluída (imagem AWS fornecida)	Não x	Sim ⁵	Não x	Sim	Sem suporte	Não é necessário
SQL Server como licença incluída (sua mídia)						

x Você deve implantar uma nova instância com uma configuração alternativa, pois a conversão para os tipos de licença de destino não são compatíveis. Para ter mais informações, consulte [Compatibilidade de mídia](#).

Para outros cenários de conversão, talvez seja necessário seguir as etapas a seguir:

- ¹ Primeiro instale o SQL Server antes de converter para “BYOL para SQL Server”.
- ² Primeiro modifique a configuração do Windows para usar seu próprio servidor KMS para ativação da licença. Para ter mais informações, consulte [Convert Windows Server from license included to BYOL](#).
- ³ Primeiro instale o SQL Server ao converter de uma origem sem o SQL Server para um destino com o SQL Server (independentemente do tipo de licença).
- ⁴ Primeiro desinstale o SQL Server ao converter de uma origem com o SQL Server para um destino sem o SQL Server (independentemente do tipo de licença).
- ⁵ Primeiro desinstale o SQL Server antes de converter para o SQL Server com licença incluída.
- ⁶ Primeiro execute as etapas para ² e ⁵. Depois que essas etapas forem concluídas, converta o tipo de licença para Windows Server como licença incluída e, em seguida, converta o tipo de licença mais uma vez para Windows Server como BYOL.

Tipos de assinatura elegíveis para Linux

A conversão de tipo de licença está disponível para versões compatíveis do Ubuntu. As versões compatíveis incluem atualizações como o Ubuntu 18.04.1 LTS. Quando você converte uma assinatura para o Ubuntu Pro, as atualizações de segurança são fornecidas por mais cinco anos. Para obter mais informações, consulte [Ubuntu Pro](#) na documentação da Canonical.

Você pode usar a conversão de tipo de licença com as seguintes versões do Ubuntu:

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

Detalhes do sistema operacional	Operação de uso
Linux/UNIX	RunInstances
Ubuntu Pro	RunInstances0g00

Caminhos de conversão para Linux

Você pode converter qualquer versão compatível do Ubuntu LTS para o Ubuntu Pro. Para converter do Ubuntu Pro para o Ubuntu LTS, faça uma solicitação para o AWS Support. Para obter mais informações, consulte [Criação de um caso de suporte](#).

Pré-requisitos da conversão

Para converter tipos de licença com o License Manager, existem pré-requisitos gerais e específicos de cada sistema operacional.

Tópicos

- [Geral](#)
- [Windows](#)
- [Linux](#)

Geral

Você deve atender aos seguintes pré-requisitos gerais antes de realizar uma conversão de tipo de licença:

- Você Conta da AWS deve estar integrado ao License Manager. Consulte [Começando com AWS License Manager](#).
- A instância de destino deve estar no estado interrompido antes de você converter o tipo de licença. Para obter mais informações, consulte [Encerrar e iniciar sua instância](#) no Guia do Usuário do Amazon EC2.
- Se a proteção contra interrupção estiver ativada na instância de destino, o processo de conversão falhará. Para ter mais informações, consulte [Solução de problemas de conversão de tipo de licença](#).
- A instância de destino deve ser configurada com o AWS Systems Manager Inventory. Para obter mais informações, consulte [Configuração do Systems Manager para instâncias do EC2](#) e [Inventário do AWS Systems Manager](#) no Guia do usuário do AWS Systems Manager .
- Sua usuário ou perfil precisa incluir as seguintes permissões:
 - `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 obter mais informações sobre o Systems Manager Inventory, consulte [AWS Systems Manager Inventory](#).

Windows

As instâncias do Windows devem atender aos seguintes pré-requisitos:

- Instâncias originalmente lançadas a partir de uma imagem de máquina da Amazon (AMI) fornecida pela Amazon não estão qualificadas para conversão para BYOL. A instância original do Amazon EC2 deve ser executada a partir da sua própria imagem de máquina virtual (VM). Para obter mais informações sobre a conversão de uma VM para o Amazon EC2, consulte [VM Import/Export](#).
- Para alterar sua licença do SQL Server para BYOL, o SQL Server deve ter sido instalado usando sua própria mídia.

Linux

As instâncias do Linux devem atender aos seguintes pré-requisitos:

- As instâncias precisam estar executando o Ubuntu LTS.
- O Ubuntu Pro Client precisa estar instalado no seu sistema operacional Ubuntu.
 - Para confirmar se o Ubuntu Pro Client está instalado, execute o seguinte comando:

```
pro --version
```

- Se o comando não for encontrado ou se a versão precisar ser atualizada, execute o seguinte comando para instalar o Ubuntu Pro Client:

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

- As instâncias devem ser capazes de alcançar vários endpoints para ativar a assinatura do Ubuntu Pro e receber atualizações. Você deve permitir que o tráfego que sai da sua instância pela porta TCP 443 alcance os seguintes endpoints:
 - `contracts.canonical.com`: usado para ativação do Ubuntu Pro.
 - `esm.ubuntu.com`: usado para acesso ao repositório APT para a maioria dos serviços.
 - `api.snapcraft.io`: usado para instalar e executar snaps.
 - `dashboard.snapcraft.io`: usado para instalar e executar snaps.
 - `login.ubuntu.com`: usado para instalar e executar snaps.
 - `cloudfront.cdn.snapcraftcontent.com`: usado para baixar de redes de desenvolvimento de conteúdo (CDNs).
 - `livepatch.canonical.com`: usado para baixar correções do servidor Livepatch.

Para obter mais informações, consulte [Ubuntu Pro Client network requirements](#) na documentação do Ubuntu Pro Client e [Network requirements](#) na documentação do Canonical Snapcraft.

Como converter um tipo de licença

Você pode converter licenças do Windows, licenças do Microsoft SQL Server e assinaturas do Ubuntu Linux usando o console do License Manager ou o AWS CLI. Talvez seja necessário concluir etapas adicionais para converter a licença ou a assinatura no sistema operacional da instância.

Você pode converter tipos de licença usando o console do License Manager ou o AWS CLI. Quando você cria uma conversão de tipo de licença, o License Manager valida os produtos de faturamento na sua instância. Se essas validações preliminares forem bem-sucedidas, o License Manager ~~cria uma conversão de tipo de licença. Você pode verificar o status de uma conversão de tipo de~~

licença usando os `get-license-conversion-task` AWS CLI comandos `list-license-conversion-tasks` e.

O License Manager pode atualizar os atributos associados às suas licenças autogerenciadas como parte de uma conversão de tipo de licença. Especificamente, para qualquer licença autogerenciada com regras de descoberta automatizada do tipo `License Included`, o License Manager desassocia o atributo da licença durante conversão, se a regra `license included` excluir explicitamente o atributo.

Por exemplo, se sua licença autogerenciada contiver duas regras de descoberta automatizada e cada regra excluir o Windows Server com licença incluída, uma conversão de BYOL para Windows Server com licença incluída resultará na dissociação entre a instância e a licença autogerenciada. No entanto, se apenas uma das duas regras contiver uma regra `License Included`, a instância não será dissociada.

Não inicie nem interrompa sua instância enquanto a conversão de tipo de licença estiver em andamento. Quando a conversão é bem-sucedida, seu status muda de `IN_PROGRESS` para `SUCCEEDED`. Se o License Manager encontrar problemas durante o fluxo de trabalho, ele atualiza o status da conversão para `FAILED` e a mensagem de status vira uma mensagem de erro.

Note

As informações do produto de faturamento na AMI usadas para iniciar uma instância não mudam quando você converte o tipo de licença. Para recuperar informações de faturamento precisas, use a API [DescribeInstances](#) do Amazon EC2. Além disso, se você tiver fluxos de trabalho existentes que pesquisam informações de faturamento de AMIs, atualize esses fluxos de trabalho para que eles usem `DescribeInstances`.

Sumário

- [Converta um tipo de licença para Windows e SQL Server](#)
 - [Limites da conversão de tipo de licença](#)
 - [Como converter um tipo de licença usando o console do License Manager](#)
 - [Converta um tipo de licença usando o AWS CLI](#)
- [Como converter um tipo de licença no Linux](#)
 - [Considerações sobre a conversão de tipo de licença](#)
 - [Como converter um tipo de licença usando o console do License Manager](#)

- [Converte um tipo de licença usando o AWS CLI](#)
- [Como remover uma assinatura do Ubuntu Pro](#)

Converte um tipo de licença para Windows e SQL Server

Você pode usar o License Manager Console ou o AWS CLI para converter o tipo de licença das instâncias elegíveis do Windows e do SQL Server.

Tópicos

- [Limites da conversão de tipo de licença](#)
- [Como converter um tipo de licença usando o console do License Manager](#)
- [Converte um tipo de licença usando o AWS CLI](#)

Limites da conversão de tipo de licença

Important

O uso de software da Microsoft está sujeito aos termos de licenciamento da Microsoft. Você é responsável por cumprir os termos de licenciamento da Microsoft. Esta documentação é fornecida por conveniência e você não pode confiar em sua descrição. Esta documentação não constitui aconselhamento jurídico. Se tiver dúvidas sobre seus direitos de licenciamento relacionados aos softwares da Microsoft, consulte sua equipe jurídica, a Microsoft ou seu revendedor da Microsoft.

O License Manager restringe os tipos de conversões de licença que você pode criar de acordo com o Contrato de Licenciamento do Provedor de Serviços da Microsoft (SPLA). Algumas das restrições às quais a conversão de tipo de licença está sujeita estão listadas a seguir. Esta é uma lista incompleta e sujeita a alterações.

- A instância do Amazon EC2 deve ser executada a partir da sua própria imagem de máquina virtual (VM).
- O SQL Server com licença incluída não pode ser executado em um host dedicado.
- Uma instância do SQL Server com licença incluída deve ter pelo menos 4 vCPUs.

Como converter um tipo de licença usando o console do License Manager

Você pode usar o console do License Manager para converter um tipo de licença.

Note

Somente as instâncias em estado interrompido e associadas pelo Inventário do AWS Systems Manager são exibidas.

Para iniciar uma conversão de tipo de licença no console

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação esquerdo, escolha Conversão de tipo de licença e, em seguida, escolha Criar conversão de tipo de licença.
3. Em Sistema operacional de origem, escolha a plataforma da instância que você deseja converter:
 1. Ubuntu LTS
 2. BYOL do Windows
 3. Windows com licença incluída
4. (Opcional) Filtre as instâncias disponíveis especificando um valor para o ID da instância ou para o valor da operação de uso.
5. Selecione as instâncias cujas licenças você deseja converter e escolha Avançar.
6. Insira o valor da operação de uso para o tipo de licença, selecione a licença para a qual você está convertendo e escolha Avançar.
7. Verifique se está satisfeito com a configuração da conversão de tipo de licença e escolha Iniciar conversão.

Você pode ver o status da conversão de tipo de licença no painel correspondente. A coluna “Status da conversão” exibe o status da conversão, como Em andamento, Concluída ou Com falha.

⚠ Important

Se você converter o Windows Server de licença incluída para BYOL, ative o Windows de acordo com seu contrato de licença da Microsoft. Consulte [Convert Windows Server from license included to BYOL](#) Para mais informações.

Converta um tipo de licença usando o AWS CLI

Para iniciar uma conversão de tipo de licença no AWS CLI:

Determine o tipo de licença da instância

1. Verifique se você instalou e configurou o AWS CLI. Para obter mais informações, consulte [Instalar, atualizar e desinstalar o AWS CLI](#) e [Configuração do AWS CLI](#).

⚠ Important

Talvez seja necessário atualizar o AWS CLI para executar determinados comandos e receber todas as saídas necessárias nas etapas a seguir.

2. Verifique se você tem permissões para executar o `create-license-conversion-task-for-resource` AWS CLI comando. Para obter ajuda, consulte [Criar políticas do IAM para o License Manager](#).
3. Para determinar o tipo de licença atualmente associado à sua instância, execute o AWS CLI comando a seguir. Substitua o ID da instância pelo ID da instância cujo tipo de licença você quer determinar.

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

4. O seguinte é um exemplo de resposta ao comando `describe-instances`. Observe que o valor `UsageOperation` é o código de informações de faturamento associado à licença. `UsageOperationUpdateTime` é a hora em que o código de faturamento foi atualizado. Para obter mais informações, consulte [DescribeInstances](#) na Referência de API do Amazon EC2.

```
"InstanceId": "i-0123456789abcdef",
```

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

Note

A operação de uso do Windows Server com o SQL Server Enterprise BYOL é igual à operação de uso do Windows BYOL, já que elas são cobradas de forma idêntica.

Como converter o Windows Server de licença incluída para BYOL

Quando você converte o Windows Server de licença incluída para BYOL, o License Manager não ativa automaticamente o Windows. Você deve alternar o servidor KMS da sua instância do servidor AWS KMS para o seu próprio servidor KMS.

Important

Para converter de licença incluída para BYOL, a instância original do Amazon EC2 deve ser executada a partir da sua própria imagem de máquina virtual (VM). Para obter mais informações sobre a conversão de uma VM para o Amazon EC2, consulte [VM Import/Export](#). Instâncias originalmente lançadas a partir de uma Imagem de Máquina da Amazon (AMI) não estão qualificadas para conversão para BYOL.

Verifique o contrato de licença da Microsoft para determinar quais métodos você pode usar para ativar o Microsoft Windows Server. Por exemplo, se você estiver usando um servidor KMS, obtenha o endereço do servidor KMS da configuração BYOL original da instância.

1. Para converter o tipo de licença da sua instância, execute o comando a seguir, substituindo o ARN pelo ARN da instância que você deseja converter:

```
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 ativar o Windows depois de converter sua licença, aponte o servidor KMS do Windows Server do seu sistema operacional para seus próprios servidores KMS. Faça login na instância do Windows e execute o seguinte comando:

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

Como converter o Windows Server de BYOL para licença incluída

Quando você converte o Windows Server de BYOL para a licença incluída, o License Manager muda automaticamente o servidor KMS da sua instância para o servidor AWS KMS.

Para converter o tipo de licença da sua instância de BYOL para licença incluída, execute o comando a seguir, substituindo o ARN pelo ARN da instância que você deseja converter:

```
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
```

Converta o Windows Server e o SQL Server de BYOL para a licença incluída

É possível alterar vários produtos ao mesmo tempo. Por exemplo, é possível converter o Windows Server e SQL Server em uma única conversão.

Para converter o tipo de licença da sua instância do Windows Server de BYOL para licença incluída, e o SQL Server Standard de BYOL para licença incluída, execute o comando a seguir, substituindo o ARN pelo ARN da instância que você deseja converter:

```
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
```

Como converter um tipo de licença no Linux

Você pode usar o License Manager Console ou o AWS CLI para converter o tipo de licença das instâncias elegíveis do Ubuntu LTS.

Tópicos

- [Considerações sobre a conversão de tipo de licença](#)
- [Como converter um tipo de licença usando o console do License Manager](#)
- [Converta um tipo de licença usando o AWS CLI](#)
- [Como remover uma assinatura do Ubuntu Pro](#)

Considerações sobre a conversão de tipo de licença

Algumas das considerações às quais a conversão de tipo de licença está sujeita estão listadas a seguir. Esta é uma lista incompleta e sujeita a alterações.

- A instância deve estar executando o Ubuntu LTS para converter o tipo de licença para Ubuntu Pro.
- Não é possível usar a conversão de tipo de licença com uma assinatura do Ubuntu Pro. Para remover uma assinatura do Ubuntu Pro, consulte [Como remover uma assinatura do Ubuntu Pro](#).
- O Ubuntu Pro não está disponível como uma instância reservada. Para obter economias significativas em comparação com os preços de instâncias sob demanda, recomendamos usar o Ubuntu Pro com Savings Plans. Para obter mais informações, consulte [Instâncias reservadas](#) no Guia do usuário do Amazon EC2 e [What are Savings Plans?](#) no Guia do usuário do Savings Plans.

Como converter um tipo de licença usando o console do License Manager

Você pode usar o console do License Manager para converter um tipo de licença.

Note

Somente as instâncias em estado interrompido e associadas pelo Inventário do AWS Systems Manager são exibidas.

Para iniciar uma conversão de tipo de licença no console

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação esquerdo, escolha Conversão de tipo de licença e, em seguida, escolha Criar conversão de tipo de licença.
3. Em Sistema operacional de origem, escolha a plataforma da instância que você deseja converter:

1. Ubuntu LTS

2. BYOL do Windows
3. Windows com licença incluída
4. (Opcional) Filtre as instâncias disponíveis especificando um valor para o ID da instância ou para o valor da operação de uso.
5. Selecione as instâncias cujas licenças você deseja converter e escolha Avançar.
6. Insira o valor da operação de uso para o tipo de licença, selecione a licença para a qual você está convertendo e escolha Avançar.
7. Verifique se está satisfeito com a configuração da conversão de tipo de licença e escolha Iniciar conversão.

Você pode ver o status da conversão de tipo de licença no painel correspondente. A coluna “Status da conversão” exibe o status da conversão, como Em andamento, Concluída ou Com falha.

Converta um tipo de licença usando o AWS CLI

Para iniciar uma conversão do tipo de licença no AWS CLI, você deve confirmar se o tipo de licença da sua instância está qualificado e, em seguida, realizar uma conversão do tipo de licença para mudar para a assinatura necessária. Para obter mais informações sobre os tipos de assinatura elegíveis, consulte [Tipos de assinatura elegíveis para Linux](#).

Determine o tipo de licença da instância

Verifique se você instalou e configurou o AWS CLI. Para obter mais informações, consulte [Instalando, atualizando e desinstalando o AWS CLI e Configurando o AWS CLI](#)

Important

Talvez seja necessário atualizar o AWS CLI para executar determinados comandos e receber todas as saídas necessárias nas etapas a seguir. Verifique se você tem permissões para executar o `create-license-conversion-task-for-resource` AWS CLI comando. Para ter mais informações, consulte [Criar políticas do IAM para o License Manager](#).

Para determinar o tipo de licença atualmente associado à sua instância, execute o AWS CLI comando a seguir. Substitua o ID da instância pelo ID da instância cujo tipo de licença você quer determinar:

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

O seguinte é um exemplo de resposta ao comando `describe-instances`. O `UsageOperation` valor é o código de informações de cobrança associado à licença. Um valor de operação de uso "RunInstances" indica que a instância está usando o licenciamento fornecido pela AWS. `UsageOperationUpdateTime` é a hora em que o código de faturamento foi atualizado. Para obter mais informações, consulte [DescribeInstances](#) na Referência de API do Amazon EC2.

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

Como converter para Ubuntu Pro

Ao converter sua instância do Ubuntu LTS para o Ubuntu Pro, você deve ter acesso à Internet de saída na instância para recuperar um token de licença dos servidores da Canonical e instalar o Ubuntu Pro Client. Para ter mais informações, consulte [Pré-requisitos da conversão](#).

Para converter o Ubuntu LTS em Ubuntu Pro:

1. Execute o comando a seguir a partir do AWS CLI enquanto especifica o ARN da sua instância:

```
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. Execute o comando a seguir de dentro da instância para recuperar detalhes sobre o status da sua assinatura do Ubuntu Pro:

```
pro status
```

3. Confirme se sua saída indica que a instância tem uma assinatura válida do 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

```

Como remover uma assinatura do Ubuntu Pro

A Conversão de tipo de licença só pode ser usada para converter do Ubuntu LTS para o Ubuntu Pro. Para converter do Ubuntu Pro para o Ubuntu LTS, faça uma solicitação para o AWS Support. Para obter mais informações, consulte [Criação de um caso de suporte](#).

Conversão de localização

Você pode alterar a localização da instância para melhor se adequar ao seu caso de uso. Você pode usar o AWS CLI comando [modify-instance-placement](#) para alternar entre as seguintes localizações:

- Compartilhada
- Instância Dedicada
- Host Dedicado
- Grupos de atributos de host

Sua conta deve ter um host dedicado com capacidade disponível para iniciar a instância se você quiser mudar para o tipo de localização “Host Dedicado”. Para obter mais informações sobre o trabalho com Hosts Dedicados, consulte [Como trabalhar com Hosts Dedicados](#) no Guia do usuário do Amazon Elastic Compute Cloud.

Para migrar para o tipo de localização de grupos de recursos de host, você deve ter pelo menos um grupo de recursos de host na conta. Para iniciar uma instância em um grupo de recursos de host, a instância deve ter o mesmo conjunto de licenças associadas ao grupo de recursos de host. Para ter mais informações, consulte [Hospede grupos de recursos em AWS License Manager](#).

Limites de conversão de locação

Os limites a seguir se aplicam à conversão de locação:

- O código de faturamento do Linux é permitido em todos os tipos de locação.
- O código de faturamento Windows BYOL não é permitido na locação “Compartilhada”.
- O código de faturamento do Windows Server com licença incluída é permitido em todos os tipos de locação.
- Todos os códigos de faturamento das edições do SQL Server, do Red Hat (RHEL) e do SUSE (SLES) com licença incluída são permitidos nos tipos “Locação compartilhada” e “Instâncias dedicadas”. No entanto, esses códigos de faturamento não são permitidos em Hosts dedicados e grupos de recursos de host.
- Com exceção do Windows Server, códigos de faturamento com licença incluída não são permitidos em Hosts dedicados e grupos de recursos de host.

Alterar a locação de uma instância usando o AWS CLI

Uma instância deve estar no estado `stopped` para ter sua locação alterada.

Para interromper a instância, execute o seguinte comando:

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

Para alterar uma instância de qualquer locação para as locações `default` ou `dedicated`, execute os seguintes 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 alterar uma instância de qualquer locação para a locação `host` com posicionamento automático, execute o seguinte comando:

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

Para alterar uma instância de qualquer localização para a localização host, segmentando um Host Dedicado específico, execute o seguinte comando:

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

Para alterar uma instância de qualquer localização para a localização host usando um Grupo de atributos de Host, execute o seguinte comando:

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

Solução de problemas de conversão de tipo de licença

Tópicos de solução de problemas

- [Ativação do Windows](#)
- [A instância \[instância\] é executada a partir de uma AMI de propriedade da Amazon. Forneça uma instância iniciada originalmente a partir de uma AMI BYOL.](#)
- [Falha ao validar que a instância \[instância\] foi executada a partir de uma AMI BYOL. Certifique-se de que o SSM Agent está em execução na instância.](#)
- [Ocorreu um erro \(InvalidParameterValueException\) ao chamar a CreateLicenseConversionTaskForResource operação: ResourceId - \[instance\] está em um estado inválido para alterar o tipo de licença.](#)
- [A instância \[instância\] do EC2 falhou ao ser interrompida. Verifique se você tem permissões para EC2 StopInstances.](#)

Ativação do Windows

Uma conversão de tipo de licença contém várias etapas. Em alguns casos, quando você converte instâncias do Windows Server de BYOL para a licença incluída, os produtos de faturamento em uma instância são atualizados com êxito. No entanto, o servidor KMS pode não mudar para o servidor KMS da AWS .

Para corrigir esse problema, siga as etapas em [Por que a ativação do Windows falhou na minha instância EC2 do Windows?](#) Assim, você pode ativar o Windows com o Automation runbook [AWSsupport-ActivateWindowsWithAmazonLicense](#) do Systems Manager ou fazer login na instância e alterar manualmente para o servidor KMS da AWS .

A instância [instância] é executada a partir de uma AMI de propriedade da Amazon. Forneça uma instância iniciada originalmente a partir de uma AMI BYOL.

Você deve iniciar sua instância do Amazon EC2 Windows a partir de uma AMI importada para realizar uma conversão de tipo de licença para o modelo Traga sua própria licença (BYOL). Instâncias originalmente lançadas a partir de uma AMI de propriedade da Amazon não estão qualificadas para conversão para BYOL. Para ter mais informações, consulte [Pré-requisitos da conversão](#).

Falha ao validar que a instância [instância] foi executada a partir de uma AMI BYOL. Certifique-se de que o SSM Agent está em execução na instância.

Para que a Conversão de tipo de licença seja bem-sucedida, sua instância deve primeiro estar on-line e ser gerenciada pelo Systems Manager para que o inventário seja coletado. O AWS Systems Manager Agent (SSM Agent) reunirá o inventário da sua instância, que inclui detalhes sobre o sistema operacional. Para obter mais informações, consulte [Verificar o status do SSM Agent e iniciar o agente](#) e [Solução de problemas do SSM Agent](#) no Guia do Usuário do AWS Systems Manager .

Ocorreu um erro (InvalidParameterValueException) ao chamar a **CreateLicenseConversionTaskForResource** operação: ResourceId - [instance] está em um estado inválido para alterar o tipo de licença.

Para realizar uma conversão de tipo de licença, a instância de destino deve estar no estado interrompido. Para obter mais informações, consulte [Pré-requisitos da conversão](#) e [Solução de problemas na interrupção da instância](#) no Guia do usuário do Amazon Elastic Compute Cloud.

A instância [instância] do EC2 falhou ao ser interrompida. Verifique se você tem permissões para EC2 **StopInstances** .

Você deve ter permissões para realizar a API StopInstances do EC2 na instância de destino. Se a proteção contra interrupção estiver ativada na instância de destino, o processo de conversão falhará. Para obter mais informações, consulte [Desabilitar a proteção contra interrupção de uma instância em execução ou interrompida](#) no Guia do usuário do Amazon Elastic Compute Cloud.

Hospede grupos de recursos em AWS License Manager

Hosts Dedicados do Amazon EC2 são servidores físico com capacidade de instância EC2 totalmente dedicada para seu uso. Um grupo de atributos de host é uma coleção de Hosts Dedicados gerenciados como uma única entidade. Conforme você executa instâncias, o License Manager aloca os hosts e executa instâncias neles com base nas configurações que você definiu. Você pode adicionar Hosts Dedicados existentes a um grupo de atributos de host e aproveitar o gerenciamento automatizado de hosts por meio do License Manager. Para obter mais informações, consulte [Hosts Dedicados](#) no Guia do Usuário do Amazon EC2.

Você pode usar esses grupos de recursos de host para separar hosts por finalidade. Por exemplo, hosts de teste de desenvolvimento versus produção, unidade organizacional ou restrição de licença. Depois de adicionar um Host Dedicado a um grupo de recursos de host, você não pode executar instâncias diretamente no Host Dedicado. Execute-as usando o grupo de recursos de host.

Configurações

Você pode definir as seguintes configurações para um grupo de recursos de host:

- **Alocar hosts automaticamente** — Indica se o Amazon EC2 pode alocar novos hosts em seu nome caso a execução de uma instância nesse grupo exceda a capacidade disponível.
- **Liberar hosts automaticamente** — Indica se o Amazon EC2 pode liberar hosts não utilizados em seu nome. Um host não utilizado não tem instâncias em execução.
- **Recuperar hosts automaticamente** — Indica se o Amazon EC2 pode passar instâncias de um host que falhou inesperadamente para um novo host.
- **Licenças autogerenciadas associadas** — As licenças autogerenciadas que podem ser usadas para executar instâncias nesse grupo de atributos de host.
- **(Opcional) Famílias de instâncias** — Os tipos de instâncias que você pode executar. Por padrão, você pode executar qualquer tipo de instância compatível com um Host Dedicado. Se você executar instâncias [baseadas em Nitro](#), poderá executar instâncias de diferentes tipos no mesmo grupo de recursos de host. Caso contrário, você deverá executar somente instâncias do mesmo tipo no mesmo grupo de recursos de host.

Conteúdo

- [Criar um grupo de atributos de host](#)
- [Compartilhar um grupo de recursos de host](#)

- [Adicionar hosts dedicados a um grupo de atributos de host](#)
- [Como executar uma instância em um grupo de atributos de host](#)
- [Modificar um grupo de recursos de host](#)
- [Remover Hosts dedicados de um grupo de recursos de host](#)
- [Excluir um grupo de atributos de host](#)

Criar um grupo de atributos de host

Configure um grupo de recursos de host para permitir que o License Manager gerencie seus hosts dedicados. Para melhor utilizar suas licenças mais caras, associe uma ou mais licenças autogerenciadas baseadas em núcleo ou soquete ao grupo de recursos de host. Para otimizar a utilização de hosts, você pode permitir todas as licenças autogerenciadas baseadas em núcleo ou soquete no grupo.

Como criar um grupo de atributos de host

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação esquerdo, selecione Grupos de atributos de host.
3. Escolha Criar grupo de atributos de host.
4. Para Detalhes do grupo de recursos de hosts, especifique um nome e uma descrição para o grupo de recursos de host.
5. Para Configurações de gerenciamento de host dedicado do EC2, ative ou desative as seguintes configurações conforme necessário:
 - Alocar hosts automaticamente
 - Liberar hosts automaticamente
 - Recuperar hosts automaticamente
6. (Opcional) Para Configurações adicionais, selecione as famílias de instâncias que podem ser executadas no grupo de recursos de host.
7. Para licenças autogerenciadas, selecione uma ou mais licenças autogerenciadas baseadas em núcleo ou soquete.
8. (Opcional) Para Tags, adicione uma ou mais tags.
9. Escolha Criar.

Compartilhar um grupo de recursos de host

Você pode usar AWS Resource Access Manager para compartilhar seus grupos de recursos anfitriões por meio de AWS Organizations. Depois de compartilhar um grupo de recursos de host e uma licença autogerenciada, as contas de membro podem executar instâncias no grupo compartilhado. Os novos hosts são alocados na conta proprietária do grupo de recursos de host. A conta-membro é proprietária das instâncias. Para obter mais informações, consulte o [Guia do usuário do AWS RAM](#).

Adicionar hosts dedicados a um grupo de atributos de host

Você pode adicionar seus hosts existentes a um grupo de recursos de host a partir da AWS API AWS Management Console AWS CLI,, ou. Para adicionar seus anfitriões, você deve ser o proprietário da AWS conta na qual criou o host dedicado e os grupos de recursos do host. Se seu grupo de recursos de host lista licenças autogerenciadas e tipos de instância, o host adicionado precisará ter estes requisitos.

Note

Suponha que você interrompa as instâncias e queira reiniciá-las. Siga as seguintes etapas:

- [Modifique](#) a instância para que ela aponte para o grupo de recursos de host.
- [Associe](#) licenças autogerenciadas para corresponder ao grupo de recursos de host.

Para obter mais informações sobre Grupos de atributos, consulte o [Guia do Usuário do AWS Resource Groups](#).

Siga as etapas a seguir para adicionar um ou mais Hosts dedicados a um grupo de atributos:

1. Faça login no console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Escolha Grupo de atributos de host.
3. Na lista de nomes do grupo de recursos de host, clique no nome do grupo de recursos do host onde o Host Dedicado será adicionado.
4. Escolha Hosts dedicados.
5. Escolha Adicionar.
6. Escolha um ou mais Hosts dedicados para adicionar ao grupo de recursos de host.

7. Escolha Adicionar.

Adicionar o host pode levar de 1 a 2 minutos. Em seguida, ele aparece na lista de Hosts Dedicados.

Como executar uma instância em um grupo de atributos de host

Ao executar uma instância, você pode especificar um grupo de recursos de host. Por exemplo, você pode executar o comando [run-instances](#). É necessário associar uma licença autogerenciada baseada em núcleo ou soquete à AMI.

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

Você também pode usar o console do Amazon EC2. Para obter mais informações, consulte [Iniciar instâncias em um grupo de atributos de host](#) no Guia do usuário do Amazon EC2.

Modificar um grupo de recursos de host

É possível modificar as configurações de um grupo de recursos de host a qualquer momento. O limite de host não pode ficar abaixo do número de hosts existentes no grupo de recursos de host. Você não pode remover um tipo de instância se houver uma instância desse tipo em execução no grupo de recursos de host.

Como modificar um grupo de atributos de host

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação esquerdo, selecione Grupos de atributos de host.
3. Selecione o grupo de recursos de host e escolha Ações, Editar.
4. Modifique as configurações conforme necessário.
5. Escolha Salvar alterações.

Remover Hosts dedicados de um grupo de recursos de host

Quando você remove um host do grupo, a instância em execução nesse host permanece nele. As instâncias anexadas ao grupo de recursos de host permanecem associadas ao grupo, e as

instâncias diretamente anexadas ao host por afinidade mantêm a mesma propriedade. Se você compartilhar o grupo de recursos do host com outras AWS contas, o License Manager removerá automaticamente o host compartilhado e os consumidores receberão um aviso de despejo para mover suas instâncias do host em 15 dias. Para trabalhar com um Host dedicado que foi removido de um grupo de recursos de host, consulte [Como trabalhar com Hosts dedicados](#) no Guia do usuário do Amazon EC2.

Siga as etapas a seguir para adicionar um Host dedicado de um grupo:

1. Faça login no console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Escolha Grupo de atributos de host.
3. Clique no nome do atributo de host do qual você deseja remover um Host Dedicado.
4. Escolha Hosts Dedicados.
5. Escolha o Host dedicado a ser excluído do grupo. Você também pode pesquisar um Host Dedicado por ID, tipo, estado ou zona de disponibilidade.
6. Escolha Remover.
7. Escolha Remover novamente para confirmar.

Excluir um grupo de atributos de host

Você poderá excluir um grupo de recursos de host se ele não tiver hosts.

Como excluir um grupo de atributos de host

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação esquerdo, selecione Grupos de atributos de host.
3. Selecione o host e escolha Ações, Excluir.
4. Quando a confirmação for solicitada, escolha Excluir.

Pesquisa de inventário no License Manager

O License Manager permite descobrir aplicativos on-premises usando o [Inventário do Systems Manager \(SSM\)](#) e anexar regras de licenciamento a eles. Depois que as regras de licenciamento

forem anexadas a esses servidores, você poderá rastreá-las junto com seus AWS servidores no painel do License Manager.

O License Manager não pode, porém, validar regras de licenciamento para esses servidores no momento do lançamento ou encerramento. Para manter informações sobre AWS não-servidores up-to-date, você deve atualizar periodicamente as informações do inventário usando a seção Pesquisa de inventário do console do License Manager.

O Systems Manager armazena dados nos dados de Inventário por 30 dias. Durante esse período, o License Manager conta uma instância gerenciada como ativa até mesmo se ela não for compatível com ping. Assim que os dados de inventário forem eliminados do Systems Manager, o License Manager marcará a instância como inativa e atualizará os dados de inventário local. Para manter as contagens de instâncias gerenciadas precisas, recomendamos cancelar o registro das instâncias manualmente no Systems Manager, para que o License Manager possa executar operações de limpeza.

A consulta do inventário do Systems Manager requer uma sincronização de dados de recursos para armazenar o inventário em um bucket do Amazon S3, e o Amazon Athena para agregar dados de inventário de contas organizacionais AWS Glue e fornecer uma experiência de consulta rápida. Para ter mais informações, consulte [Usando funções vinculadas a serviços para AWS License Manager](#).

O rastreamento de inventário de atributos também é útil se a sua organização não restringir a capacidade dos usuários da AWS de criar instâncias derivadas da AMI ou instalar software adicional nas instâncias em execução. O License Manager fornece um mecanismo para descobrir facilmente essas instâncias e aplicativos usando a pesquisa de inventário. Você pode anexar regras a esses atributos descobertos e rastreá-los e validá-los como instâncias criadas de AMIs gerenciadas.

Conteúdo

- [Trabalhando com a pesquisa de inventário](#)
- [Descoberta automatizada de inventário](#)

Trabalhando com a pesquisa de inventário

O License Manager usa o [Inventário do Systems Manager](#) para descobrir o uso de software on-premises. Depois que você associa uma licença autogerenciada a servidores on-premises, o License Manager coleta periodicamente o inventário de software, atualiza as informações de licenciamento e atualiza seus painéis para criar relatórios sobre o uso.

Tarefas

- [Configuração da pesquisa de inventário](#)
- [Como usar a pesquisa de inventário](#)
- [Como adicionar regras de descoberta automatizada a uma licença autogerenciada](#)
- [Como associar uma licença autogerenciada à pesquisa de inventário](#)
- [Como desassociar uma licença autogerenciada de um atributo](#)

Configuração da pesquisa de inventário

Preencha os seguintes requisitos antes de usar a pesquisa de inventário de atributos:

- Permita a descoberta de inventário entre contas integrando o License Manager à sua AWS Organizations conta. Para ter mais informações, consulte [Configurações em AWS License Manager](#).
- Crie licenças autogerenciadas para gerenciar os servidores e aplicativos. Por exemplo, crie uma licença autogerenciada que reflita os termos do seu contrato de licenciamento com a Microsoft para o SQL Server Enterprise.

Como usar a pesquisa de inventário

Conclua as etapas a seguir para pesquisar no seu inventário de atributos. Você pode pesquisar aplicativos por nome (por exemplo, nomes que começam com “SQL Server”) e pelo tipo de licença incluída (por exemplo, uma licença que não seja para “SQL Server Web”).

Pesquise seu inventário de recursos

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação, escolha Pesquisa de inventário.
3. (Opcional) Você pode especificar as opções de filtro para simplificar os resultados da pesquisa da seguinte maneira.

Recursos do Amazon EC2

Nome do filtro	Descrição	Operadores lógicos	Valores com suporte
ID do recurso	O ID do recurso.		

Nome do filtro	Descrição	Operadores lógicos	Valores com suporte
		Equals, Not equals	
ID da conta	O ID da AWS conta que possui o recurso.	Equals, Not equals	
nome-da-plataforma	A plataforma do sistema operacional para o recurso.	Equals, Not equals, Begins with, Contains	
Nome da aplicação	O nome da aplicação .	Equals, Begins with	
Nome incluído na licença	O tipo de licença incluída.	Equals, Not equals	<ul style="list-style-type: none"> • SQL Server Enterprise • SQL Server Standard • SQL Server Web • Windows Server Datacenter

Nome do filtro	Descrição	Operadores lógicos	Valores com suporte
Tag	<p>Uma chave de tag de metadados e um valor opcional atribuído ao recurso.</p> <p>Observe que o operador Not equals lógico só estará disponível se a descoberta entre contas estiver ativada.</p>	Equals, Not equals	

Recursos do Amazon RDS

Nome do filtro	Descrição	Operadores lógicos	Valores com suporte
Edição do mecanismo	A edição do mecanismo de banco de dados.	Equals	<ul style="list-style-type: none"> • oracle-ee • oracle-se • oracle-se1 • oracle-se2 • db2-se • db2-ae

Nome do filtro	Descrição	Operadores lógicos	Valores com suporte
Pacote de licenças (somente Oracle)	O pacote de gerenciamento associado a uma licença do 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 obter mais informações sobre as licenças de produtos de banco de dados Amazon RDS, consulte as opções de licenciamento do [RDS para Oracle ou as opções de licenciamento do RDS for Db2 no Guia do usuário](#) do Amazon RDS.


Como adicionar regras de descoberta automatizada a uma licença autogerenciada

Depois de adicionar informações do produto à sua licença autogerenciada, o License Manager pode rastrear o uso da licença para as instâncias que têm esses produtos instalados. Para ter mais informações, consulte [Descoberta automatizada de inventário](#).

Para adicionar regras de descoberta automatizada a uma licença autogerenciada

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Abra a página de Pesquisa de inventário.
3. Selecione o atributo e escolha Adicionar regras de descoberta automatizada.

4. Para Licença autogerenciada, selecione uma licença autogerenciada.
5. Especifique os produtos que você quer descobrir e rastrear.
6. (Opcional) Selecione Parar de rastrear instâncias quando o software for desinstalado para disponibilizar a licença para reutilização depois que o License Manager detectar que o software foi desinstalado e que qualquer período de afinidade de licença tenha passado.
7. (Opcional) Para excluir recursos da descoberta automática, selecione Adicionar regra de exclusão.

 Note

As regras de exclusão não se aplicam aos produtos Amazon RDS (como RDS for Oracle e RDS for Db2).

- a. Escolha uma Propriedade para filtrar. Atualmente, há suporte para ID da conta e Tag.
 - b. Insira informações para identificar essa propriedade. Para um ID da conta, especifique o ID da AWS conta de 12 dígitos como o valor. Para Tags, insira um par de chave/valor.
 - c. Repita a etapa 7 para adicionar regras adicionais.
8. Escolha Adicionar.

Como associar uma licença autogerenciada à pesquisa de inventário

Depois de identificar os atributos não gerenciados que você precisa gerenciar, é possível associá-los manualmente a uma licença autogerenciada, em vez de usar a descoberta automatizada.

Para associar uma licença autogerenciada a um atributo

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Abra a página de Pesquisa de inventário.
3. Selecione o atributo e escolha Associar licença autogerenciada.
4. Para Nome da licença autogerenciada, selecione uma licença autogerenciada.
5. (Opcional) Selecione Compartilhar licença autogerenciada com todas as contas-membro.
6. Selecione Associar.

Como desassociar uma licença autogerenciada de um atributo

Se os termos de licenciamento de seus fornecedores de software mudarem, é possível desassociar atributos que foram associados manualmente e excluir a licença autogerenciada.

Para desassociar uma licença autogerenciada de um atributo

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Licença autogerenciada.
3. Selecione o nome da licença autogerenciada.
4. Escolha atributos.
5. Selecione os atributos que você deseja desassociar da licença autogerenciada e depois clique em Desassociar atributo.

Descoberta automatizada de inventário

O License Manager usa o [Inventário do Systems Manager](#) para descobrir o uso de software nas instâncias do Amazon EC2 ou em instâncias on-premises. Você pode adicionar informações do produto à sua licença autogerenciada, e o License Manager rastreará as instâncias que têm esses produtos instalados. Além disso, você pode especificar regras de exclusão com base no seu contrato de licenciamento para decidir quais instâncias excluir. Você pode excluir instâncias pertencentes a IDs de contas da AWS ou instâncias associadas a tags de atributos. Assim, elas não serão consideradas para a descoberta automatizada.

A descoberta automatizada pode ser adicionada a um novo conjunto de licenças, a uma licença autogerenciada existente ou a atributos do seu inventário. As regras para descoberta automatizada podem ser editadas a qualquer momento por meio da CLI usando o comando [UpdateLicenseConfiguration](#) API. Para editar regras no console, exclua a licença autogerenciada existente e crie uma nova.

Para usar a descoberta automatizada, adicione informações do produto à sua licença autogerenciada. Você pode fazer isso ao criar a licença autogerenciada usando a Pesquisa de inventário.

Você não pode desassociar manualmente as instâncias rastreadas pela descoberta automatizada. Por padrão, a descoberta automatizada não dissocia as instâncias rastreadas após a desinstalação do software. Você pode configurar a descoberta automatizada para que ela interrompa o rastreamento de instâncias quando o software for desinstalado.

Depois de fazer isso, você pode acompanhar o uso de licenças pelo painel do License Manager.

Pré-requisitos

- Habilite a pesquisa de inventário entre contas integrando o License Manager à sua AWS Organizations conta. Para ter mais informações, consulte [Configurações em AWS License Manager](#).

Note

Contas individuais podem configurar a descoberta automatizada, mas não podem adicionar regras de exclusão.

- Instale o inventário do Systems Manager em suas instâncias.

Para configurar a descoberta automatizada ao criar uma licença autogerenciada

Você pode configurar regras automatizadas de descoberta e regras de exclusão ao criar uma licença autogerenciada. Para ter mais informações, consulte [Como criar uma licença autogerenciada](#).

Para adicionar regras de descoberta automatizada a uma licença autogerenciada

Use o processo abaixo para adicionar regras de descoberta automatizada às licenças autogerenciadas existentes usando o console. Você também pode fazer isso no painel Pesquisa de inventário, selecionando um ID de atributo e clicando em Adicionar regras de descoberta automatizada.

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Licenças autogerenciadas.
3. Escolha o nome para abrir a página de detalhes da licença.
4. Na guia Regras de descoberta automatizada, escolha Adicionar regras de descoberta automatizada.
5. Especifique os produtos que você quer descobrir e rastrear.
6. (Opcional) Selecione Parar de rastrear instâncias quando o software for desinstalado para disponibilizar a licença para reutilização depois que o License Manager detectar que o software foi desinstalado e que qualquer período de afinidade de licença tenha passado.
7. (Opcional) Para definir atributos a serem excluídos da descoberta automatizada, selecione Adicionar regra de exclusão.

Note

- As regras de exclusão não se aplicam aos produtos de banco de dados do RDS (como Amazon RDS for Oracle e Amazon RDS for Db2).
- As regras de exclusão só estão disponíveis se o [Descoberta de atributos entre contas](#) estiver ativado.

- a. Escolha uma Propriedade para filtrar. Atualmente, há suporte para ID da conta e Tag.
 - b. Insira informações para identificar essa propriedade. Para um ID de conta, especifique o ID da AWS conta de 12 dígitos como o valor. Para Tags, insira um par de chave/valor.
 - c. Repita a etapa 7 para adicionar regras adicionais.
8. Ao terminar, escolha Adicionar para aplicar sua regra de descoberta automatizada.

Licenças concedidas no License Manager

Licenças concedidas são licenças para produtos que sua organização comprou no [AWS Marketplace](#), no [AWS Data Exchange](#), ou diretamente de um vendedor que integrou seu software com direitos gerenciados. Os administradores de licenças podem usar AWS License Manager para controlar o uso dessas licenças e distribuir direitos de uso, conhecidos como direitos, para contas específicas. AWS

As licenças de dados distribuídas aos produtos do AWS Data Exchange estão disponíveis para a AWS conta por meio do AWS Data Exchange. Antes de distribuir licenças de AWS Marketplace, você deve habilitar o compartilhamento de assinaturas. Para obter mais informações, consulte [Compartilhar assinaturas em uma organização](#).

Depois que um administrador de licença distribui o direito de uma AWS Marketplace licença para uma AWS conta e o destinatário aceita e ativa a licença concedida, a assinatura fica disponível para a conta por meio de. AWS AWS Marketplace A conta também tem acesso ao produto. Por exemplo, se um administrador de licença comprar uma Amazon Machine Image (AMI) AWS Marketplace e distribuir um direito à sua AWS conta, você pode iniciar instâncias do Amazon EC2 a partir da AMI usando o Amazon EC2. AWS Marketplace

Tópicos

- [Visualizar suas licenças concedidas](#)
- [Como gerenciar suas licenças concedidas](#)
- [Como distribuir direitos](#)
- [Como aceitar e ativar concessões](#)
- [Status da licença](#)
- [Métricas para contas de compradores](#)

Visualizar suas licenças concedidas

O License Manager possui guias para visualizar e gerenciar suas licenças concedidas com base nas permissões com as quais você está autenticado. A página de licenças concedidas pode exibir as seguintes guias:

Minhas licenças

Essa guia está disponível para qualquer usuário que tenha acesso para visualizar as licenças concedidas no License Manager. A guia tem uma seção Minhas licenças concedidas, que inclui informações como o ID da licença e o nome do produto. Nessa página, você pode ver informações adicionais sobre cada licença.

Resumo da licença (para administradores da organização)

Essa guia está disponível somente para administradores da organização. Ela tem uma seção de Totais, que lista a quantidade total de produtos e licenças concedidas em todas as contas da sua organização. Ela também mostra uma seção Produtos, que inclui uma tabela detalhando propriedades como o Nome do produto e Número de licenças concedidas.

Licenças agregadas (para administradores da organização)

Essa guia está disponível somente para administradores da organização. Ela tem uma seção que detalha as Licenças concedidas à minha organização, que inclui informações como o ID da licença e o Nome do produto. Nessa página, você pode ver informações adicionais sobre cada licença.

Como gerenciar suas licenças concedidas

As licenças que foram concedidas a você aparecerão no console do License Manager. Os destinatários precisam aceitar e ativar as licenças concedidas antes de poderem usar o produto. A

forma como você aceita e ativa uma licença depende se a licença é de AWS Marketplace, se sua conta é membro de uma organização e se todos os recursos estão habilitados para sua organização. AWS Organizations

As licenças concedidas exigem a replicação entre Regiões dos metadados da licença. O License Manager replica automaticamente cada licença concedida e suas informações associadas para outras Regiões da AWS. Isso permite que você tenha uma visão centralizada de todas as Regiões em que licenças são concedidas a você.

Licenças AWS Marketplace e AWS Data Exchange

- As licenças das assinaturas que você compra são automaticamente aceitas e ativadas.
- Se a conta de gerenciamento de uma organização com todos os atributos habilitados comprar uma assinatura e distribuir licenças para as contas dos membros, as licenças serão automaticamente aceitas nessas contas. A conta de gerenciamento ou as contas dos membros podem ativar a licença posteriormente.
- Se a conta de gerenciamento de uma organização com apenas os atributos de faturamento consolidado habilitados comprar uma assinatura e distribuir licenças para as contas dos membros, cada membro precisa aceitar e ativar a licença.

Licenças de um vendedor

- Você precisa aceitar e ativar licenças para produtos que usam o License Manager para distribuir licenças.
- Se a conta de gerenciamento de uma organização com todos os atributos habilitados comprar um produto e distribuir licenças para as contas dos membros, as licenças serão automaticamente aceitas nessas contas. A conta de gerenciamento ou as contas dos membros podem ativar a licença posteriormente.
- Se a conta de gerenciamento de uma organização com apenas os atributos de faturamento consolidado habilitados comprar um produto e distribuir licenças para as contas dos membros, cada membro precisa aceitar e ativar a licença.

Console (My licenses)

Você só pode visualizar e gerenciar as licenças concedidas em uma única conta da Conta da AWS.

Como gerenciar licenças concedidas na sua conta

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação, escolha Licenças concedidas.
3. Selecione a guia Minhas licenças, se ela não estiver selecionada.
4. (Opcional) Use as opções de filtro, como as mostradas abaixo, para restringir o escopo da lista exibida.
 - SKU do produto — O identificador do produto para esta licença, definido pelo emissor da licença ao criá-la. O mesmo SKU do produto pode existir em vários ISVs.
 - Destinatário — O ARN do destinatário da licença.
 - Status — O status da licença. Por exemplo, Disponível.
5. Para ver informações adicionais sobre a licença, escolha o ID correspondente para abrir a página Visão geral da licença.
6. Se o emissor da licença for uma entidade diferente AWS Marketplace, o status inicial da concessão será Aceitação pendente. Execute um destes procedimentos:
 - Escolha Aceitar e ativar a licença. O status de concessão resultante é Ativa.
 - Escolha Aceitar licença. O status de concessão resultante é Desativada. Quando quiser usar a licença, escolha Ativar licença.
 - Escolha Rejeitar licença. O status de concessão resultante é Rejeitada. Depois de rejeitar uma licença, não é possível ativá-la.

Se você quiser parar de usar uma licença que foi ativada, retorne à página Visão geral da licença e escolha Desativar licença. Se você quiser voltar a usar uma licença que foi desativada, retorne à página Visão geral da licença e escolha Ativar licença.

Console (Aggregated licenses)

Você pode ver as licenças concedidas que foram agregadas a partir de todas as contas da organização.

Important

Para usar a visão geral da organização para suas licenças concedidas, você deve primeiro vincular AWS Organizations usando as configurações do AWS License Manager console. Para ter mais informações, consulte [Configurações em AWS License Manager](#).

Para gerenciar as licenças concedidas em suas contas em AWS Organizations

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação, escolha Licenças concedidas.
3. Selecione a guia Licenças agregadas, se ela não estiver selecionada.
4. (Opcional) Use as opções de filtro, como as mostradas abaixo, para restringir o escopo da lista exibida.
 - SKU do produto — O identificador do produto para esta licença, definido pelo emissor da licença ao criá-la. O mesmo SKU do produto pode existir em vários ISVs.
 - Beneficiário — A conta da sua organização à qual a licença foi concedida.
5. Para ver informações adicionais sobre a licença, escolha o ID correspondente para abrir a página “Detalhes da licença”.
6. Se o emissor da licença for uma entidade diferente de AWS Marketplace, faça o seguinte:
 - Escolha Ativar a licença. O status de concessão resultante é Ativa.
 - Escolha Desativar a licença. O status de concessão resultante é Desativada.

Se você quiser parar de usar uma licença que foi ativada, retorne à página Visão geral da licença e escolha Desativar licença. Se você quiser voltar a usar uma licença que foi desativada, retorne à página Visão geral da licença e escolha Ativar licença.

AWS CLI

Você pode usar o AWS CLI para trabalhar com suas licenças concedidas.

Para gerenciar as licenças usando o 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](#)

Como distribuir direitos

Se você for um administrador de licenças operando na conta de gerenciamento da organização com [todos os atributos](#) habilitados, você pode distribuir direitos para a organização a partir das licenças concedidas criando uma concessão. Para obter mais informações sobre AWS Organizations, consulte [AWS Organizations terminologia e conceitos](#).

Os destinatários da licença podem ser os seguintes:

- Um Conta da AWS, que inclui somente a conta especificada.
- A raiz de uma organização, o que incluirá todas as contas dela.
- Uma Unidade Organizacional (UO) (não aninhada), o que inclui todas as contas desta UO e das UOs aninhadas nela.

Note

Você pode criar até 2.000 concessões por licença.

Você pode usar o AWS License Manager console ou o AWS CLI para distribuir seus direitos. Você pode especificar o ID ou o ARN da organização ao criar uma concessão no console, mas o formato ARN deve ser usado com o AWS CLI. Por exemplo, os ARNs seguirão este modelo:

ARN do ID da organização

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

ARN da UO da organização

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

Console

Para criar uma concessão (Console)

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação, escolha Licenças concedidas.

3. Escolha um ID de licença para abrir a página Visão geral da licença.
4. Na seção Concessões, escolha Criar concessão.
5. Na página Detalhes da concessão, faça o seguinte:
 - a. Insira um nome que vai ajudar você a identificar a finalidade ou o destinatário da concessão.
 - b. Insira o Conta da AWS ID, AWS Organizations ID da OU ou ARN, ou AWS Organizations ID ou ARN do beneficiário do subsídio.
 - c. Escolha Criar concessão.
6. Na página de Visão geral da licença, você verá uma entrada para a concessão no painel Concessões. O status inicial da concessão é Aceitação pendente. O status muda para Ativa quando o destinatário aceita a concessão ou para Rejeitada quando o destinatário a rejeita.

AWS CLI

Você pode usar o AWS CLI para distribuir um direito. Você deve especificar uma ID da organização ou OU no formato ARN ao usar a AWS License Manager API.

Para criar e listar suas concessões usando o AWS CLI:

- [create-grant](#)
- [list-distributed-grants](#)

A página “Detalhes das concessões” exibe a lista de contas às quais você concedeu acesso ao direito. Depois de distribuir uma licença para sua organização, você pode desativar ou ativar as licenças individualmente em cada conta.

Como aceitar a ativar concessões

Quando uma concessão é criada para uma licença concedida, ela é distribuída ao destinatário. Uma licença concedida deve ser aceita e ativada antes que possa ser usada pelo destinatário. O processo de ativação da concessão pode incluir opções adicionais para licenças concedidas provenientes do AWS Marketplace.

Por padrão, a página Visão geral da concessão de uma licença concedida tem o status de Pending Acceptance. Você pode Accept, Accept and Activate ou Reject a concessão. Concessões

aceitas, mas ainda não ativadas, têm o status de `Disabled`. Concessões aceitas e ativadas têm o status de `Active`.

Uma licença concedida deve ser aceita e ativada antes que possa ser usada pelo destinatário. Por padrão, a página “Detalhes da concessão” de uma licença concedida tem o status de Aceitação pendente. Você pode Aceitar, Aceitar e Ativar ou Rejeitar a licença. Concessões aceitas, mas ainda não ativadas, têm o status de Desativadas. Concessões aceitas e ativadas têm o status de Ativas.

Tip

Você pode aceitar automaticamente concessões provenientes da conta de gerenciamento da sua organização. Para ativar a aceitação automática da concessão, vincule as contas da sua organização na página de [configurações](#) no AWS License Manager console a partir da conta de gerenciamento.

Você não pode ativar duas licenças para o mesmo produto AWS Marketplace ao mesmo tempo. Se você tiver duas assinaturas (por exemplo, a oferta pública para um produto e uma oferta privada, ou uma licença assinada para um produto e uma licença concedida para o mesmo produto), você tem as seguintes opções:

1. Desative a concessão existente para o produto e, em seguida, ative a nova concessão.
2. Ative a nova concessão e especifique que você deseja desativar e substituir a concessão existente. Você pode usar o console do License Manager ou o AWS CLI:
 - a. Usando o console do License Manager, ative a nova concessão e selecione Sim, pois você deseja substituir as concessões ativas.
 - b. Usando a API `CreateGrantVersion`, ative a nova concessão especificando `ALL_GRANTS_PERMITTED_BY_ISSUER` para o `ActivationOverrideBehavior` com um Status de `Active`.

Console

Você pode usar o console do License Manager para ativar uma concessão. Ao ativar um subsídio proveniente do AWS Marketplace, você pode ter a opção de substituir os subsídios ativos:

- Como administrador de licenças, você precisa especificar se deseja substituir as concessões ativas ao ativar uma concessão.

- Como concedente, você pode, opcionalmente, especificar se deseja substituir as concessões ativas ao ativar uma concessão para outra conta em sua organização.
- Se o concedente não especificar se deseja substituir as concessões ativas, você, como beneficiário, precisará fazer essa seleção.

Como ativar uma licença (Console)

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação, escolha Licenças concedidas.
3. Escolha um ID de licença para abrir a página Visão geral da licença.
4. Escolha o nome de uma concessão para abrir a página Visão geral da concessão.
5. Se precisar, selecione uma opção de ativação para decidir se deseja substituir as concessões ativas:
 - a. Não — Essa opção ativará a concessão sem substituir as já existentes para o destinatário (beneficiário).
 - b. Sim — Essa opção desativará as concessões para o mesmo produto e ativará uma nova concessão para o destinatário definido (beneficiário):
 - i. Um especificado Conta da AWS.
 - ii. Contas de membros da UO da organização especificada.
 - iii. Todas as contas de membros da organização.
6. (Opcional) Forneça um motivo para ativar a concessão.
7. Digite **activate** na caixa de entrada e escolha Ativar.

AWS CLI

Você pode usar o AWS CLI para trabalhar com suas licenças concedidas.

Para trabalhar com subsídios distribuídos usando AWS CLI:

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

- [reject-grant](#)

Status da licença

As licenças têm dois status: o Status da licença, que mostra a disponibilidade e a capacidade de compartilhamento geral da licença, e o Status da concessão, que mostra a capacidade de usar a licença.

A tabela a seguir mostra os vários status de uma licença concedida:

Status	Descrição
DISPONÍVEL	A licença está disponível para uso e compartilhamento.
PENDENTE_DISPONÍVEL	A licença não está disponível para uso, pois ainda está sendo processada.
DESATIVADA	A licença não está disponível para uso porque foi desativada pelo emissor.
SUSPENSA	A licença não está disponível para uso, pois está suspensa.
EXPIRADA	A licença não está disponível para uso porque chegou ao fim do prazo.
PENDENTE_EXCLUÍDA	A licença não está disponível para uso, pois está sendo excluída.
EXCLUÍDA	A licença não está disponível para uso porque o contrato foi cancelado.

A tabela a seguir mostra os vários status de uma concessão:

Status	Descrição
PENDENTE_WORKFLOW	A concessão está em processo de distribuição.

Status	Descrição
PENDENTE_ACEITA	A concessão foi criada e o beneficiário ainda não a aceitou.
REJEITADA	A concessão foi rejeitada pelo destinatário.
ATIVA	A concessão foi aceita e ativada para uso pelo destinatário. O atributo licenciado pode ser usado.
FALHA_WORKFLOW	A distribuição da concessão falhou.
EXCLUÍDA	A concessão foi excluída pelo concedente.
PENDENTE_EXCLUÍDA	A concessão distribuída está em processo de ser excluída.
DESATIVADA	A concessão foi aceita pelo destinatário, mas não foi ativada para uso.
WORKFLOW_CONCLUÍDO	A concessão para uma organização foi distribuída ou retirada. Os detalhes da concessão mostram o status das subconcessões para cada conta na organização.

Métricas para contas de compradores

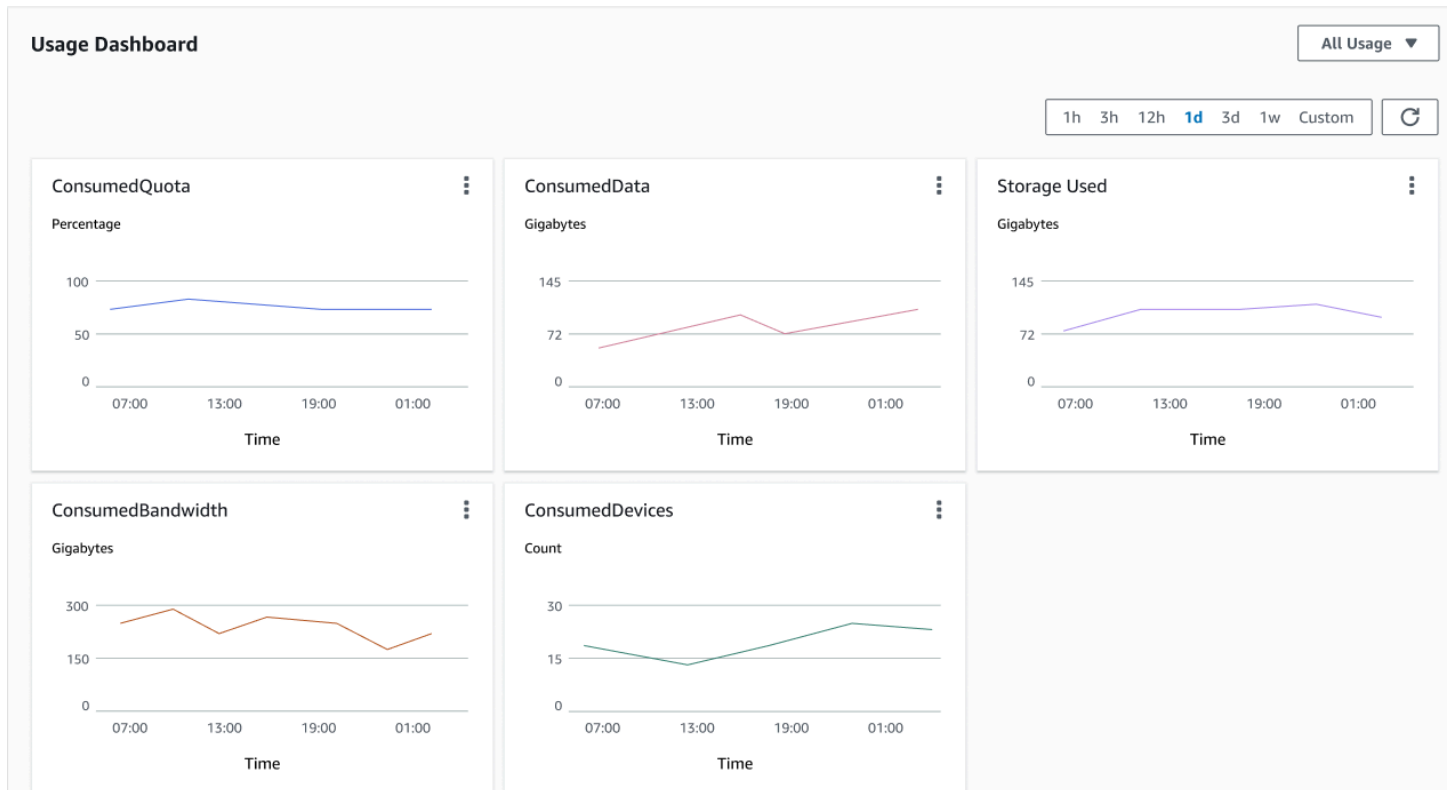
Quando uma concessão para uma licença emitida por um vendedor é configurada com a opção Permitir envio de registros de uso selecionada, o License Manager emite uma CloudWatch métrica para a conta do vendedor, a conta do comprador raiz e a conta na qual o uso está sendo registrado. As contas de compradores são Contas da AWS aquelas que compraram ou receberam uma licença emitida pelo vendedor. Para obter mais informações, consulte [Conceder licenças a clientes](#).

Painel de uso

Quando um aplicativo vendedor ou fornecedor independente de software (ISV) registra o uso de uma licença para uma conta de comprador, a conta na qual o uso está sendo registrado e a conta raiz do comprador veem um CloudWatch widget com registros de uso na página do painel de uso

no console do License Manager. Os compradores também podem ver métricas das contas para as quais distribuíram licenças no AWS Organizations. Os gráficos no Painel de uso estão disponíveis para todas as licenças que recebem registros de uso.

A imagem a seguir é um exemplo do painel de uso:



Licenças emitidas pelo vendedor no License Manager

Fornecedores independentes de software (ISVs) podem usar AWS License Manager para gerenciar e distribuir licenças de software para usuários finais. Como emissor, você pode monitorar centralmente o uso das licenças emitidas pelo vendedor usando o painel do License Manager.

O License Manager usa padrões abertos e seguros do setor para representar licenças e permite que os clientes verifiquem criptograficamente sua autenticidade. O License Manager associa cada licença a uma chave assimétrica. Como ISV, você possui as AWS KMS chaves assimétricas e as armazena em sua conta.

As licenças emitidas pelo vendedor exigem a replicação entre Regiões dos metadados da licença. O License Manager replica automaticamente cada licença emitida pelo vendedor e respectivas informações associadas para outras regiões.

O License Manager oferece suporte a uma variedade de modelos de licenciamento diferentes, incluindo os seguintes:

- Perpétuas — licenças vitalícias sem data de expiração, que autorizam os usuários a usar o software indefinidamente.
- Flutuantes — licenças que podem ser compartilhadas com várias instâncias do aplicativo. As licenças podem ser pré-pagas e um conjunto fixo de direitos pode ser adicionado a elas.
- Por assinatura — licenças com datas de expiração que podem ser renovadas automaticamente, a menos que sejam especificamente desativadas.
- Baseadas no uso — licenças com termos específicos baseados no uso, como o número de solicitações de API, transações ou atributos de armazenamento.

Você pode criar licenças no License Manager e distribuí-las aos clientes usando uma identidade AWS do IAM ou por meio de tokens portadores gerados pelo License Manager. Clientes com uma AWS conta podem redistribuir os direitos de licença para AWS identidades em suas respectivas organizações. Clientes com direitos distribuídos podem fazer check-out e check-in dos direitos exigidos pela licença por meio de integração de seu software com o License Manager.

Direitos

O License Manager captura os atributos da licença como direitos na licença. Os direitos podem ser caracterizados com uma quantidade limitada ou ilimitada. Um exemplo de direito limitado é '40 GB de transferência de dados'. Um exemplo de direito de quantidade ilimitada é o 'Nível Platina'.

Uma licença captura todos os direitos concedidos, as datas de ativação e expiração e os detalhes do emissor. Uma licença é uma entidade versionada e cada versão é imutável. As versões da licença são atualizadas sempre que a licença é alterada.

Para fazer o check-out ou o check-in de direitos limitados, os pedidos de ISV devem especificar o valor de cada capacidade limitada. Para direitos ilimitados, os pedidos de ISV podem simplesmente especificar o direito relevante para fazer o check-out ou fazer o check-in novamente. Por fim, os atributos limitados também oferecem suporte a um sinalizador de "excedente", que indica se os usuários finais podem exceder o uso dos direitos iniciais. O License Manager rastreia e relata o uso, bem como os excedentes, ao ISV.

Uso da licença

O License Manager permite acompanhar centralmente as licenças em várias regiões, mantendo uma contagem de todos os direitos com check out. O License Manager também rastreia a identidade do usuário e o identificador de atributo subjacente, se disponível, associado a cada check out, além de quando o check-out foi feito. Você pode acompanhar esses dados de séries temporais por meio de CloudWatch Eventos.

As licenças podem estar em um dos seguintes estados:

- Criada — a licença foi criada.
- Atualizada — a licença está atualizada.
- Desativada — a licença está desativada.
- Excluída — a licença foi excluída.

Requisitos

Para começar a usar esse atributo, você precisa de permissão para chamar as seguintes ações da API do 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": "*"
}
]
}

```

Se você se integrar ao License Manager para que clientes sem uma AWS conta possam consumir licenças vendidas fora dele AWS Marketplace, você deverá criar uma função que permita que seu aplicativo de software chame a API do License Manager. Por exemplo, você pode usar a AWS CLI. Primeiro, use o comando [create-role](#) para criar uma função chamada `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

```

O seguinte é `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"
      }
    }
  }
}

```

Em seguida, use o [attach-role-policy](#) comando para adicionar a política `AWSLicenseManagerConsumptionPolicy` AWS gerenciada à `AWSLicenseManagerConsumptionRole` função.

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

Criação de licenças emitidas pelo vendedor

Use o procedimento a seguir para criar um bloco de licenças para conceder aos clientes que usam o AWS Management Console. Como alternativa, você pode criar a licença usando a ação [CreateLicense](#) da API.

Para criar uma licença usando o console

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Escolha Licenças emitidas pelo vendedor no menu à esquerda.
3. Escolha Criar licença.
4. Para Metadados de licença, forneça as seguintes informações:
 - Nome da licença — o nome, com até 150 caracteres, a ser exibido aos compradores.
 - Descrição da licença — uma descrição opcional, de até 400 caracteres, que diferencia essa licença de outras licenças.
 - SKU do produto — o SKU do produto.
 - Destinatário — o nome do destinatário (empresa ou pessoa física).
 - Região de origem — A AWS região da licença. Embora as licenças possam ser consumidas globalmente, as licenças somente podem ser alteradas na região de origem. Não é possível alterar a região de origem de uma licença depois de criá-la.
 - Data de início da licença — a data de ativação.
 - Data de término da licença — a data de término da licença, se aplicável.
5. Para Configuração de consumo, forneça as seguintes informações:
 - Frequência de renovação — se deve o consumo deve ser renovado semanalmente, mensalmente ou não deve ser renovado.
 - Configuração de consumo — escolha Opções de configuração de consumo provisório se a licença for usada para conectividade contínua ou Empréstimo se a licença for usada offline. Insira Tempo máximo de vida (minutos) para definir a duração da disponibilidade da licença.
6. Para Emissor, forneça as seguintes informações:

- Insira uma AWS KMS chave — o License Manager usa essa chave para assinar e verificar o emissor. Para ter mais informações, consulte [Assinatura criptográfica de licenças](#).
 - Nome do emissor — o nome comercial do vendedor.
 - Vendedor registrado — um nome comercial opcional.
 - URL do contrato — o URL do contrato de licença.
7. Para Direitos, forneça as seguintes informações sobre os atributos que a licença concede aos destinatários:
- Nome – o nome do destinatário.
 - Tipo de unidade — selecione o tipo de unidade e, em seguida, forneça a contagem máxima.
 - Marque Permitir check-in se os destinatários precisarem fazer o check-in das licenças antes da renovação.
 - Marque Excedentes permitidos se os destinatários puderem usar o atributo além da contagem máxima. Essa opção pode gerar cobranças adicionais para o destinatário.
8. Escolha Criar licença.

Concessão de licenças aos clientes

Depois de adicionar a nova licença, você pode conceder a licença a um cliente com uma conta da AWS usando o AWS Management Console. O destinatário deve aceitar a concessão antes de usar a licença. Para ter mais informações, consulte [Licenças concedidas no License Manager](#).

Como alternativa, se o cliente não tiver uma AWS conta, você pode usar a API License Manager para permitir que os clientes [consumam licenças](#).

Para conceder uma licença a um cliente usando o console

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Escolha Licenças emitidas pelo vendedor no menu à esquerda.
3. Escolha a ID da licença para abrir a página de detalhes.
4. Em Concessões, escolha Criar concessão.
5. Para Detalhes da concessão, forneça as seguintes informações:
 - Nome da concessão — o nome da concessão. Isso é usado para ativar os atributos de pesquisa.

- AWS ID da conta — O número da AWS conta do destinatário da licença.
- Direitos da licença
 - Selecione Consumo se o destinatário puder consumir os direitos concedidos.
 - Selecione Distribuição se o destinatário puder distribuir os direitos concedidos para outras AWS contas.
 - Selecione Permitir geração de token local para autenticar licenças compartilhadas sem usar AWS identidades ou credenciais.
 - Selecione Permitir envio de registros de uso para permitir que os destinatários da licença emitam registros de uso para tipos de uso.
- Região de origem — A Região da AWS para a licença.

6. Escolha Criar concessão.

Obter credenciais temporárias para clientes sem uma conta AWS

Para clientes sem uma AWS conta, você pode usar os direitos da mesma forma que usa para seus clientes com uma AWS conta. Use o procedimento a seguir para obter AWS credenciais temporárias para seus clientes sem uma AWS conta. As chamadas de API devem ser feitas na região de origem.

Para obter credenciais temporárias para usar na chamada da API do License Manager

1. Chame a ação [CreateToken](#) da API para obter um token de atualização codificado como um token JWT.
2. Chame a ação da [GetAccessToken](#) API, especificando o token de atualização que você recebeu CreateToken na etapa anterior, para receber um token de acesso temporário.
3. Chame a ação da [AssumeRoleWithWebIdentity](#) API, especificando o token de acesso que você recebeu GetAccessToken na etapa anterior e a `AWSLicenseManagerConsumptionRole` função que você criou para obter AWS credenciais temporárias.

Para criar um token a partir do AWS License Manager console

1. No [console do License Manager](#), navegue até a página de detalhes da licença para ver o direito de licença específico que você deseja usar sem uma AWS conta.
2. Escolha Criar token para gerar um token de acesso temporário.

Note

Na primeira vez que gerar um token de acesso temporário, deverá criar um perfil de serviço para que o License Manager possa acessar os serviços em seu nome. O seguinte perfil de serviço será criado: `AWSLicenseManagerConsumptionRole`.

3. Faça o download do arquivo do token .csv ou copie a string do token quando ela for gerada.

Important

Esta é a única vez que você poderá visualizar ou baixar esse token. Recomendamos que baixe o token e armazene o arquivo em um lugar seguro. Você pode criar novos tokens a qualquer momento, até o [limite do serviço](#).

Consumo de licenças

O License Manager permite que vários usuários consumam simultaneamente direitos, com atributos limitados, de uma única licença. Chame a ação de API [CheckoutLicense](#). A seguir, está uma descrição dos parâmetros.

- Impressão digital da chave — emissor de licenças confiável.

Exemplo: `aws:123456789012:issuer:issuer-fingerprint`

- SKU do produto — o identificador do produto para esta licença, definido pelo emissor da licença ao criá-la. O mesmo SKU do produto pode existir em vários ISVs. Portanto, impressões digitais confiáveis desempenham um papel importante.

Exemplo: `1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0daEXAMPLE`

- Direitos — capacidades para fazer check-out. Se você especificar uma capacidade ilimitada, a quantidade será zero. Exemplo:

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

```
{
  "Name": "DataStorage",
  "Unit": "Gigabytes",
  "Value": 5
}
```

- **Beneficiário** — os ISVs de software como serviço (SaaS) podem verificar as licenças em nome de um cliente incluindo o identificador do cliente. O License Manager limita a chamada ao repositório de licenças criadas na conta SaaS do ISV.

Exemplo: user@domínio.com.br

- **ID do nó** — um identificador usado para bloquear a licença a uma única instância do aplicativo.

Exemplo: 10.0.21.57

Exclusão de licenças emitidas pelo vendedor

Depois de excluir uma licença, você pode recriá-la. A licença e seus dados são retidos e disponibilizados para o emissor e os detentores da licença no modo somente leitura por seis meses.

Use o procedimento a seguir para excluir uma licença que você criou usando o AWS Management Console. Como alternativa, você pode excluir a licença usando a ação [DeleteLicense](#) da API.

Para excluir uma configuração de licença usando o console

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Escolha Licenças emitidas pelo vendedor no menu à esquerda.
3. Escolha o botão de opção ao lado da licença para selecioná-la para exclusão.
4. Escolha Excluir. Quando a confirmação for solicitada, insira **delete** e escolha Excluir.

Gerencie assinaturas baseadas no usuário no License Manager

Com as assinaturas baseadas no usuário AWS License Manager, você pode comprar assinaturas de software licenciado totalmente compatíveis. As licenças são fornecidas pela Amazon e têm uma taxa de assinatura baseada no usuário. O Amazon EC2 fornece Imagens de máquina da Amazon (AMIs) pré-configuradas com o software compatível e com as licenças do Windows Server incluídas. As licenças podem ser usadas sem compromisso de licenciamento de longo prazo.

Para utilizar assinaturas baseadas no usuário, basta associar usuários do [AWS Directory Service for Microsoft Active Directory](#) (AWS Managed Microsoft AD) ou do domínio autogerenciado (on-premises) às instâncias do EC2 que fornecem o software. Para disponibilizar o software licenciado, devem ser criadas assinaturas baseadas no usuário e associá-las a instâncias inicializadas a partir de AMIs pré-configuradas. O [AWS Systems Manager](#) configura e fortalece as instâncias incluídas na licença executada. Os usuários devem se conectar ao software Remote Desktop para acessar as instâncias que fornecem o software.

Incorrem cobranças para cada usuário e [vCPU](#) associados às instâncias incluídas na licença. Os modelos de preços das Instâncias Reservadas e Savings Plans do Amazon EC2 ajudam a otimizar os custos do Amazon EC2. Para obter mais informações, consulte [Instâncias reservadas](#) no Manual do usuário do Amazon Elastic Compute Cloud. As assinaturas baseadas no usuário são cobradas da primeira metade até o final do mês.

Sumário

- [Pré-requisitos](#)
- [Considerações](#)
- [Software para assinaturas baseadas no usuário](#)
 - [Software com suporte para assinaturas baseadas no usuário](#)
 - [Microsoft Visual Studio](#)
 - [Microsoft Office](#)
 - [Inicie a partir de uma AMI compatível](#)
 - [Software adicional](#)
- [Conceitos básicos das assinaturas baseadas no usuário](#)
 - [Etapa 1: Configurar a nuvem privada virtual \(VPC\) do AWS Directory Service for Microsoft Active Directory](#)
 - [Etapa 2: Assinar um produto](#)
 - [Etapa 3: Executar uma instância para fornecer assinaturas baseadas no usuário](#)
 - [Etapa 4: Associar usuários a uma instância de assinatura baseada no usuário](#)
 - [Etapa 5: Conectar-se a uma instância de assinatura baseada no usuário](#)
- [Modificar configurações de diretório para assinaturas baseadas no usuário](#)
- [Modificar as configurações de VPC para assinaturas baseadas no usuário](#)
- [Desassociar usuários de assinaturas baseadas no usuário](#)
- [Cancelar a inscrição de usuários em assinaturas baseadas no usuário](#)

- [Terminar instâncias do EC2 que fornecem assinaturas baseadas no usuário](#)
- [Remover um diretório para assinaturas baseadas no usuário](#)
- [Solução de problemas com assinaturas baseadas no usuário](#)
 - [Solução de problemas de conformidade da instância](#)
 - [Solução de problemas de conformidade de licenças](#)
 - [Solução de problemas de conectividade de instância](#)
 - [Solucionar falhas ao ingressar no domínio](#)
 - [Solução de problemas de conectividade do Systems Manager](#)
 - [Solução de problemas do Run Command do Systems Manager](#)

Pré-requisitos

Os pré-requisitos a seguir devem estar implementados no ambiente antes que seja possível criar assinaturas baseadas no usuário.

- Você deve permitir que o License Manager crie um perfil vinculado ao serviço para integrar as assinaturas da sua Conta da AWS para usuários. Uma solicitação aparecerá uma vez na seção Assinaturas baseadas no usuário do console do License Manager, na qual você deverá concordar em conceder permissão ao License Manager para criar o perfil necessário vinculado ao serviço. Depois de conceder permissão ao License Manager, escolha Criar para criar o perfil vinculado ao serviço. Para ter mais informações, consulte [Usando funções vinculadas a serviços para AWS License Manager](#).
- Você deve ter um AWS Managed Microsoft AD diretório criado. AWS Managed Microsoft AD diretórios que foram compartilhados não são suportados. Para obter mais informações sobre como criar um AWS Managed Microsoft AD diretório, consulte os [AWS Managed Microsoft AD pré-requisitos](#) e [Crie seu AWS Managed Microsoft AD diretório no Guia](#) do AWS Directory Service usuário.
- Você deve associar usuários ao seu AWS Managed Microsoft AD diretório ou a um Active Directory autogerenciado para utilizar as assinaturas baseadas no usuário.
 - Para associar usuários a AWS Managed Microsoft AD, você deve provisionar usuários em seu AWS Managed Microsoft AD diretório. Para obter mais informações, consulte [Gerenciar usuários e grupos no AWS Managed Microsoft AD](#) no Guia de administração AWS Directory Service .
 - Para associar usuários no diretório autogerenciado, você deve estabelecer uma relação de confiança bidirecional entre o diretório autogerenciado e o diretório do AWS Managed Microsoft

AD . Para obter mais informações, consulte [Tutorial: Crie uma relação de confiança entre seu domínio autogerenciado do Active Directory AWS Managed Microsoft AD e o seu](#) no Guia de AWS Directory Service Administração.

- As sub-redes configuradas para seu diretório devem ser todas da mesma VPC do seu. Conta da AWS
- O acesso de saída à Internet a partir das instâncias que fornecem assinaturas baseadas no usuário, ou [endpoints da VPC](#), deve ser configurado para que as instâncias se comuniquem com o AWS Systems Manager. Para obter mais informações, consulte [Configuração do Systems Manager para instâncias do EC2](#) no AWS Systems Manager Guia do usuário.
- O License Manager cria duas interfaces de rede que usam o grupo de segurança padrão da VPC em que a sua AWS Managed Microsoft AD está provisionada. Essas interfaces são usadas para a funcionalidade de serviço necessária com o diretório. Certifique-se de que seu grupo de segurança padrão permita tráfego de saída para o endereço IPv4 da interface de rede de cada controlador de domínio ou para o grupo de segurança usado pelos controladores de domínio. Para obter mais informações, consulte [Etapa 1: Configurar a nuvem privada virtual \(VPC\) do AWS Directory Service for Microsoft Active Directory](#) e [O que é criado](#) no Guia de administração do AWS Directory Service .

Quando o processo de provisionamento estiver concluído, será possível associar um grupo de segurança diferente às interfaces criadas pelo License Manager. O grupo de segurança selecionado também deve permitir o tráfego necessário para cada endereço IPv4 ou grupo de segurança da interface de rede do controlador de domínio. Para obter mais informações, consulte [Trabalhar com grupos de segurança](#) no Guia do usuário do Amazon Virtual Private Cloud.

- Você deve configurar o encaminhamento de DNS para quaisquer VPCs adicionais às AWS Managed Microsoft AD que você registra para assinaturas baseadas em usuário. Você pode usar o Amazon Route 53 ou outro serviço DNS para encaminhamento DNS. Para obter mais informações, consulte a postagem do blog [Integrar a resolução de DNS do serviço de diretório com o Amazon Route 53 Resolvers](#).
- Caso assine o Microsoft Office com assinaturas baseadas no usuário, você deverá:
 - Habilitar os nomes de host DNS e a resolução DNS para a VPC. Para obter mais informações, consulte [Visualizar e atualizar atributos DNS para a VPC](#).
 - Certifique-se de que as instâncias executadas para fornecer assinaturas baseadas no usuário com o Microsoft Office tenham uma rota para a sub-rede em que os endpoints da VPC estão provisionados.

- Identifique ou crie um grupo de segurança para os endpoints da VPC que permita a conectividade da porta TCP 1688 de entrada. Esse grupo de segurança será especificado quando definir as configurações de nuvem privada virtual. Para obter mais informações, consulte [Trabalhar com grupos de segurança](#). O License Manager associará esse grupo de segurança aos endpoints da VPC que ele cria em seu nome ao configurar a VPC. Para obter mais informações, consulte [Acessar um serviço da AWS por meio de um endpoint da VPC de interface](#) no Guia de AWS PrivateLink .
- Identificar ou criar um grupo de segurança para as instâncias executadas para fornecer assinaturas baseadas no usuário que permitam a conectividade da porta TCP 3389 de fontes de conexão aprovadas. O grupo de segurança também deve permitir que a conectividade de saída da porta TCP 1688 alcance os endpoints da VPC. Para obter mais informações, consulte [Trabalhar com grupos de segurança](#).

Se estiver se preparando para usar assinaturas baseadas no usuário pela primeira vez, atenda os pré-requisitos listados e consulte [Conceitos básicos das assinaturas baseadas no usuário](#). Se as assinaturas baseadas no usuário já estão configuradas e você deseja adicionar esses produtos à AWS Managed Microsoft AD e configurar a VPC para produtos do Microsoft Office, preencha os pré-requisitos listados e consulte [Modificar configurações de diretório para assinaturas baseadas no usuário](#).

- É necessário ter uma função de perfil de instância associada às instâncias que fornecem os produtos de assinatura baseada no usuário que permite que o recurso seja gerenciado pelo AWS Systems Manager. Para obter mais informações, consulte [Criar um perfil de instância do IAM para o Systems Manager](#) no Guia do usuário do AWS Systems Manager .

Warning

As instâncias que fornecem assinaturas baseadas no usuário devem ser AWS Systems Manager gerenciadas para que tenham um status saudável. Além disso, as instâncias devem ser capazes de ativar o licenciamento por assinatura baseada no usuário e permanecer em conformidade após a ativação da licença. O License Manager tentará recuperar instâncias não íntegras, mas as instâncias que não puderem retornar ao status íntegro serão terminadas. Para obter informações sobre solução de problemas sobre como manter as instâncias gerenciadas pelo Systems Manager e sobre a conformidade das instâncias, consulte a seção [Solução de problemas com assinaturas baseadas no usuário](#) deste guia.

- Para criar assinaturas baseadas no usuário, o usuário ou perfil deve ter as seguintes permissões:

- `ec2:CreateNetworkInterface`
- `ec2>DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:DescribeSubnets`
- `ds:DescribeDirectories`
- `ds:AuthorizeApplication`
- `ds:UnauthorizeApplication`
- `ds:GetAuthorizedApplicationDetails`
- `ds:DescribeDomainControllers`
- Para criar assinaturas baseadas no usuário para produtos do Microsoft Office, o usuário ou perfil também deve ter as permissões adicionais a seguir:
 - `ec2:CreateVpcEndpoint`
 - `ec2>DeleteVpcEndpoints`
 - `ec2:DescribeVpcEndpoints`
 - `ec2:ModifyVpcEndpoint`
 - `ec2:DescribeSecurityGroups`

Considerações

As considerações a seguir se aplicam ao utilizar assinaturas baseadas no usuário com o License Manager:

- As licenças SAL do Win Remote Desktop Services não podem ser usadas separadamente dos produtos de assinatura baseada no usuário compatíveis.
- As instâncias que fornecem assinaturas baseadas no usuário oferecem suporte a até duas sessões ativas de usuário por vez.
- Quando são criados usuários locais com privilégios de administrador em instâncias que fornecem assinaturas baseadas no usuário, o status de integridade da instância pode mudar para não íntegro. O License Manager pode terminar instâncias que não estejam íntegras devido à não conformidade. Para obter mais informações, consulte [Solucionar problemas de não conformidade de uma instância](#).

- Para parar de incorrer em cobranças por assinaturas baseadas no usuário, você deve desassociar o usuário de todas as instâncias às quais ele está associado. Para ter mais informações, consulte [Desassociar usuários de assinaturas baseadas no usuário](#).
- Quando você configura o diretório com produtos do Microsoft Office, a VPC deve ter [endpoints da VPC](#) provisionados em pelo menos uma sub-rede. Se quiser remover todos os atributos de endpoint da VPC criados pelo License Manager, deverá executar as seguintes ações:
 - Desassociar todos os usuários das assinaturas baseadas no usuário. Para ter mais informações, consulte [Desassociar usuários de assinaturas baseadas no usuário](#).
 - Remova qualquer diretório que esteja configurado das configurações do License Manager. Para ter mais informações, consulte [Remover um diretório para assinaturas baseadas no usuário](#).
 - Terminar todas as instâncias que fornecem produtos de assinatura baseada no usuário. Para ter mais informações, consulte [Terminar instâncias do EC2 que fornecem assinaturas baseadas no usuário](#).
- A chave de tag de `AWSLicenseManager` com o valor de `UserSubscriptions` atribuído pelo License Manager às suas instâncias não deve ser alterada nem excluída.
- As duas interfaces de rede elástica (ENI) criadas para o License Manager não devem ser alteradas ou excluídas para que o serviço funcione.
- Os objetos que o License Manager cria na unidade organizacional AWS reservada (OU) do AWS Managed Microsoft AD diretório não devem ser alterados nem excluídos.
- As instâncias implantadas para assinaturas baseadas no usuário devem ser nós gerenciados por AWS Systems Manager e ingressar no mesmo domínio. Para obter informações sobre como manter as instâncias gerenciadas pelo Systems Manager, consulte a seção [Solução de problemas com assinaturas baseadas no usuário](#) deste guia.

Software para assinaturas baseadas no usuário

AWS License Manager oferece suporte a assinaturas baseadas em usuário para o Microsoft Visual Studio e o Microsoft Office. É necessária uma única assinatura da Licença de Acesso de Assinante dos Serviços de Área de Trabalho Remota (RDS SAL) do Windows Server para que cada usuário acesse uma instância com licença incluída que fornece um produto de assinatura baseada no usuário. O software compatível terá sua utilização monitorada pelo License Manager. Para ter mais informações, consulte [Conceitos básicos das assinaturas baseadas no usuário](#).

Plataformas de sistema operacional (SO) Windows compatíveis

Você pode encontrar AMIs do Windows que incluem produtos cobertos pela licença RDS SAL para as seguintes plataformas do sistema operacional Windows:

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

Software com suporte para assinaturas baseadas no usuário

O License Manager oferece suporte ao licenciamento baseado no usuário com o software a seguir.

Microsoft Visual Studio

O Microsoft Visual Studio é um ambiente de desenvolvimento integrado (IDE) que permite aos desenvolvedores criar, editar, depurar e publicar aplicativos. As AMIs fornecidas pelo Microsoft Visual Studio incluem o [AWS Toolkit for .NET Refactoring](#) e o [AWS Toolkit for Visual Studio](#).

Edições com suporte

- Visual Studio Professional 2022
- Visual Studio Enterprise 2022

A tabela a seguir detalha os nomes das assinaturas de software e o valor do produto associado usado para as operações da API de assinatura baseada no usuário do License Manager.

Nome da assinatura de software	Valor do produto
Visual Studio Enterprise 2022	VISUAL_STUDIO_ENTERPRISE
Visual Studio Professional 2022	VISUAL_STUDIO_PROFESSIONAL

Microsoft Office

O Microsoft Office é uma coleção de software desenvolvida pela Microsoft para vários casos de uso de produtividade, incluindo trabalhar com documentos, planilhas e apresentações de slides.

Edições com suporte

- Office LTSC Professional Plus 2021

A tabela a seguir detalha os nomes das assinaturas de software e o valor do produto associado usado para as operações da API de assinatura baseada no usuário do License Manager.

Nome da assinatura de software	Valor do produto
Office LTSC Professional Plus 2021	OFFICE_PROFESSIONAL_PLUS

Inicie a partir de uma AMI compatível

Quando você executa uma instância de uma AMI que oferece suporte Office LTSC Professional Plus ao Microsoft Visual Studio, o padrão de execução é a versão mais recente da plataforma do sistema operacional Windows da AMI (por exemplo, Windows Server 2022). Para iniciar com uma versão anterior da plataforma do sistema operacional, siga estas etapas.

1. Abra o AWS Marketplace console em <https://console.aws.amazon.com/marketplace>.
2. No painel de navegação, escolha Gerenciar assinaturas.
3. Para otimizar os resultados da assinatura, você pode pesquisar todo ou parte do nome da assinatura. Por exemplo, o Office LTSC Professional Plus 2021 ou o Visual Studio Enterprise.
4. Selecione Iniciar nova instância no painel de assinatura. Isso abre uma página de configuração de execução.
5. Para iniciar uma instância a partir de uma AMI baseada em uma versão anterior da plataforma do sistema operacional Windows, selecione o link completo AWS Marketplace do site, localizado abaixo da versão do software. Isso leva você a uma página de configuração na qual você pode selecionar em uma lista de versões.
6. A lista mostra as versões mais recentes da AMI para as plataformas de sistema operacional Windows compatíveis. Selecione a versão do sistema operacional Windows a partir da qual você deseja iniciar.

Software adicional

É possível instalar software adicional em suas instâncias que não estejam disponíveis como assinaturas baseadas no usuário. Instalações adicionais de software não são monitoradas pelo License Manager. Essas instalações devem ser realizadas usando a conta Admin, que é criada por padrão em seu AWS Managed Microsoft AD diretório. Para obter mais informações, consulte [Conta de administrador](#) no Guia de administração do AWS Directory Service .

Para instalar software adicional com a conta Admin, você deve:

- Inscrever a conta de administrador no produto fornecido pela instância.
- Associar a conta de administrador à instância.
- Conectar-se à instância usando a conta Admin para realizar a instalação.

Para ter mais informações, consulte [Conceitos básicos das assinaturas baseadas no usuário](#).

Conceitos básicos das assinaturas baseadas no usuário

As etapas a seguir detalham como começar a utilizar assinaturas baseadas no usuário. Essas etapas pressupõem que você já tenha implementado os pré-requisitos necessários. Para obter mais informações, consulte [Pré-requisitos](#).

Se você já configurou seu AWS Managed Microsoft AD diretório para assinaturas baseadas em usuário e também gostaria de usar o Microsoft Office, consulte. [Modificar as configurações de VPC para assinaturas baseadas no usuário](#)

Etapas

- [Etapa 1: Configurar a nuvem privada virtual \(VPC\) do AWS Directory Service for Microsoft Active Directory](#)
- [Etapa 2: Assinar um produto](#)
- [Etapa 3: Executar uma instância para fornecer assinaturas baseadas no usuário](#)
- [Etapa 4: Associar usuários a uma instância de assinatura baseada no usuário](#)
- [Etapa 5: Conectar-se a uma instância de assinatura baseada no usuário](#)

Etapa 1: Configurar a nuvem privada virtual (VPC) do AWS Directory Service for Microsoft Active Directory

O License Manager exige AWS Managed Microsoft AD a associação dos usuários com assinaturas baseadas em usuários. Devem ser selecionados todos os produtos necessários para as assinaturas baseadas no usuário ao configurar o diretório, pois os usuários só podem assinar os produtos configurados. <directory_id>Quando você registra seu AWS Managed Microsoft AD diretório, o License Manager cria duas Elastic Network Interfaces (ENIs) para que o serviço se comunique com seu diretório com uma descrição semelhante à interface de rede AWS criada para LicenseManager .

Important

Você deve permitir que o License Manager crie o perfil vinculado [ao serviço](#) necessária antes de continuar. Para obter mais informações, consulte [Pré-requisitos](#).

Para usar o Microsoft Office com assinaturas baseadas em usuário, você deve conceder permissão ao License Manager para atualizar sua configuração de VPC. Quando você configura sua VPC, o License Manager cria [VPC endpoints](#) em seu nome. Esses endpoints são necessários para que seus atributos se conectem aos servidores de ativação e permaneçam em conformidade.

Você deve configurar o encaminhamento de DNS para quaisquer VPCs adicionais às quais AWS Managed Microsoft AD você se registra para assinaturas baseadas em usuário. Se você tiver várias assinaturas baseadas em usuário Regiões da AWS, cada região deverá ter a sua própria, AWS Managed Microsoft AD com o encaminhamento de DNS configurado da seguinte forma.

É possível usar um dos métodos a seguir para configurar o ambiente para assinaturas baseadas no usuário.

Console (Active Directory)

Para configurar AWS Managed Microsoft AD para assinaturas baseadas no usuário (Console)

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Navegue até a página Configurações escolhendo Configurações no painel de navegação à esquerda ou escolha Abrir configurações no banner.
3. Na página Configurações, na seção AWS Managed Microsoft AD, selecione Configurar.
4. Para o Nome e ID do Diretório gerenciado de AWS , escolha o diretório que contém os usuários para os quais deseja criar assinaturas baseadas no usuário.

5. Em Nome e ID do produto, selecione os produtos necessários e escolha Configurar.

Depois de escolher Configurar, a seção AWS Managed Microsoft AD na página Configurações exibirá o ID de diretório com o status de configuração. Quando o processo de configuração estiver concluído, o Status exibirá Configurado e você poderá prosseguir com as etapas restantes.

Console (Active Directory and VPC)

Para configurar AWS Managed Microsoft AD para assinaturas baseadas no usuário (Console)

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Navegue até a página Configurações escolhendo Configurações no painel de navegação à esquerda ou escolha Abrir configurações no banner.
3. Na página Configurações, na seção AWS Managed Microsoft AD, selecione Configurar.
4. Para o Nome e ID do Diretório gerenciado de AWS, escolha o diretório que contém os usuários para os quais deseja criar assinaturas baseadas no usuário.
5. Em Nome e ID do produto, selecione todos os produtos necessários.
6. Para a nuvem privada virtual, escolha uma VPC para configuração adicional.
7. Para sub-redes para vpc-**x**, escolha pelo menos uma sub-rede na qual provisionar endpoints da VPC.
8. Em Grupos de segurança para vpc-**x**, escolha o grupo de segurança que você criou para associar aos endpoints da VPC e, em seguida, escolha Configurar.

Depois de escolher Configurar, as seções AWS Managed Microsoft AD e Nuvem privada virtual na página Configurações exibirão o ID de diretório e o ID de VPC com o status de Configuração. Quando o processo de configuração estiver concluído, cada Status exibirá Configurado e você poderá prosseguir com as etapas restantes.

AWS CLI

Para configurar AWS Managed Microsoft AD para assinaturas baseadas no usuário (AWS CLI)

Você pode registrá-lo AWS Managed Microsoft AD como provedor de identidade para assinaturas baseadas em usuário com a operação. [RegisterIdentityProvider](#)

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

Para configurar AWS Managed Microsoft AD e sua VPC para assinaturas baseadas em usuário (AWS CLI)

Você pode registrá-lo AWS Managed Microsoft AD como provedor de identidade e configurar sua VPC para assinaturas baseadas em usuário com a operação. [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 obter mais informações sobre produtos de software disponíveis, consulte [Software para assinaturas baseadas no usuário](#).

Etapa 2: Assinar um produto

Para assinar produtos configurados no AWS Marketplace

Depois de configurar o diretório com os produtos necessários, talvez também seja necessário assinar os produtos necessários. Os produtos com status de assinatura do Marketplace como Inativa exigem que você assine antes de poder associar usuários a uma instância e utilizá-los.

Sua conta deve ter uma assinatura da Licença de Acesso de Assinante dos Serviços de Área de Trabalho Remota do Windows Server (RDS SAL). O Microsoft Remote Desktop Services (RDS), conhecido como Serviços de Terminal no Windows Server 2008 e versões anteriores, é um dos componentes do Microsoft Windows que permite ao usuário assumir o controle de um computador remoto ou máquina virtual por meio de uma conexão de rede. O RDS permite que os usuários acessem remotamente desktops gráficos e aplicativos do Windows.

Todos os usuários associados às instâncias que fornecem produtos de assinatura com base no usuário devem ter uma única assinatura ativa dessa licença, além de todos os outros produtos que quiserem usar. O usuário será inscrito no RDS SAL em seu nome quando assinar um produto de assinatura baseada no usuário.

Note

As licenças do RDS SAL não podem ser usadas separadamente dos produtos de assinatura baseada no usuário com suporte. Para ter mais informações, consulte [Considerações](#).

Você pode assinar seus produtos diretamente no AWS Marketplace usando os seguintes links:

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

Para descobrir e assinar produtos do console do License Manager

Você também pode descobrir e assinar produtos do console do License Manager.

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Produtos.
3. Escolha o nome de um produto para exibir os detalhes da assinatura.
4. Escolha Exibir em AWS Marketplace.
5. Revise os detalhes da assinatura e escolha Continuar para assinar.
6. Revise os termos e escolha Aceitar termos se quiser continuar.

Se você aceitar os termos, a assinatura do produto precisará ser processada. A assinatura ficará com uma mensagem em andamento até ser concluída. Você poderá repetir essas etapas para todos os outros produtos configurados necessários. Depois que todos os produtos necessários tiverem uma assinatura ativa, você poderá prosseguir com a inscrição dos usuários nos produtos.

Note

A fatura estimada de cobranças sobre o número de usuários e os custos relacionados levará 48 horas para aparecer nos períodos de cobrança que não foram encerrados (marcados com status de cobrança pendente) em AWS Billing. Para obter mais informações, consulte [Como visualizar as cobranças mensais](#) no Guia do usuário do AWS Billing .

Etapa 3: Executar uma instância para fornecer assinaturas baseadas no usuário

Depois de assinar um produto, você deve iniciar instâncias para que seus usuários se conectem a partir da AWS Marketplace AMI que inclui o produto. Depois de executar uma instância, AWS Systems Manager tentará ingressar a instância no domínio e realizar configurações e fortalecimento adicionais no atributo. As configurações para tornar a instância pronta para uso podem levar cerca de 20 minutos para serem concluídas. Você pode confirmar se o atributo está pronto para uso na página Associação de usuários do console do License Manager verificando o Status de integridade Active para a instância.

Important

As instâncias que você executa devem atender aos pré-requisitos exigidos para estarem em conformidade. Os atributos que não conseguirem concluir a configuração inicial serão encerrados. Para obter mais informações, consulte [Pré-requisitos](#) e [Solução de problemas com assinaturas baseadas no usuário](#).

Para executar uma instância com assinaturas baseadas no usuário

1. Acesse o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Em Imagens, escolha Catálogo AMI.
3. Escolha AWS Marketplace AMIs.
4. Insira o nome do produto na caixa de pesquisa e pressione enter. Por exemplo, você pode pesquisar por **Visual Studio**.
5. Em Publicador, selecione Amazon Web Services.
6. Escolha Selecionar para o produto que deseja executar uma instância para fornecer assinaturas baseadas no usuário.
7. Escolha Continuar para prosseguir.
8. Escolha Executar instância com AMI.
9. Execute o assistente e garanta que:
 - a. Escolherá um tipo de instância baseada em Nitro que não seja baseada em Graviton.
 - b. Escolherá uma VPC e uma sub-rede a partir das quais a instância possa se conectar ao diretório do AWS Managed Microsoft AD .

- c. Escolha um grupo de segurança que permita a conectividade da sua instância com seu AWS Managed Microsoft AD diretório.
- d. Expanda Detalhes avançados e escolha um perfil do IAM que permita a funcionalidade do Systems Manager para sua instância.

10. Escolha Iniciar instância.

Depois de executar as instâncias da AWS Marketplace AMI, você deve inscrever os usuários no produto e associá-los às instâncias, que fornecem o produto para que eles possam utilizá-lo.

Etapa 4: Associar usuários a uma instância de assinatura baseada no usuário

Depois de assinar a AWS Marketplace AMI do produto necessário, você pode inscrever usuários em um produto e associá-los a uma instância que fornece o produto. Você pode inscrever usuários em produtos e associá-los a uma instância em uma única etapa ou separadamente. Quando você inscreve um usuário, o diretório é verificado para garantir que a identidade do usuário esteja presente. Uma assinatura será criada para cada usuário que você inscrever no produto.

Note

Cada usuário deve ter uma assinatura da Licença de Acesso de Assinante dos Serviços de Área de Trabalho Remota do Windows Server (RDS SAL) e do produto que utilizará. Quando a conta estiver inscrita no RDS SAL, conforme detalhado em [Etapa 2: Assinar um produto](#), o usuário será inscrito no RDS SAL em seu nome quando assinar um produto de assinatura baseada no usuário.

A página Produtos no License Manager exibirá as assinaturas ativas listando o status da assinatura do Marketplace como Ativa. Na página de detalhes do produto, o License Manager exibirá assinaturas ativas de usuários com o status Assinado.

Important

Se o diretório não estiver configurado com o produto, uma barra de notificação aparecerá na parte superior do console aconselhando você a ajustar as configurações do diretório. Na barra de notificação, escolha Abrir configurações para acessar a página Configurações no License Manager e editar o diretório.

Cada usuário deve ter uma assinatura do RDS SAL e do produto que utilizará. A assinatura de usuários em um produto no qual o status da assinatura do Marketplace é Inativo falhará.

Inscrever usuários em um produto e associá-los a uma instância

É possível inscrever usuários em um produto e associá-los a uma instância com o processo a seguir.

Para inscrever e associar usuários a uma instância

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Associação de usuário.
3. Selecione a instância à qual você deseja associar usuários e escolha Inscrever e associar usuários.
4. Especifique até cinco nomes de usuário que existem no diretório, incluindo o nome do domínio, se existirem em um domínio confiável, e escolha Inscrever e associar.

Na página Associação de usuários, os usuários selecionados devem ser exibidos em Usuários com um Status de associação como Associado. Além disso, na página Produtos, você pode revisar a página de detalhes do produto escolhendo o Nome do produto. Os usuários inscritos serão exibidos em Usuários com status de Inscrito.

Inscrever usuário em um produto

Você pode inscrever usuários em um produto usando um dos métodos a seguir.

Console

Para inscrever usuários em um produto (Console)

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Produtos.
3. Selecione um produto para inscrever usuários no qual o status da assinatura do Marketplace seja Ativo e escolha Inscrever usuário.
4. Especifique até cinco nomes de usuário que existem no diretório, incluindo o nome do domínio, se existirem em um domínio confiável, e escolha Inscrever.

Os usuários que estiverem inscritos serão exibidos em Usuários com status de Inscrito.

AWS CLI

Para inscrever usuário em um produto (AWS CLI)

Você pode inscrever usuários em um produto registrado com seu provedor de identidade usando a operação [StartProductSubscription](#).

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

Para inscrever usuários em um produto com um Active Directory autogerenciado (AWS CLI)

Você pode inscrever usuários do seu Active Directory autogerenciado em um produto registrado em seu AWS Managed Microsoft AD diretório usando a [StartProductSubscription](#) operação.

```
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 obter mais informações sobre produtos de software disponíveis, consulte [Software para assinaturas baseadas no usuário](#).

Os usuários que estiverem inscritos serão exibidos em Usuários com status de Inscrito.

Associar usuários a uma instância

É possível associar usuários a uma instância usando um dos métodos a seguir.

Important

Antes de associar um produto a uma instância, você deve primeiro inscrever usuários nos produtos.

Console

Para associar usuários a uma instância (Console)

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Associação de usuário.
3. Selecione a instância à qual você deseja associar usuários e escolha Associar usuários.
4. Especifique até cinco nomes de usuário que existem no diretório, incluindo o nome do domínio, se existirem em um domínio confiável, e escolha Associar.

Na página Associação de usuários, os usuários selecionados devem ser exibidos em Usuários com um Status de associação como Associado.

AWS CLI

Associar usuários a uma instância (AWS CLI)

É possível associar usuários a uma instância executada para fornecer a assinatura baseada no usuário com a operação [AssociateUser](#).

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

Para associar usuários autogerenciados do Active Directory a uma instância (AWS CLI)

É possível associar usuários a uma instância executada a partir do Active Directory autogerenciado para fornecer a assinatura baseada no usuário com a operação [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 obter mais informações sobre produtos de software disponíveis, consulte [Software para assinaturas baseadas no usuário](#).

Na página Associação de usuários, os usuários selecionados devem ser exibidos em Usuários com um Status de associação como Associado.

Etapa 5: Conectar-se a uma instância de assinatura baseada no usuário

Depois de associar os usuários à instância que fornece o produto, eles podem se conectar à instância se o status de integridade da instância for Ativo. Os usuários precisarão se conectar com suas credenciais de usuário do domínio para utilizar o produto com a identidade associada.

Important

O processo de criar a instância do EC2 e prepará-la para os usuários pode levar cerca de 20 minutos. O status de associação da instância deve ser Ativo para acessá-la e utilizar o produto.

Para se conectar a uma instância de assinatura baseada no usuário

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Associação de usuário.
3. Na página Associação de usuário, confirme se o status de integridade da instância está Ativo.
4. Anote o ID da instância, pois você precisará dele para coletar os detalhes da conexão.
5. Siga as etapas listadas em [Conectar sua instância do Windows usando RDP](#) e, ao mesmo tempo, certifique-se de especificar o nome de usuário totalmente qualificado do usuário associado.

Modificar configurações de diretório para assinaturas baseadas no usuário

É possível adicionar ou remover produtos para assinaturas baseadas no usuário do diretório configurado na página de configurações do License Manager. As etapas serão diferentes se você usar produtos do Microsoft Office porque o License Manager deve criar [endpoints da VPC](#) para essas assinaturas.

Para modificar a configuração do diretório sem os produtos do Microsoft Office

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Configurações.
3. Na página Configurações, na seção AWS Managed Microsoft AD, escolha Editar.

4. Em Nome e ID do produto, selecione produtos adicionais e limpe as seleções anteriores conforme necessário e escolha Salvar alterações.

Para modificar a configuração do diretório com produtos do Microsoft Office

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Navegue até a página Configurações escolhendo Configurações no painel de navegação à esquerda ou escolha Abrir configurações no banner.
3. Na página Configurações, na seção AWS Managed Microsoft AD, escolha Editar.
4. Em Nome e ID do produto, selecione todos os produtos necessários, incluindo o Microsoft Office.
5. Para a nuvem privada virtual, escolha uma VPC para configuração adicional.
6. Para sub-redes para vpc-**x**, escolha pelo menos uma sub-rede na qual provisionar endpoints da VPC.
7. Em Grupos de segurança para vpc-**x**, escolha o grupo de segurança que você criou para associar aos endpoints da VPC e, em seguida, escolha Salvar alterações.

Depois de escolher Salvar alterações, as seções AWS Managed Microsoft AD e Nuvem privada virtual na página Configurações exibirão ID de diretório e ID de VPC com o status de Configuração. Você deve esperar até que o diretório apresente o status de Configurado e a VPC tenha um status de Ativa antes de usar assinaturas baseadas no usuário com o Microsoft Office.

Modificar as configurações de VPC para assinaturas baseadas no usuário

Se você adicionou produtos do Microsoft Office, poderá modificar a configuração da VPC. O License Manager criará [endpoints da VPC](#) em seu nome nas sub-redes que você especificar para que os atributos cheguem aos servidores de ativação e permaneçam em conformidade. Você deve especificar pelo menos duas sub-redes. Para ter mais informações, consulte [Pré-requisitos](#).

Note

As configurações de VPC só estão disponíveis para modificação se o diretório tiver sido configurado com produtos do Microsoft Office. Para ter mais informações, consulte [Conceitos básicos das assinaturas baseadas no usuário](#).

Se você quiser remover todos os endpoints da VPC, consulte [Considerações](#).

Para modificar a configuração do diretório

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Configurações.
3. Na página Configurações, na seção Nuvem privada virtual configurada, escolha Editar.
4. Altere as sub-redes e o grupo de segurança conforme necessário para a VPC configurada e escolha Salvar alterações.

Desassociar usuários de assinaturas baseadas no usuário

É possível desassociar usuários de uma instância para remover o acesso ao atributo.

Note

A exclusão de um usuário do diretório não alterará as associações ou assinaturas do usuário. Você deve desassociar o usuário no License Manager da página de detalhes do produto para remover a associação dele com uma instância.

Para desassociar usuários de assinatura baseada no usuário

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Associação de usuário.
3. Selecione a instância da qual você quer desassociar os usuários.
4. Selecione os nomes de usuário a serem desassociados e, em seguida, escolha Desassociar usuários.

Cancelar a inscrição de usuários em assinaturas baseadas no usuário

Você pode cancelar a assinatura de usuários de um produto para remover o acesso e parar de incorrer em cobranças pelo produto para os usuários.

⚠ Important

Primeiro, o usuário deve ser desassociado das instâncias em que está atualmente associado antes seja possível cancelar a assinatura.

Para cancelar a inscrição de usuários em assinaturas baseadas no usuário

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Produtos.
3. Selecione o produto do qual você deseja cancelar a assinatura de usuários.
4. Selecione os nomes de usuário para cancelar a assinatura e, em seguida, escolha Cancelar assinatura de usuários.

Terminar instâncias do EC2 que fornecem assinaturas baseadas no usuário

É possível excluir uma instância que fornece uma assinatura baseada no usuário quando não precisar mais dela. Isso é chamado de terminar a instância. Primeiro você deve desassociar todos os usuários da instância e, em seguida, terminar a instância do console do Amazon EC2.

ℹ Note

Os usuários devem ser desassociados da instância para parar de incorrer em cobranças pela assinatura. Para ter mais informações, consulte [Desassociar usuários de assinaturas baseadas no usuário](#).

Para identificar e terminar instâncias que fornecem assinaturas baseadas no usuário

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas baseadas no usuário, escolha Associação de usuário.
3. Na página de Associação de usuários, escolha o ID da instância para acessar a página de detalhes da instância.
4. Anote o ID da instância, pois você precisará dele para terminar a instância.
5. Desassociar todos os usuários da instância.

6. Siga as etapas listadas em [Terminar uma instância](#).

Remover um diretório para assinaturas baseadas no usuário

É possível remover o diretório se não quiser mais usá-lo para assinaturas baseadas no usuário. A remoção da configuração do diretório do License Manager não exclui o diretório em si. Ao remover o diretório, você não poderá associar usuários do diretório para assinaturas baseadas no usuário.

Important

Primeiro, você deve desassociar usuários e terminar as instâncias que fornecem assinaturas baseadas no usuário antes de remover o diretório do License Manager.

Para remover um diretório

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Configurações.
3. Na página Configurações, na AWS Managed Microsoft AD seção, escolha Remove.
4. Insira o texto necessário para confirmar que deseja remover o diretório e escolha Remove.

Depois de escolher Remove, a seção AWS Managed Microsoft AD na página Configurações exibirá o ID de diretório com o status de configuração. Quando o processo de configuração estiver concluído, o diretório deverá ser removido da seção AWS Managed Microsoft AD.

Solução de problemas com assinaturas baseadas no usuário

Veja a seguir dicas de solução de problemas para ajudar a resolver problemas que podem ocorrer no AWS License Manager com assinaturas baseadas no usuário.

Sumário

- [Solução de problemas de conformidade da instância](#)
- [Solução de problemas de conformidade de licenças](#)
- [Solução de problemas de conectividade de instância](#)
- [Solucionar falhas ao ingressar no domínio](#)
- [Solução de problemas de conectividade do Systems Manager](#)

- [Solução de problemas do Run Command do Systems Manager](#)

Solução de problemas de conformidade da instância

As instâncias que fornecem assinaturas baseadas no usuário devem permanecer com status íntegro para estarem em conformidade. As instâncias marcadas como não íntegras não atendem mais aos pré-requisitos exigidos. O License Manager tentará retornar a instância ao status íntegro, mas as instâncias que não conseguirem retornar ao status íntegro serão terminadas.

As instâncias que forem executadas para fornecer assinaturas baseadas no usuário e não conseguirem concluir a configuração inicial serão terminadas. Você deve corrigir o problema de configuração e executar novas instâncias para fornecer assinaturas baseadas no usuário nesse cenário. Para obter mais informações, consulte [Pré-requisitos](#).

Solução de problemas de conformidade de licenças

Se o diretório está configurado para fornecer assinaturas baseadas no usuário com o Microsoft Office, você deverá garantir que os atributos possam se conectar aos endpoints da VPC criados pelo License Manager. Os endpoints exigem tráfego de entrada na porta TCP 1688 das instâncias que fornecem assinaturas baseadas no usuário.

É possível usar o [Reachability Analyzer](#) para ajudar a confirmar se a configuração de rede das instâncias que fornecem assinaturas baseadas no usuário e os endpoints da VPC estão configurados corretamente. É possível especificar como origem uma ID de instância executada em uma sub-rede que fornece assinaturas baseadas no usuário e um endpoint da VPC provisionado para produtos do Microsoft Office como destino. Especifique TCP como protocolo e 1688 como porta de destino para o caminho a ser analisado. Para obter mais informações, consulte [Como posso solucionar problemas de conectividade em meus endpoints da VPC de gateway e interface?](#).

Solução de problemas de conectividade de instância

Os usuários devem poder usar o RDP para se conectar às instâncias que fornecem assinaturas baseadas no usuário para utilizar os produtos contidos. Para obter mais informações sobre como solucionar problemas de conectividade de instâncias, consulte [Solucionar problemas de conexão com sua instância do Windows](#) no Guia do usuário do Amazon EC2.

Solucionar falhas ao ingressar no domínio

Os usuários devem poder se conectar às instâncias que fornecem os produtos de assinatura baseados em usuário com suas identidades de usuário, a partir do diretório definido nas

configurações do License Manager. As instâncias que não conseguirem ingressar no domínio serão encerradas.

Para solucionar o problema, talvez seja necessário executar uma instância e [ingressar manualmente no domínio](#) para que o atributo não seja encerrado antes de poder investigar. A instância deve receber e executar o comando de execução do Systems Manager com êxito, e a instância também deve ser capaz de ingressar no domínio dentro do sistema operacional. Para obter mais informações, consulte [Compreender os status de comando](#) no Guia do usuário do AWS Systems Manager e [Como solucionar erros que ocorrem quando computadores baseados no Windows ingressam em um domínio](#) no site da Microsoft.

Solução de problemas de conectividade do Systems Manager

As instâncias que fornecem assinaturas baseadas no usuário devem ser gerenciadas AWS Systems Manager ou serão encerradas. Para obter mais informações, consulte [Solução de problemas do SSM Agent](#) e [Solução de problemas de disponibilidade do nó gerenciado](#) no Guia do usuário do AWS Systems Manager .

Solução de problemas do Run Command do Systems Manager

O Run Command, um atributo do Systems Manager, é usado com instâncias que fornecem assinaturas baseadas no usuário para ingressar no domínio, fortalecer o sistema operacional e realizar auditorias de acesso ao produto incluído. Para obter mais informações, consulte [Entender os status dos comandos](#) no Guia do usuário do AWS Systems Manager .

Gerencie assinaturas Linux no License Manager

Com AWS License Manager, você pode visualizar e gerenciar assinaturas comerciais do Linux que suas instâncias do Amazon EC2 usam. Você pode monitorar a utilização de suas assinaturas Linux para as contas Regiões da AWS e nas AWS Organizations que você definiu em suas configurações. O License Manager oferece uma visão abrangente de suas instâncias em execução que usam assinaturas Linux. Também indica quando uma instância tem mais de uma assinatura definida.

Os dados que o License Manager descobre são agregados e exibidos no console do License Manager e no painel da Amazon CloudWatch . Você também pode acessar os dados da sua assinatura por meio da API AWS CLI de assinatura Linux do License Manager ou dos SDKs associados.

As assinaturas de licenças do Linux podem vir das seguintes fontes:

AMIs incluídas na assinatura

- Red Hat Enterprise Linux (RHEL)
- Modelo RHEL BYOS (Bring Your Own Subscription model) com o Red Hat Cloud Access Program
- SUSE Linux Enterprise Server
- AMI incluída na assinatura do Ubuntu Pro

Provedores de assinatura de terceiros

- Assinatura RHEL do Red Hat Subscription Manager (RHSM)

A descoberta de assinaturas do Linux usa o modelo de consistência eventual. Um modelo de consistência determina a maneira e o tempo em que os dados são carregados e apresentados na visualização de assinaturas do Linux. Com esse modelo, o License Manager garante que seus dados de assinatura do Linux sejam atualizados periodicamente a partir de seus recursos. Caso alguns dados não sejam ingeridos durante esses intervalos, as informações são fornecidas na próxima emissão métrica. Esse comportamento pode atrasar a exibição de atributos, como instâncias Linux comerciais do EC2 recém-lançadas, no painel de assinaturas do Linux.

Note

Pode levar até 36 horas para que a descoberta inicial de atributos seja concluída e até 12 horas para que as instâncias recém-lançadas sejam descobertas e relatadas. Depois que seus recursos são descobertos, as CloudWatch métricas da Amazon são emitidas de hora em hora para dados de assinaturas Linux.

Se suas contas estiverem ativas AWS Organizations, você poderá registrar uma conta de membro como administrador delegado. Para ter mais informações, consulte [Administradores delegados](#).

Assinaturas duplicadas detectadas

Quando o License Manager detecta duas assinaturas Linux na mesma instância do EC2, ele define o alerta de assinatura duplicada. Você pode visualizar e filtrar dados de assinatura do Linux na página Instâncias no console do License Manager.

Instâncias do Red Hat Enterprise Linux 7 Extended Lifecycle Support (RHEL 7 ELS): quando você executa uma instância a partir de uma AMI incluída na assinatura para o RHEL 7 ELS, você

ainda deve registrar sua instância na Red Hat e consumir uma autorização. Nesse caso, o License Manager relata uma assinatura duplicada, mas esse é o comportamento esperado.

Outras instâncias do Red Hat Linux: recomendamos que você pesquise o inventário de assinaturas no [Red Hat Hybrid Cloud Console](#) para descobrir quais assinaturas sua instância consome.

Tópicos adicionais

- [Configurar a descoberta de assinaturas do Linux](#)
- [Veja os dados da instância descoberta](#)
- [Informações de cobrança de assinaturas Linux](#)
- [Gerencie CloudWatch alarmes da Amazon para assinaturas Linux](#)

Configurar a descoberta de assinaturas do Linux

Você pode configurar a descoberta de assinaturas Linux por meio do console do License Manager AWS CLI, da API de assinatura Linux do License Manager ou dos SDKs associados. Ao ativar a descoberta de assinaturas Linux para o Regiões da AWS que você especifica, você pode, opcionalmente, estender a descoberta às suas contas em AWS Organizations Se você não quiser mais monitorar a utilização da assinatura, você também pode desativar a descoberta.

Note

Você pode descobrir e exibir até 5.000 recursos por conta, Região da AWS por padrão. Para solicitar um aumento desse limite, use o [Formulário de aumento de limite](#).

Tópicos

- [Configurar a descoberta de assinaturas do Linux](#)
- [Ative a descoberta de assinaturas do Red Hat Subscription Manager](#)
- [Motivos de status da descoberta de atributos](#)
- [Desative a descoberta de assinaturas Linux](#)

Configurar a descoberta de assinaturas do Linux

Para configurar a descoberta de assinaturas do Linux na página Configurações no console do License Manager, siga estas etapas:

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação, selecione Configurações. Isso abre a página Configurações.
3. Abra a guia Assinaturas Linux e escolha Configurar. Isso abre o painel Configurar configurações de assinaturas Linux.
4. Selecione a Fonte em Regiões da AWS que a descoberta de assinaturas do Linux deve ser executada.
5. Para agregar dados de assinatura em todas as suas contas em AWS Organizations, selecione Vincular AWS Organizations. Essa opção só aparece se AWS Organizations estiver configurada para sua conta.
6. Analise e reconheça a opção que concede AWS License Manager permissão para criar uma função vinculada ao serviço para assinaturas Linux.
7. Escolha Save configuration.

Ative a descoberta de assinaturas do Red Hat Subscription Manager

Para recuperar informações de assinatura do Red Hat Subscription Manager (RHSM) em seu nome, o License Manager deve fornecer as credenciais da API da sua conta de cliente Red Hat.

Pré-requisitos

Antes de ativar a descoberta de assinaturas, verifique se você atendeu aos seguintes pré-requisitos.

- A descoberta padrão para assinaturas Linux deve ser ativada para você Conta da AWS antes que você possa configurar a descoberta de assinaturas do RHSM. Se a descoberta padrão não estiver ativada, consulte [Configurar a descoberta de assinaturas do Linux](#).
- Se você usa um login corporativo da Red Hat fornecido pelo administrador da organização, certifique-se de que seu ID de login tenha as seguintes funções e permissões atribuídas:
 - Função: Gerenciar suas assinaturas
 - Permissões: View All, ou View/Edit All

Se sua ID de login não tiver as funções e permissões necessárias, entre em contato com o Administrador da Organização do portal Red Hat e solicite que ela seja adicionada ao seu login. Para obter mais informações sobre funções e permissões da Red Hat, consulte [Funções e permissões do Red Hat Customer Portal](#). Para obter mais informações sobre como entrar em contato com o administrador da organização do Red Hat Portal, consulte [Como eu sei quem é meu administrador da organização?](#) na base de conhecimento do Red Hat Customer Portal.

- Para ativar a descoberta da assinatura do RHSM, você deve fornecer o token offline da API da conta do cliente Red Hat ou um AWS Secrets Manager segredo que contenha o token offline. Para obter seu token offline, siga as etapas descritas em [Geração de um novo token offline](#) no site de documentação da Red Hat.

Important

Sua segurança é importante para nós. Seu token de acesso off-line da Red Hat é armazenado com segurança no Secrets Manager. O License Manager usa seu segredo para gerar um token de acesso temporário sempre que solicita detalhes da assinatura da Red Hat.

Ativação

Para ativar a descoberta do RHSM na página Configurações no console do License Manager, siga estas etapas:

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação, selecione Configurações.
3. Na página Configurações, abra a guia Assinaturas Linux.
4. Escolha Editar para atualizar suas configurações de assinatura do Linux. Isso abre a página de descoberta de Configurar assinaturas Linux.
5. Para iniciar o processo de ativação, marque a caixa de seleção Ativar a descoberta do Red Hat Subscription Manager (RHSM). Isso exibe o painel Vincular conta RHSM.
6. Selecione a opção Segredo (Token) que se aplica ao seu segredo e siga as etapas restantes que dependem da opção escolhida.
7. Opção: criar um novo segredo — recomendado

Forneça o token de acesso off-line da Red Hat e deixe o License Manager criar o segredo de acesso no Secrets Manager em seu nome.

- a. Insira um nome para seu segredo em Nome secreto.
- b. Cole seu token de acesso off-line da Red Hat na caixa de token offline. Certifique-se de que não haja espaços extras ou quebras de linha antes ou depois do valor do token.

Opção: Selecione um segredo

Selecione um segredo existente no Secrets Manager que contenha seu token de acesso offline da Red Hat.

8. (opcional) Adicione tags para seu segredo.
9. Selecione a caixa de seleção na parte inferior da página para reconhecer que, ao ativar a descoberta do Red Hat Subscription Manager, você concede acesso ao AWS License Manager serviço para coletar dados relacionados às assinaturas da Red Hat usadas nas instâncias do Amazon EC2.
10. Selecione Ativar.

Motivos de status da descoberta de atributos

AWS License Manager exibirá um status e um motivo de status correspondente para cada um Região da AWS que você escolher para habilitar a descoberta para assinaturas Linux. O motivo do status variará se você tiver vinculado assinaturas Linux com: AWS Organizations

- In progress (Em andamento)
- Com êxito
- Failed (Falha)

O motivo do status exibido para cada região que você escolher mostrará até dois motivos de status por vez. A tabela a seguir oferece mais detalhes:

Ação de motivo de status	Descrição
Account-onboard	Integração em uma única conta.
Account-offboard	Não integração em uma única conta.
Org-onboard	Integração de uma organização inteira.
Org-Offboard	Não integração de uma organização inteira.

É possível chamar a API `UpdateServiceSettings` e, posteriormente, chamar a API `GetServiceSettings` para monitorar o progresso da habilitação das assinaturas Linux. Cada status e motivo de status podem ser aplicados a várias regiões ao mesmo tempo. A tabela a seguir fornece mais detalhes sobre o status e o motivo do status:

Status	Motivo do status	Descrição
Em andamento	"Region": "Account-Onboard: Pending"	A habilitação de assinaturas Linux para uma única conta está em andamento.
	"Region": "Org-Onboard: Pending"	A habilitação de assinaturas Linux para uma organização está em andamento.
	"Region": "Account-Offboard: Pending"	A desabilitação de assinaturas Linux para uma única conta está em andamento.
	"Region": "Org-Offboard: Pending"	A desabilitação de assinaturas Linux para uma organização está em andamento.
Com êxito	"Region": "Account-Onboard: Successful"	A habilitação de assinaturas Linux para uma única conta foi bem-sucedida.
	"Region": "Org-Onboard: Successful"	A habilitação de assinaturas Linux para uma organização foi bem-sucedida.
	"Region": "Account-Offboard: Successful"	A desabilitação de assinaturas Linux para uma única conta foi bem-sucedida.
	"Region": "Org-Offboard: Successful"	A desabilitação de assinaturas Linux para uma organização foi bem-sucedida.

Status	Motivo do status	Descrição
Failed (Falha)	"Region": "Account-Onboard: Failed - Service-linked role not present"	A ativação de assinaturas Linux para uma única conta falhou porque não foi criada o perfil vinculado ao serviço, que é obrigatória. Crie o perfil necessário e tente novamente.
	"Region": "Account-Onboard: Failed - An internal error occurred"	A ativação de assinaturas do Linux para uma única conta falhou devido a um erro interno.
	"Region": "Org-Onboard: Failed - Account isn't the management account"	A habilitação de assinaturas Linux para uma organização falhou porque a conta que executa a operação não é a conta de gerenciamento da organização. Faça login na conta de gerenciamento e tente novamente.
	"Region": "Org-Onboard: Failed - Account isn't part of an organization"	A habilitação de assinaturas Linux para uma organização falhou porque a conta que executa a operação não pertence à organização. Experimente a operação a partir de uma conta da organização ou adicione essa conta à organização e tente novamente.

Status	Motivo do status	Descrição
	<code>"Region": "Org-Onboard: Failed - Linux subscriptions can't access the organization"</code>	A habilitação de assinaturas Linux para uma organização falhou porque o License Manager não tem as permissões para acessar a organização. Crie um perfil vinculado ao serviço para assinaturas do Linux e tente novamente.

Desative a descoberta de assinaturas Linux

Você pode desativar a descoberta de assinaturas Linux na página de configurações. AWS License Manager No entanto, se você ativou a descoberta para

Warning

Se você desativar a descoberta, todos os seus dados descobertos anteriormente para assinaturas Linux serão removidos do AWS License Manager

Para desabilitar a descoberta de assinaturas Linux

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Configurações.
3. Na página Configurações, escolha a guia Assinaturas Linux e escolha Desativar descoberta de assinaturas Linux.
4. Digite **Disable** e escolha Desativar para confirmar a desativação.
5. (Opcional) Remover o perfil vinculado ao serviço usada para assinaturas do Linux. Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço para o License Manager](#).
6. (Opcional) Desative o acesso confiável entre o License Manager e sua organização. Para obter mais informações, consulte [AWS License ManagerAWS Organizations e](#).

Veja os dados da instância descoberta

Depois que o License Manager concluir o processo inicial de descoberta de recursos no seu selecionado Regiões da AWS, você poderá visualizar os resultados no console. Se você optar por vincular AWS Organizations, o License Manager agrega dados de contas em toda a sua organização. Para ver uma lista de instâncias com assinaturas que atendem aos seus critérios de filtro, navegue até a seção Instâncias do AWS License Manager console. A lista exibe os seguintes campos principais.

- ID da instância – a ID da instância.
- Status – o status da instância.
- Tipo da instância – o tipo da instância.
- Assinatura — O nome da assinatura de licença que a instância usa.
- Alerta de duplicatas — Indica que você tem duas assinaturas de licença diferentes para o mesmo software na sua instância.
- ID da conta – a ID da conta proprietária da instância.
- Região — A região Região da AWS em que a instância reside.
- ID do AMI – a ID do AMI usado para executar a instância.
- Operação de uso – a operação da instância e o código de faturamento associado à AMI. Para ter mais informações, consulte [Valores da operação de uso](#).
- Código do produto – O código do produto associado ao AMI usado para executar a instância. Para obter mais informações, consulte [Códigos do produto AMI](#).
- LastUpdatedTime— A hora em que a última descoberta atualizou os detalhes da instância.

Tópicos

- [Visualize dados de todas as instâncias](#)
- [Visualize dados de instâncias por assinatura](#)

Visualize dados de todas as instâncias

Você pode visualizar e filtrar os dados de assinatura do Linux que o License Manager descobriu para as instâncias em sua conta ou AWS Organizations, da seguinte forma.

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.

2. No painel de navegação à esquerda, em Assinaturas Linux, escolha Instâncias. Isso exibe uma lista de instâncias com dados de assinatura do Linux.
3. (Opcional) Você pode usar os seguintes filtros para otimizar seus resultados:
 - Conta
 - ID de AMI
 - Assinatura duplicada
 - ID da instância
 - Região
 - Código do produto
 - Operação de uso
4. (Opcional) Escolha Exportar visualização como CSV para exportar dados de todas as instâncias como um arquivo de valores separados por vírgula (CSV).

Visualize dados de instâncias por assinatura

É possível ver os dados de todas as instâncias que foram agregados em todas as contas da organização, nas regiões escolhidas.

Para visualizar dados descobertos por instâncias com uma assinatura específica

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas Linux, escolha Assinaturas.
3. Na coluna Nome da assinatura, escolha a assinatura da qual você gostaria de ver os dados.
4. Escolha a guia Instâncias e revise os dados conforme necessário no console. É possível filtrar os dados por:
 - ID da instância
 - Conta
 - Região
 - ID de AMI
 - Operação de uso
 - Código do produto

- (Opcional) Escolha Exportar visualização como CSV para exportar dados das instâncias com essa assinatura como um arquivo de valores separados por vírgula (CSV).

Informações de cobrança de assinaturas Linux

Cada assinatura comercial do Linux executada no Amazon EC2 tem informações de cobrança associadas à Amazon Machine Image (AMI). As assinaturas comerciais do Linux têm a operação de uso do Amazon EC2 AWS Marketplace , o código do produto ou uma combinação de ambos. Para obter mais informações, consulte os [campos de informações de cobrança do AMI](#) no Guia do usuário do Amazon Elastic Compute Cloud para instâncias Linux e os [códigos do produto AMI](#) no Guia do vendedor do AWS Marketplace .

Nome da assinatura	Operação de uso do Amazon EC2	AWS Marketplace código do produto	Tipo de assinatura
Red Hat Enterprise Linux Server BYOS	RunInstances0:00g	x	Traga seu próprio modelo de assinatura (BYOS)
Red Hat Enterprise Linux Server	RunInstances00:10	x	Assinatura EC2 incluída
Red Hat Enterprise Linux com complemento de alta disponibilidade	RunInstances:1010	x	Assinatura EC2 incluída
Red Hat Enterprise Linux com SQL Server Standard e alta disponibilidade	RunInstances:1014	x	Assinatura EC2 incluída
Red Hat Enterprise Linux com SQL Server Enterprise e alta disponibilidade	RunInstances: 1110	x	Assinatura EC2 incluída

Nome da assinatura	Operação de uso do Amazon EC2	AWS Marketplace código do produto	Tipo de assinatura
Red Hat Enterprise Linux com SQL Server Standard	RunInstances00:14	x	Assinatura EC2 incluída
Red Hat Enterprise Linux com SQL Server Web	RunInstances02:10	x	Assinatura EC2 incluída
Red Hat Enterprise Linux com SQL Server Enterprise	RunInstances01:10	x	Assinatura EC2 incluída
SUSE Linux Enterprise Server	RunInstances: 000g	x	Assinatura EC2 incluída
Red Hat Enterprise Linux para SAP com alta disponibilidade e serviços de atualização	RunInstances00:10	✓	AWS Marketplace assinatura ¹
SUSE Linux Enterprise Server com SAP	x	✓	AWS Marketplace Assinatura
Ubuntu Pro	RunInstances0g00	✓	AWS Marketplace Assinatura
Workstation do Red Hat Enterprise Linux	x	✓	AWS Marketplace Assinatura

¹ Essa assinatura tem uma operação de uso do Amazon EC2 e um código de AWS Marketplace produto.

Métricas de uso para assinaturas Linux

As seguintes métricas e dimensões estão disponíveis para assinaturas Linux:

Métrica	Descrição
RunningInstancesCount	<p>O número total de instâncias em execução na conta atual agrupadas pelo nome da assinatura ou, pelo nome da assinatura e região.</p> <p>Unidades: contagem</p> <p>Dimensões:</p> <p>SubscriptionName : o nome da assinatura.</p> <p>Region: a região em que o atributo usando uma assinatura comercial do Linux foi descoberto.</p>

Gerencie CloudWatch alarmes da Amazon para assinaturas Linux

A página da lista de assinaturas Linux no console do License Manager mostra os seguintes detalhes importantes, incluindo os CloudWatch alarmes da Amazon que você configurou para cada assinatura Linux que o License Manager encontrou em suas instâncias.

- Nome da assinatura
- Tipo de assinatura
- Número de instâncias em execução por assinatura
- CloudWatch Alarmes configurados da Amazon

Quando você escolhe uma assinatura Linux na página da lista, a guia Métricas de uso e alarmes exibe os dados dessa assinatura. Nessa guia, os CloudWatch painéis da Amazon são exibidos para a assinatura escolhida no console do License Manager. Você pode ajustar o painel para abranger um determinado período ou intervalo de avaliação, em horas, dias ou uma semana a partir de uma data selecionada.

Na guia Métricas de uso e alarmes, cada assinatura tem uma seção de Alarmes com os seguintes detalhes:

- Nome do alarme – O nome do alarme.
- Estado – o estado do alarme.

- **Dimensão** – as dimensões do alarme. A dimensão incluirá o tipo de instância Região da AWS e que foi definido.
- **Condição** – a condição do alarme. A condição incluirá o operador de comparação e o valor limite de alarme que foi definido.

Você pode criar CloudWatch alarmes usando as dimensões e condições definidas para rastrear e alertar com base na utilização atual da sua assinatura. O console de assinaturas do Linux exibe um resumo dos nomes de assinatura em uso, os tipos de assinatura, a quantidade de instâncias em execução de cada uma e o status do alarme.

A seguir estão os possíveis estados CloudWatch de alarme:

- **OK** – a métrica ou a expressão está dentro do limite definido.
- **ALARME** – a métrica ou a expressão está fora do limite definido.
- **DADOS INSUFICIENTES** – o alarme acabou de ser acionado, a métrica não está disponível ou não há dados suficientes para a métrica determinar o estado do alarme.

Tópicos

- [Crie um CloudWatch alarme para assinaturas Linux](#)
- [Modificar um CloudWatch alarme para assinaturas Linux](#)
- [Excluir um CloudWatch alarme para assinaturas Linux](#)

Crie um CloudWatch alarme para assinaturas Linux

É possível criar alarmes para cada assinatura comercial do Linux descoberta nas instâncias do EC2 em execução. Se necessário, é possível criar vários alarmes com diferentes dimensões e condições para cada assinatura.

Para criar um CloudWatch alarme para assinaturas Linux a partir do console

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas Linux, escolha Assinaturas.
3. Na coluna Nome da assinatura, escolha a assinatura para a qual criar um alarme e escolha Criar alarme.
4. Especifique o seguinte para o alarme:

- Nome do alarme — especifique um nome que se assemelhe ao `AWS-LM-LS-AlarmName`.
 - Tipo de instância — escolha um tipo de instância que usará a assinatura selecionada.
 - Região de uso — escolha as regiões para as quais criar os alarmes.
 - Operador de comparação — o operador de comparação para o limite de alarme.
 - Valor do limite do alarme — o valor do limite do alarme.
5. Escolha Create para criar o alarme.

Modificar um CloudWatch alarme para assinaturas Linux

Você pode modificar CloudWatch os alarmes existentes no console do License Manager para se adaptar às mudanças nos requisitos.

Para modificar um CloudWatch alarme para assinaturas Linux a partir do console

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas Linux, escolha Assinaturas.
3. Na coluna Nome da assinatura, escolha a assinatura a ser modificada e escolha Editar.
4. Modifique os valores definidos conforme necessário.
5. Escolha Editar para modificar o alarme.

Excluir um CloudWatch alarme para assinaturas Linux

Você pode excluir CloudWatch os alarmes existentes do console do License Manager para se adaptar às mudanças nos requisitos.

Para excluir um CloudWatch alarme para assinaturas Linux do console

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, em Assinaturas Linux, escolha Assinaturas.
3. Na coluna Nome da assinatura, escolha a assinatura a ser modificada e escolha Excluir.

Configurações em AWS License Manager

A seção Configurações do AWS License Manager console exibe as configurações da conta atual. Você deve definir as configurações para ativar a funcionalidade associada.

Managed licenses

As configurações a seguir são configuráveis para licenças gerenciadas:

- Distribuição de direitos gerenciados e licenças autogerenciadas para sua organização
- Descoberta de atributos entre contas
- Notificação do Amazon SNS

Para ter mais informações, consulte [Licenças gerenciadas](#).

Linux subscriptions

As configurações a seguir são configuráveis para assinaturas Linux:

- Descoberta e agregação de dados de assinatura de licenças do Commercial Linux
- Descoberta do Red Hat Subscription Manager (RHSM) para assinaturas Linux

Para ter mais informações, consulte [Assinaturas Linux](#).

User-based subscriptions

As configurações a seguir são configuráveis para assinaturas baseadas no usuário:

- AWS Managed Microsoft AD
- Nuvem privada virtual (VPC)

Para ter mais informações, consulte [Conversão de tipo de licença](#).

Delegated administration

Essa guia será exibida se sua conta tiver acesso administrativo à sua organização. Como administrador, você pode registrar um administrador delegado a partir do AWS CLI ou AWS Management Console. Para ter mais informações, consulte [Administradores delegados](#).

Tópicos de configurações

- [Editar configurações do License Manager](#)
- [Licenças gerenciadas](#)
 - [Detalhes da conta](#)
 - [Descoberta de atributos entre contas](#)
 - [Simple Notification Service \(SNS\)](#)
- [Assinaturas Linux](#)
 - [Configurações de assinaturas Linux](#)
 - [Descoberta do Red Hat Subscription Manager](#)
- [Conversão de tipo de licença](#)
 - [AWS Managed Microsoft AD](#)
 - [Virtual private cloud](#)
- [Administradores delegados](#)
 - [Regiões com suporte aos administradores delegados](#)
 - [Registro de um administrador delegado](#)
 - [Cancelar registro de um administrador delegado](#)

Editar configurações do License Manager

Para editar suas configurações do License Manager, siga estas etapas:

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Configurações.
3. Escolha a guia que contém as configurações a serem definidas. Por exemplo, escolha Licenças gerenciadas para configurar os Detalhes da conta.
4. Depois de definir suas configurações, escolha Salvar ou escolha Cancelar para voltar atrás.

Licenças gerenciadas

As seguintes configurações estão disponíveis para as licenças gerenciadas.

Detalhes da conta

Você pode revisar os detalhes da sua conta para ver informações como o tipo de conta, se as contas AWS Organizations estão vinculadas, o ARN do bucket S3 do License Manager da conta e o ARN

do AWS Resource Access Manager compartilhamento. Esta seção também permite que você vincule suas AWS Organizations contas.

Para distribuir direitos gerenciados ou licenças autogerenciadas em sua organização, escolha Vincular contas. AWS Organizations As concessões distribuídas para direitos gerenciados são aceitas automaticamente por todas as contas de seus membros. Quando você seleciona essa opção, adicionamos um perfil vinculado ao serviço às contas de [gerenciamento](#) e de [membro](#).

Note

Para habilitar esta opção, você deve estar conectado à sua conta de gerenciamento e todos os atributos devem estar habilitados no AWS Organizations. Para obter mais informações, consulte [Enabling all features in your organization](#) no Manual do usuário do AWS Organizations .

Essa seleção também cria um compartilhamento de AWS Resource Access Manager recursos em sua conta de gerenciamento, o que permite que você compartilhe facilmente licenças autogerenciadas. Para obter mais informações, consulte o [Guia do usuário do AWS Resource Access Manager](#).

Para desativar essa opção, chame a [UpdateServiceSettingsAPI](#).

Descoberta de atributos entre contas

É possível ativar a descoberta de atributos entre contas para gerenciar o uso da licença em todas as contas no AWS Organizations.

Para habilitar a descoberta de atributos entre contas em sua organização, escolha Ativar para descoberta de atributos entre contas. Quando você ativa a descoberta de recursos entre contas, ela é AWS Organizations automaticamente vinculada para realizar a descoberta de recursos em todas as suas contas.

O License Manager usa o [inventário do Systems Manager](#) para descobrir o uso de software. Verifique se configurou o inventário do SSM em todos os seus atributos. A consulta do inventário do Systems Manager exige o seguinte:

- [Sincronização de dados de atributos](#) para armazenar inventário em um bucket do Amazon S3.
- [Amazon Athena](#) para agregar dados de inventário de suas contas no AWS Organizations.
- [AWS Glue](#) para fornecer uma experiência de consulta rápida.

Note

Os itens a seguir Regiões da AWS não exigem Amazon Athena nem AWS Glue consultam nem agregam dados de inventário do Systems Manager para descobrir o uso do software:

- Ásia-Pacífico (Jacarta)
- Israel (Tel Aviv)

Simple Notification Service (SNS)

É possível configurar um Amazon SNS para receber notificações e alertas do License Manager.

Para configurar um tópico do Amazon SNS

1. Escolha Editar ao lado de Simple Notification Service (SNS).
2. Especifique um ARN do tópico do SNS no seguinte formato:

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

3. Escolha Salvar alterações.

Assinaturas Linux

Durante o processo de descoberta, o License Manager pesquisa as instâncias do EC2 que estão sendo executadas sob suas Conta da AWS assinaturas Linux. Ele detecta se você tem mais de uma assinatura Linux definida para qualquer instância e agrega os dados.

Configurações de assinaturas Linux

Você pode definir as configurações das assinaturas Linux para controlar como o License Manager lida com a descoberta e a agregação. As configurações padrão de descoberta se aplicam a todos os tipos de assinaturas Linux.

As ações a seguir estão disponíveis para configurar a descoberta de assinaturas do Linux.

Edite

Altere as configurações para descoberta de assinaturas do Linux.

Desativar

Desative a descoberta e a agregação de assinaturas Linux associadas às suas instâncias do EC2. Se você também tiver a descoberta ativada para o Red Hat Subscription Manager, o License Manager primeiro desativa seu provedor registrado no RHSM e depois continua com a desativação para descoberta de assinaturas Linux.

Note

A desativação não afeta seu segredo de acesso ao Red Hat Subscription Manager (RHSM). Para evitar cobranças em sua AWS fatura por um segredo associado que você não precisa mais, consulte [Excluir um AWS Secrets Manager segredo](#) no Guia do AWS Secrets Manager usuário.

As configurações a seguir são exibidas no console do License Manager para descoberta de assinaturas do Linux.

Configurações de descoberta de assinaturas do Linux

Descoberta de assinaturas Linux

Indica se você ativou a descoberta de assinaturas Linux para sua conta.

Origem Regiões da AWS

Regiões da AWS onde você deseja que o License Manager descubra os dados da assinatura.

AWS Organizations

Opcionalmente, adicione dados de assinatura em todas as suas contas em AWS Organizations

Para ter mais informações, consulte [Gerencie assinaturas Linux no License Manager](#).

Descoberta do Red Hat Subscription Manager

Se você ativou a descoberta de assinaturas do Linux, você pode configurar o acesso ao License Manager para recuperar dados adicionais para assinaturas do RHEL que são gerenciadas por meio do Red Hat Subscription Manager (RHSM).

As ações a seguir estão disponíveis para configurar sua descoberta de assinatura do RHSM.

Editar tags

Altere as tags associadas ao seu segredo de acesso.

Note

Se precisar fazer outras alterações em sua assinatura do RHSM, primeiro desative seu registro atual e, em seguida, configure um novo registro.

Desativar

Desative seu provedor registrado no RHSM.

Note

A desativação não afeta seu segredo de acesso ao Red Hat Subscription Manager (RHSM). Para evitar cobranças em sua AWS fatura por um segredo associado que você não precisa mais, consulte [Excluir um AWS Secrets Manager segredo](#) no Guia do AWS Secrets Manager usuário.

As configurações a seguir são exibidas no console do License Manager para descoberta do RHSM.

Configurações de descoberta do Red Hat Subscription Manager

Status da descoberta

Indica se você ativou a descoberta para assinaturas do RHSM.

Nome secreto

Links para o segredo de acesso do RHSM AWS Secrets Manager que contém seu token offline da Red Hat. O License Manager usa esse segredo para gerar um novo token de acesso temporário para solicitar dados de assinatura do Red Hat Subscription Manager (RHSM).

Você pode fazer alterações em um segredo existente por meio do Secrets Manager. Para atualizar tags ou outros metadados do seu segredo, consulte [Modificar um AWS Secrets Manager segredo](#) no Guia do AWS Secrets Manager usuário. Para atualizar o valor secreto, consulte [Atualizar o valor de um AWS Secrets Manager segredo](#).

Últimos dados sincronizados em

A data e hora da última atualização bem-sucedida dos dados de assinatura da conta registrada do Red Hat Subscription Manager (RHSM).

Tags

Você pode definir pares de valores-chave para tags que o License Manager atribui ao seu segredo de acesso RHSM no Secrets Manager. Para recuperar e descriptografar seu segredo de acesso ao RHSM, a política de função vinculada ao serviço do License Manager exige que o segredo, e qualquer associado AWS KMS key, tenha a seguinte tag atribuída:

```
"LicenseManagerLinuxSubscriptions": "enabled"
```

A tag é atribuída automaticamente se o License Manager criou seu segredo durante o processo de registro. Se você criar seu próprio segredo para o token offline, certifique-se de atribuir essa tag ao segredo e à chave KMS associada, se ela estiver criptografada. Para adicionar a tag, consulte [Modificar um AWS Secrets Manager segredo](#) no Guia AWS Secrets Manager do usuário.

Conversão de tipo de licença

As configurações a seguir estão disponíveis dependendo de quais produtos você precisa para Conversão de tipo de licença.

AWS Managed Microsoft AD

O License Manager AWS Managed Microsoft AD precisa ser configurado para que você possa trabalhar com assinaturas baseadas no usuário. Para ter mais informações, consulte [Gerencie assinaturas baseadas no usuário no License Manager](#).

Virtual private cloud

O License Manager exige que sua VPC seja configurada, além da sua AWS Managed Microsoft AD, quando você usa assinaturas baseadas em usuário com o Microsoft Office. Para ter mais informações, consulte [Gerencie assinaturas baseadas no usuário no License Manager](#).

Administradores delegados

É possível registrar um administrador delegado para executar tarefas administrativas para licenças gerenciadas e assinaturas do Linux no License Manager. Para simplificar a administração,

recomendamos usar o console do License Manager para registrar um único administrador delegado para cada atributo do License Manager. Com essa abordagem, você terá um único administrador delegado na sua organização para o License Manager.

Usando os SDKs AWS CLI ou, você pode registrar diferentes contas de membros em sua organização como administrador delegado para cada recurso suportado do License Manager. Isso faz com que diferentes contas de membros em sua organização possam realizar tarefas administrativas para licenças gerenciadas e assinaturas Linux.

Important

Para usar os atributos de administração delegada no console do License Manager, você deve ter a mesma conta de membro registrada como administrador delegado para cada atributo do License Manager. Se você registrou mais de uma conta de membro como administrador delegado, primeiro você precisa cancelar o registro das contas de membros existentes e, em seguida, registrar a mesma conta para cada atributo do License Manager.

Antes de registrar um administrador delegado, você deve habilitar o acesso confiança com as organizações. Para obter mais informações, consulte [Convidar uma AWS conta para se juntar à sua organização](#) e [Habilitar acesso confiável com AWS Organizations](#).

A seguir estão os atributos para os quais você pode registrar um administrador delegado:

Licenças gerenciadas

É possível realizar tarefas administrativas, como compartilhar licenças autogerenciadas com outras contas-membro, realizar a descoberta de atributos entre contas e distribuir direitos gerenciados para outras contas-membro.

Assinaturas Linux

Você pode realizar tarefas administrativas, como visualizar e gerenciar assinaturas comerciais do Linux que você possui e administra Regiões da AWS e suas contas em AWS Organizations. Você também pode criar e gerenciar CloudWatch alarmes da Amazon para suas assinaturas Linux. Primeiro os dados devem ser descobertos e agregados antes de ficarem visíveis no console do License Manager e todos os alarmes poderem funcionar, caso estejam configurados.

⚠ Important

Depois de registrado, o administrador delegado tem visibilidade das instâncias do EC2 pertencentes às contas da organização.

Você pode registrar e cancelar o registro de administradores delegados usando o [AWS License Manager console](#), [a AWS CLI](#) ou [SDKs](#) da AWS .

Regiões com suporte aos administradores delegados

As seguintes regiões oferecem suporte aos administradores delegados do License Manager:

- Leste dos EUA (Ohio)
- Leste dos EUA (N. da Virgínia)
- Oeste dos EUA (N. da Califórnia)
- Oeste dos EUA (Oregon)
- Asia Pacific (Mumbai)
- Ásia-Pacífico (Seul)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Tóquio)
- Ásia-Pacífico (Hong Kong)
- Oriente Médio (Barém)
- Canadá (Central)
- Europa (Frankfurt)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Paris)
- Europa (Estocolmo)
- Europa (Milão)
- África (Cidade do Cabo)
- América do Sul (São Paulo)

Registro de um administrador delegado

Você pode registrar um administrador delegado usando o AWS CLI ou AWS Management Console.

Console

Para registrar um administrador delegado usando o AWS License Manager console, execute as seguintes etapas:

1. Faça login AWS como administrador da conta de gerenciamento.
2. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
3. Selecione Configurações no painel de navegação à esquerda.
4. Escolha a guia Administração delegada.
5. Selecione Registrar administrador delegado.
6. Insira a ID da conta-membro para se registrar como administrador delegado, confirme que deseja conceder ao License Manager as permissões necessárias e escolha Registrar.
7. Uma mensagem indica se a conta especificada foi registrada com sucesso como administrador delegado do License Manager.

AWS CLI

Para registrar um administrador delegado para licenças gerenciadas usando o AWS CLI, execute as seguintes etapas:

1. Na linha de comando, execute o seguinte AWS CLI comando:

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

2. Execute o comando a seguir para verificar se a conta-membro especificada foi registrada com êxito como o administrador delegado.

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

Para registrar um administrador delegado para assinaturas Linux usando o AWS CLI, execute as seguintes etapas:

1. Na linha de comando, execute o seguinte AWS CLI comando:

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

2. Execute o comando a seguir para verificar se a conta-membro especificada foi registrada com êxito como o administrador delegado.

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

Cancelar registro de um administrador delegado

Você pode cancelar o registro de um administrador delegado usando o ou. AWS CLI AWS Management Console

Console

Para cancelar o registro de um administrador delegado usando o AWS License Manager console, execute as seguintes etapas:

1. Faça login AWS como administrador da conta de gerenciamento.
2. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
3. Selecione Configurações no painel de navegação à esquerda.
4. Escolha a guia Administração delegada.
5. Escolha Remove.
6. Digite o texto **remove** para confirmar que quer remover o administrador delegado do License Manager e escolha Remove.
7. Uma mensagem indica se a conta especificada foi removida com sucesso como administrador delegado do License Manager.

AWS CLI

Para cancelar o registro de um administrador delegado para licenças gerenciadas usando o AWS CLI, execute as seguintes etapas:

1. Na linha de comando, execute o seguinte AWS CLI comando:

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

2. Execute o comando a seguir para verificar se a conta-membro especificada teve o registro cancelado com êxito como administrador delegado:

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

Para cancelar o registro de um administrador delegado para assinaturas Linux usando o AWS CLI, execute as seguintes etapas:

1. Na linha de comando, execute o seguinte AWS CLI comando:

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

2. Execute o comando a seguir para verificar se a conta-membro especificada teve o registro cancelado com êxito como administrador delegado:

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

É possível registrar novamente uma conta cujo registro foi cancelado a qualquer momento.

Painel na AWS License Manager

A seção Painel do console do License Manager fornece detalhes de uso para monitorar o consumo de licenças associado a cada licença autogerenciada, direitos de licença concedidos, usuários inscritos em assinaturas desse tipo e instâncias em execução. O painel também exibe alertas resultantes de violações de regras de licença.

Visão geral

A seção “Visão geral” fornece os seguintes detalhes sobre suas licenças.

Licenças concedidas

A quantidade total de licenças concedidas nesta conta, nesta Região.

Licenças autogerenciadas

A quantidade total de licenças autogerenciadas nesta conta, nesta Região.

Licenças emitidas pelo vendedor

A quantidade total de licenças emitidas pelo vendedor nesta conta, nesta Região.

Produtos

A seção “Produtos” fornece os seguintes detalhes para assinaturas com usuários.

Product name (Nome do produto)

O nome do produto da assinatura com usuários.

Usuários inscritos

A quantidade de usuários inscritos no produto.

Direitos de licença concedidas

A seção “Direitos de licença concedidas” fornece os seguintes detalhes.

Product name (Nome do produto)

O nome do produto da licença concedida.

Direito

O nome do direito.

Uso

A utilização do direito.

Licenças autogerenciadas

A seção “Licenças autogerenciadas” fornece os seguintes detalhes.

Nome da licença

O nome da licença autogerenciada.

Direito

O nome do direito.

Uso

A utilização do direito.

Uso da instância

A seção “Uso da instância” fornece os seguintes detalhes.

Contagem de instâncias em execução

A quantidade total de instâncias em execução nesta conta, nesta Região.

Contagem agregada de instâncias em execução

A quantidade total de instâncias em execução agregada de todas as suas contas AWS Organizations nessa região. Esse gráfico só é visível na Conta de gerenciamento e na Conta de administrador delegado.

Monitorar o AWS License Manager

Você pode monitorar o uso de licenças e assinaturas rastreadas em AWS License Manager usando o Amazon CloudWatch. O CloudWatch coleta dados brutos e os transforma em métricas legíveis quase em tempo real. É possível definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte [Monitorar o uso de licenças com o Amazon CloudWatch](#).

É possível capturar chamadas de API e eventos relacionados realizados pela sua conta da Conta da AWS ou em nome dela, usando o AWS CloudTrail. Eventos são capturados como arquivos de log e entregues a um bucket do Amazon S3 especificado. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte [Registrar em log chamadas de API do AWS License Manager usando o AWS CloudTrail](#).

Sumário

- [Monitorar o uso de licenças com o Amazon CloudWatch](#)
 - [Criação de alarmes para monitorar as métricas do License Manager](#)
- [Registrar em log chamadas de API do AWS License Manager usando o AWS CloudTrail](#)
 - [Informações sobre o License Manager no CloudTrail](#)
 - [Noções básicas sobre as entradas do arquivo de log do License Manager](#)

Monitorar o uso de licenças com o Amazon CloudWatch

É possível monitorar estatísticas métricas do License Manager usando o Amazon CloudWatch. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como o aplicativo web ou o serviço está se saindo. É possível definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Por exemplo, é possível observar a porcentagem de licenças usando a métrica `LicenseConfigurationUsagePercentage` e agir antes que os limites sejam excedidos. Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch](#).

O License Manager emite as seguintes métricas de hora em hora no namespace `AWSLicenseManager/licenseUsage`:

Métrica	Descrição
RunningInstancesCount	<p>O número total de instâncias em execução na conta atual agrupadas pelo nome da assinatura.</p> <p>Unidade: contagem</p> <p>Dimensões:</p> <p>SubscriptionName : o nome da assinatura.</p>
AggregateRunningInstancesCount	<p>O número total agregado de instâncias em execução de todas as suas contas do AWS Organizations na Região da AWS atual.</p> <p>Unidade: contagem</p> <p>Dimensões:</p> <p>SubscriptionName : o nome da assinatura.</p>
TotalLicenseConfigurationUsageCount	<p>O número total de uma configuração de licença que pode estar disponível.</p> <p>Unidade: contagem</p> <p>Dimensões:</p> <ul style="list-style-type: none"> LicenseConfigurationArn : a configuração da licença do nome do recurso da Amazon (ARN). LicenseConfigurationType : o tipo de configuração da licença.
LicenseConfigurationUsageCount	<p>O número total de licenças usadas dessa configuração.</p> <p>Unidade: contagem</p> <p>Dimensões:</p> <ul style="list-style-type: none"> LicenseConfigurationArn : a configuração da licença do ARN. LicenseConfigurationType : o tipo de configuração da licença.

Métrica	Descrição
LicenseConfigurationUsagePercentage	<p>As licenças usadas dessa configuração de licença expressas em porcentagem.</p> <p>Unidades: percentual</p> <p>Dimensões:</p> <ul style="list-style-type: none">• <code>LicenseConfigurationArn</code> : a configuração da licença do ARN.• <code>LicenseConfigurationType</code> : o tipo de configuração da licença.

Criação de alarmes para monitorar as métricas do License Manager

É possível criar um alarme do CloudWatch que envie uma mensagem do Amazon Simple Notification Service (Amazon SNS) quando o valor da métrica for alterado e gerar uma mudança no estado do alarme. Um alarme observa uma métrica ao longo de um período especificado por você e realiza ações com base no valor da métrica relativo a um determinado limite ao longo de vários períodos. Os alertas invocam ações apenas para alterações de estado mantidas. Os alarmes do CloudWatch não invocam ações simplesmente por estarem em um estado específico. O estado deve ter sido alterado e mantido por um número específico de períodos. Para obter mais informações, consulte [Uso de alarmes do CloudWatch](#).

Registrar em log chamadas de API do AWS License Manager usando o AWS CloudTrail

O AWS License Manager é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, por um perfil ou por um serviço da AWS no Systems Manager. O CloudTrail captura todas as chamadas de API ao Network Manager como eventos. Isso inclui as chamadas do console do License Manager e as chamadas de código para as operações de API do License Manager. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o License Manager. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita ao License Manager, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e outros detalhes.

Para saber mais sobre o CloudTrail, consulte o [Guia do usuário do AWS CloudTrail](#).

Informações sobre o License Manager no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre uma atividade no License Manager, ela é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS em Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte [Como visualizar eventos com o histórico de eventos do CloudTrail](#).

Para obter um registro de eventos em andamento na sua conta da AWS, incluindo eventos do License Manager, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços AWS para analisar mais ainda e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [Serviços e integrações compatíveis com o CloudTrail](#)
- [Configurar notificações do Amazon SNS para o CloudTrail](#)
- [Receber arquivos de log do CloudTrail de várias regiões](#) e [receber arquivos de log do CloudTrail de várias contas](#)

Todas as ações do License Manager são registradas pelo CloudTrail e estão documentadas na [Referência da API do License Manager](#). Por exemplo, as chamadas para as ações `CreateLicenseConfiguration`, `ListResourceInventory` e `DeleteLicenseConfiguration` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte o [Elemento userIdentity do CloudTrail](#).

Noções básicas sobre as entradas do arquivo de log do License Manager

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `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"
}
```

Segurança em AWS License Manager

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isso como a segurança da nuvem e a segurança na nuvem:

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam ao License Manager, consulte [AWS Services in Scope by Compliance Program AWS](#) .
- **Segurança na nuvem** — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e os regulamentos aplicáveis

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o License Manager. Mostra como configurar o License Manager para atender aos objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do License Manager.

Conteúdo

- [Proteção de dados no AWS License Manager](#)
- [Gerenciamento de identidade e acesso para o AWS License Manager](#)
- [Usando funções vinculadas a serviços para AWS License Manager](#)
- [AWS políticas gerenciadas para AWS License Manager](#)
- [Assinatura criptográfica de licenças](#)
- [Validação de conformidade para AWS License Manager](#)
- [Resiliência no AWS License Manager](#)
- [Segurança da infraestrutura no AWS License Manager](#)

- [AWS License Manager e VPC endpoints de interface \(AWS PrivateLink\)](#)

Proteção de dados no AWS License Manager

O [modelo de responsabilidade compartilhada](#) da AWS se aplica à proteção de dados no AWS License Manager. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as [Perguntas frequentes sobre privacidade de dados](#). Para mais informações sobre a proteção de dados na Europa, consulte o artigo [AWS Shared Responsibility Model and GDPR](#) no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as Conta da AWS credenciais da e configure as contas de usuário individuais com o AWS IAM Identity Center ou o AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA [multi-factor authentication]) com cada conta.
- Use SSL/TLS para se comunicar com os atributos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log das atividades da API e do usuário com o .AWS CloudTrail
- Use AWS as soluções de criptografia da , juntamente com todos os controles de segurança padrão dos Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comandos ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, consulte [Federal Information Processing Standard \(FIPS\) 140-2](#).

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso também é válido quando você trabalha com o License Manager ou outros Serviços da AWS usando o console, a API, a AWS CLI ou SDKs da AWS. Quaisquer dados inseridos

em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia em repouso

O License Manager armazena dados em um bucket do Amazon S3 na conta de gerenciamento. O bucket é configurado usando chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3).

Gerenciamento de identidade e acesso para o AWS License Manager

O AWS Identity and Access Management (IAM) é um serviço da AWS que ajuda a controlar o acesso aos atributos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) a usar os atributos da AWS. Com o IAM, é possível criar usuários e grupos na sua conta da AWS. Você controla as permissões que os usuários têm para executar tarefas usando atributos da AWS. Você pode usar o IAM sem custo adicional.

Por padrão, os usuários não têm permissões para usar os atributos e operações do License Manager. Para permitir que os usuários gerenciem atributos do License Manager, crie uma política do IAM que conceda permissões a eles de forma explícita.

Quando você anexa uma política a um usuário ou grupo de usuários, isso concede ou nega aos usuários permissão para realizar as tarefas especificadas nos atributos especificados. Para obter mais informações, consulte [Políticas e permissões](#) no Guia do usuário do IAM.

Criar usuários, grupos e perfis

Você pode criar usuários e grupos para sua Conta da AWS e, em seguida, atribuir a eles as permissões necessárias. Como prática recomendada, os usuários devem adquirir as permissões assumindo perfis do IAM. Para obter mais informações sobre como configurar usuários e grupos para a sua Conta da AWS, consulte [Começando com AWS License Manager](#).

Um [perfil do IAM](#) é uma identidade do IAM que você pode criar em sua conta que tem permissões específicas. Um perfil do IAM é semelhante a um usuário do IAM porque é uma identidade da AWS com políticas de permissão que determinam o que ela pode e não pode fazer na AWS. No entanto,

em vez de ser exclusivamente associada a uma pessoa, o propósito do perfil é ser assumido por qualquer pessoa que precisar dele. Além disso, um perfil não tem credenciais de longo prazo padrão associadas a ele, como senha ou chaves de acesso. Em vez disso, quando você assumir um perfil, ele fornecerá credenciais de segurança temporárias para sua sessão de perfil.

Estrutura da política do IAM

A política do IAM é um documento JSON que consiste em uma ou mais instruções. Cada instrução é estruturada da maneira a seguir.

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

Existem vários elementos que compõem uma instrução:

- **Effect:** o efeito pode ser Allow ou Deny. Por padrão, os usuários não têm permissão para usar atributos e operações de API. Portanto, todas as solicitações são negadas. Um allow (permitir) explícito substitui o padrão. Uma deny (negar) explícito substitui todas as permissões.
- **Action:** a ação é a operação de API específica para a qual você está concedendo ou negando permissão.
- **Resource:** o atributo afetado pela ação. Algumas operações de API do License Manager permitem que você inclua atributos específicos em sua política que podem ser criados ou modificados pela operação. Para especificar um atributo na instrução, você precisa usar o Nome do recurso da Amazon (ARN). Para obter mais informações, consulte [Ações definidas pelo AWS License Manager](#).
- **Condition:** condições são opcionais. Elas podem ser usadas para controlar quando a política está em vigor. Para obter mais informações, consulte [Uso de chaves de condição do AWS License Manager](#).

Criar políticas do IAM para o License Manager

Em uma instrução de política do IAM, você pode especificar qualquer operação de API de qualquer serviço que ofereça suporte ao IAM. O License Manager usa os seguintes prefixos com o nome da operação de API:

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

Por exemplo:

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

Para obter mais informações sobre as APIs do License Manager disponíveis, consulte as seguintes referências de API:

- [Referência de API do AWS License Manager](#)
- [Referência de API de assinaturas de usuários do AWS License Manager](#)
- [Referência de API de assinaturas do Linux do AWS License Manager](#)

Para especificar várias operações em uma única instrução, separe-as com vírgulas da seguinte maneira:

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

Você também pode especificar várias operações usando caracteres curinga. Por exemplo, você pode especificar todas as operações da API do License Manager cujo nome começa com a palavra `List` da seguinte maneira:

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

Para especificar todas as operações da API do License Manager, use o asterisco (*) conforme o seguinte:

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

Exemplo de política para um ISV que usa o License Manager

Os ISVs que distribuem licenças por meio do License Manager exigem as seguintes permissões:

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

Conceder permissões a usuários, grupos e perfis

Depois de criar as políticas do IAM necessárias, você precisa conceder essas permissões aos seus usuários, grupos e perfis.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

Crie um conjunto de permissões. Siga as instruções em [Create a permission set](#) (Criação de um conjunto de permissões) no Guia do usuário do AWS IAM Identity Center.

- Usuários gerenciados no IAM usando um provedor de identidades:

Crie um perfil para a federação de identidades. Siga as instruções em [Criar um perfil para um provedor de identidades de terceiros \(federação\)](#) no Guia do usuário do IAM.

- Usuários do IAM:

- Crie um perfil que seu usuário possa assumir. Siga as instruções em [Creating a role for an IAM user](#) (Criação de um perfil para um usuário do IAM) no Guia do usuário do IAM.
- (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em [Adição de permissões a um usuário \(console\)](#) no Guia do usuário do IAM.

Usando funções vinculadas a serviços para AWS License Manager

AWS License Manager usa funções [vinculadas ao serviço AWS Identity and Access Management](#) (IAM). Um perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao License Manager. As funções vinculadas ao serviço são predefinidas pelo License Manager e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Um perfil vinculado ao serviço facilita a configuração do License Manager porque você não precisa adicionar as permissões necessárias manualmente. O License Manager define as permissões dos perfis vinculados ao serviço e, exceto se definido de outra forma, somente o License Manager pode assumir os perfis. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Você pode excluir um perfil vinculado ao serviço somente depois de excluir os atributos relacionados. Isso protege os atributos do License Manager, pois você não pode remover por engano as permissões para acessar os atributos.

As ações do License Manager dependem de três perfis vinculados ao serviço, conforme descritos nas seções a seguir.

Funções vinculadas a serviço

- [License Manager: perfil principal](#)
- [License Manager: perfil da conta de gerenciamento](#)
- [License Manager: perfil da conta-membro](#)
- [License Manager: perfil de assinatura baseado no usuário](#)

- [License Manager: perfil de assinaturas Linux](#)

License Manager: perfil principal

O License Manager requer um perfil vinculado ao serviço para gerenciar licenças em seu nome.

Permissões do principal perfil

A função vinculada ao serviço chamada `AWSServiceRoleForAWSLicenseManagerRole` permite que o License Manager acesse AWS recursos para gerenciar licenças em seu nome.

A função vinculada ao serviço `AWSServiceRoleForAWSLicenseManagerRole` confia no serviço `license-manager.amazonaws.com` para presumir a função.

Para revisar as permissões do `AWSLicenseManagerServiceRolePolicy`, consulte [AWS política gerenciada: AWSLicenseManagerServiceRolePolicy](#). Para saber mais sobre como configurar permissões para um perfil vinculado ao serviço, consulte [Permissões do perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Criar um perfil vinculado ao serviço para o License Manager

Não é necessário criar manualmente um perfil vinculado ao serviço. Ao concluir o formulário de experiência de primeira execução do License Manager na primeira vez que acessar o console do License Manager, o perfil vinculado ao serviço será criada automaticamente.

Você também pode usar o console do IAM ou a API do IAM para criar manualmente uma função vinculada ao serviço. AWS CLI Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Important

Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Se você usava o License Manager antes de 1º de janeiro de 2017, quando começou a ser oferecido suporte aos perfis vinculados ao serviço, o License Manager criou o perfil `AWSServiceRoleForAWSLicenseManagerRole` em sua conta. Para obter mais informações, consulte [Uma novo perfil apareceu na minha conta do IAM](#).

Você pode usar o console do License Manager para criar um perfil vinculado ao serviço.

Para criar o perfil vinculado ao serviço

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Escolha Começar a usar o License Manager.
3. No formulário Permissões do IAM (one-time-setup), selecione Eu AWS License Manager concedo as permissões necessárias e escolha Continuar.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso do License Manager. Como alternativa, na AWS CLI ou na AWS API, use o IAM para criar uma função vinculada ao serviço com o nome do `license-manager.amazonaws.com` serviço. Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Se excluir esse perfil vinculado ao serviço, será possível usar o mesmo processo do IAM para criar o perfil novamente.

Editar um perfil vinculado ao serviço para o License Manager

O License Manager não permite que você edite o perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerRole`. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ela. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o License Manager

Se você não precisar mais usar um atributo ou serviço que exija uma função vinculada a um serviço, recomendamos que você exclua essa função. Dessa forma, você ficará somente com entidades que sejam monitoradas ou mantidas ativamente. No entanto, você deve limpar seu perfil vinculado ao serviço para excluí-la manualmente.

Limpar um perfil vinculado ao serviço

Antes de usar o IAM para excluir um perfil vinculado ao serviço, você deverá excluir todos os atributos usados pelo perfil. Isso significa desassociar todas as licenças autogerenciadas das instâncias e AMIs associadas e então excluir as licenças autogerenciadas.

Note

Se o License Manager estiver usando o perfil quando você tentar excluir os atributos, a exclusão poderá falhar. Se isso acontecer, aguarde alguns minutos e tente a ação novamente.

Para excluir atributos do License Manager usados pelo perfil vinculado ao serviço

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação, escolha Licenças autogerenciadas.
3. Escolha uma licença autogerenciada da qual você seja o proprietário e desassocie todas as entradas nas guias AMIs associadas e atributos. Repita este processo para cada configuração de licença.
4. Ainda na página de licenças autogerenciadas, escolha Ações e, em seguida, selecione Excluir.
5. Repita as etapas anteriores até que todas as licenças autogerenciadas tenham sido excluídas.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSServiceRoleForAWSLicenseManagerRole` vinculada ao serviço. Se você também estiver usando [AWSServiceRoleForAWSLicenseManagerMasterAccountRole](#) e [AWSLicenseManagerMemberAccountRole](#), exclua essas funções primeiro. Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

License Manager: perfil da conta de gerenciamento

O License Manager requer um perfil vinculado ao serviço para realizar o gerenciamento de licenças.

Permissões para o perfil da conta de gerenciamento

A função vinculada ao serviço chamada

`AWSServiceRoleForAWSLicenseManagerMasterAccountRole` permite que o License Manager acesse AWS recursos para gerenciar ações de gerenciamento de licenças para uma conta de gerenciamento central em seu nome.

A função vinculada ao serviço `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` confia no serviço `license-manager.master-account.amazonaws.com` para presumir a função.

Para revisar as permissões do `AWSLicenseManagerMasterAccountRolePolicy`, consulte [AWS política gerenciada: AWSLicenseManagerMasterAccountRolePolicy](#). Para saber mais sobre como configurar permissões para um perfil vinculado ao serviço, consulte [Permissões do perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Criar um perfil vinculado ao serviço para a conta de gerenciamento

Você não precisa criar manualmente esse perfil vinculado ao serviço. Quando você configura o gerenciamento de licenças entre contas no AWS Management Console, o License Manager cria a função vinculada ao serviço para você.

Note

Para usar o suporte entre contas no License Manager, você deve estar usando AWS Organizations.

Se você excluir esse perfil vinculado ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar o perfil em sua conta.

Você também pode usar o console do IAM ou a API do IAM para criar manualmente uma função vinculada ao serviço. AWS CLI Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Important

Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Se você usava o License Manager antes de 1º de janeiro de 2017, quando começou a ser oferecido suporte aos perfis vinculados ao serviço, o License Manager criou o `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` em sua conta. Para obter mais informações, consulte [Uma novo perfil apareceu na minha conta do IAM](#).

Você pode usar o console do License Manager para criar esse perfil vinculado ao serviço.

Para criar o perfil vinculado ao serviço

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. Escolha Configurações, Editar.
3. Escolha Vincular AWS Organizations contas.
4. Escolha Aplicar.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso de conta de gerenciamento do License Manager. Como alternativa, na AWS CLI ou na AWS API, use o IAM para criar uma função vinculada ao serviço com o nome de `license-manager.master-account.amazonaws.com` serviço. Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Se excluir esse perfil vinculado ao serviço, será possível usar o mesmo processo do IAM para criar o perfil novamente.

Editar um perfil vinculado ao serviço para o License Manager

O License Manager não permite editar o perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerMasterAccountRole`. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o License Manager

Se você não precisar mais usar um atributo ou serviço que exija uma função vinculada a um serviço, recomendamos que você exclua essa função. Dessa forma, você ficará somente com entidades que sejam monitoradas ou mantidas ativamente. No entanto, você deve limpar seu perfil vinculado ao serviço para excluí-la manualmente.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM ou AWS CLI a AWS API para excluir a função `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` vinculada ao serviço. Para mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

License Manager: perfil da conta-membro

O License Manager requer um perfil vinculado ao serviço que permita o gerenciamento de contas para gerenciar licenças.

Permissões para o perfil da conta-membro

A função vinculada ao serviço chamada

`AWSServiceRoleForAWSLicenseManagerMemberAccountRole` permite que o License Manager acesse AWS recursos para ações de gerenciamento de licenças a partir de uma conta de gerenciamento configurada em seu nome.

A função vinculada ao serviço `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` confia no serviço `license-manager.member-account.amazonaws.com` para presumir a função.

Para revisar as permissões do `AWSLicenseManagerMemberAccountRolePolicy`, consulte [AWS política gerenciada: AWSLicenseManagerMemberAccountRolePolicy](#). Para saber mais sobre como configurar permissões para um perfil vinculado ao serviço, consulte [Permissões do perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Criar o perfil vinculado ao serviço para o License Manager

Você não precisa criar manualmente o perfil vinculado ao serviço. Você pode ativar a integração com AWS Organizations a conta de gerenciamento no console do License Manager na página Configurações. Você também pode fazer isso usando a AWS CLI (executar `update-service-settings`) ou a AWS API (chamada `UpdateServiceSettings`). Ao fazer isso, o License Manager cria o perfil vinculado ao serviço para você nas contas-membro do Organizations.

Se você excluir esse perfil vinculado ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar o perfil em sua conta.

Você também pode usar o console do IAM ou AWS CLI a AWS API para criar manualmente uma função vinculada ao serviço. Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Important

Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Se você

usava o serviço do License Manager antes de 1º de janeiro de 2017, quando começou a ser oferecido suporte aos perfis vinculados ao serviço, o License Manager criou o perfil `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` em sua conta. Para obter mais informações, consulte [Uma novo perfil apareceu na minha conta do IAM](#).

Você pode usar o console do License Manager para criar um perfil vinculado ao serviço.

Para criar o perfil vinculado ao serviço

1. Faça login na sua conta AWS Organizations de gerenciamento.
2. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
3. Na barra de navegação à esquerda, escolha Configurações e, em seguida, escolha Básico.
4. Escolha Vincular AWS Organizations contas.
5. Selecione Apply (Aplicar). Isso cria as funções [AWSServiceRoleForAWSLicenseManagerRole](#) e [AWSServiceRoleForAWSLicenseManagerMemberAccountRole](#) em todas as contas infantis.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso License Manager - Member account. Como alternativa, na AWS CLI ou, crie uma função vinculada ao serviço com o nome de `license-manager.member-account.amazonaws.com` serviço. Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Se excluir esse perfil vinculado ao serviço, será possível usar o mesmo processo do IAM para criar o perfil novamente.

Editar um perfil vinculado ao serviço para o License Manager

O License Manager não permite editar o perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerMemberAccountRole`. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o License Manager

Se você não precisar mais usar um atributo ou serviço que exija uma função vinculada a um serviço, recomendamos que você exclua essa função. Dessa forma, você ficará somente com entidades que

sejam monitoradas ou mantidas ativamente. No entanto, você deve limpar seu perfil vinculado ao serviço para excluí-la manualmente.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM ou AWS CLI a AWS API para excluir a função `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` vinculada ao serviço. Para mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

License Manager: perfil de assinatura baseado no usuário

O License Manager exige uma função vinculada ao serviço para gerenciar AWS recursos que fornecerão assinaturas baseadas no usuário.

Permissões para o perfil de assinatura baseada no usuário

A função vinculada ao serviço chamada

`AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` permite que o License Manager utilize AWS Systems Manager e gerencie recursos do Amazon EC2 fornecendo assinaturas baseadas no usuário, bem como descreva recursos. AWS Directory Service

Para revisar as permissões do `AWSLicenseManagerUserSubscriptionsServiceRolePolicy`, consulte [AWS política gerenciada: AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#).

Para saber mais sobre como configurar permissões para um perfil vinculado ao serviço, consulte [Permissões do perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Criar o perfil vinculado ao serviço para o License Manager

Você não precisa criar manualmente o perfil vinculado ao serviço, pois você será solicitado nas páginas de assinaturas baseadas no usuário do console do License Manager para criar o perfil.

Se você excluir esse perfil vinculado ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar o perfil em sua conta.

Você também pode usar o console do IAM ou a API do IAM para criar manualmente uma função vinculada ao serviço. AWS CLI Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Você pode usar o console do License Manager para criar um perfil vinculado ao serviço.

Para criar o perfil vinculado ao serviço

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.
2. No painel de navegação à esquerda, escolha Associação de usuário ou Produtos.
3. Concorde com os termos do License Manager para criar o perfil de assinatura baseada no usuário.
4. Escolha Criar. Isso cria o perfil.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso License Manager - User-based subscriptions. Como alternativa, na AWS API AWS CLI ou, crie uma função vinculada ao serviço com o nome do `license-manager-user-subscriptions.amazonaws.com` serviço. Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Se excluir esse perfil vinculado ao serviço, será possível usar o mesmo processo do IAM para criar o perfil novamente.

Editar um perfil vinculado ao serviço para o License Manager

O License Manager não permite editar o perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService`. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o License Manager

Se você não precisar mais usar um atributo ou serviço que exija uma função vinculada a um serviço, recomendamos que você exclua essa função. Dessa forma, você ficará somente com entidades que sejam monitoradas ou mantidas ativamente. No entanto, você deve limpar seu perfil vinculado ao serviço para excluí-la manualmente.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM ou AWS CLI a AWS API para excluir a função `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` vinculada ao serviço. Para mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

License Manager: perfil de assinaturas Linux

O License Manager exige uma função vinculada ao serviço para gerenciar AWS recursos que fornecem assinaturas Linux.

Permissões para o perfil de assinaturas Linux

A função vinculada ao serviço chamada

`AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` permite que o License Manager execute as seguintes ações para assinaturas Linux.

- Conheça a Amazon Elastic Compute Cloud e AWS Organizations os recursos.
- Recupere segredos marcados com "LicenseManagerLinuxSubscriptions": "enabled" de AWS Secrets Manager para acessar provedores de assinatura Linux terceirizados para obter informações de assinatura.
- Use as chaves KMS marcadas com "LicenseManagerLinuxSubscriptions": "enabled" para descriptografar segredos.

Para revisar as permissões do `AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`, consulte [AWS política gerenciada: AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#).

Para saber mais sobre como configurar permissões para um perfil vinculado ao serviço, consulte [Permissões do perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Criar o perfil vinculado ao serviço para o License Manager

Você não precisa criar manualmente o perfil vinculado ao serviço, pois você será solicitado nas páginas de assinaturas Linux do console do License Manager para criar o perfil.

Se você excluir esse perfil vinculado ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar o perfil em sua conta.

Você também pode usar o console do IAM ou a API do IAM para criar manualmente uma função vinculada ao serviço. AWS CLI Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Você pode usar o console do License Manager para criar um perfil vinculado ao serviço.

Para criar o perfil vinculado ao serviço

1. Abra o console do License Manager em <https://console.aws.amazon.com/license-manager/>.

2. No painel de navegação à esquerda, escolha Assinaturas ou Instâncias.
3. Concorde com os termos do License Manager para criar o perfil de assinaturas Linux.
4. Escolha Criar. Isso cria o perfil.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso `License Manager - Linux subscriptions`. Como alternativa, na AWS API AWS CLI ou, crie uma função vinculada ao serviço com o nome do `license-manager-linux-subscriptions.amazonaws.com` serviço. Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Se excluir esse perfil vinculado ao serviço, será possível usar o mesmo processo do IAM para criar o perfil novamente.

Editar um perfil vinculado ao serviço para o License Manager

O License Manager não permite editar o perfil vinculado ao serviço `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o License Manager

Se você não precisar mais usar um atributo ou serviço que exija uma função vinculada a um serviço, recomendamos que você exclua essa função. Dessa forma, você ficará somente com entidades que sejam monitoradas ou mantidas ativamente. No entanto, você deve limpar seu perfil vinculado ao serviço para excluí-la manualmente.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM ou AWS CLI a AWS API para excluir a função `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` vinculada ao serviço. Para mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

AWS políticas gerenciadas para AWS License Manager

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para [criar políticas](#)

[gerenciadas pelo cliente do IAM](#) que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis em sua AWS conta. Para obter mais informações sobre políticas AWS gerenciadas, consulte [políticas AWS gerenciadas](#) no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política `ReadOnlyAccess` AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do usuário do IAM.

AWS política gerenciada: `AWSLicenseManagerServiceRolePolicy`

Esta política é anexada à perfil vinculado ao serviço com nome de `AWSServiceRoleForAWSLicenseManagerRole` para permitir que o License Manager chame ações da API para gerenciar licenças para você. Para obter mais informações sobre a função vinculada ao serviço, consulte [Permissões do principal perfil](#).

A política de permissões do perfil permite que o License Manager execute as ações a seguir nos atributos especificados.

Ação	Atributo ARN
<code>iam:CreateServiceLinkedRole</code>	<code>arn:aws:iam::*:role/aws-service-role/license-management.marketplace.amazonaws.com</code>

Ação	Atributo ARN
	/AWSServiceRoleForMarketplaceLicenseManagement
iam:CreateServiceLinkedRole	arn:aws:iam::*:role/aws-service-role/license-manager.member-account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:ListAllMyBuckets	*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
sns:Publish	arn:aws::sns::*:aws-license-manager-service-*
sns:ListTopics	*
ec2:DescribeInstances	*
ec2:DescribeImages	*
ec2:DescribeHosts	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*

Ação	Atributo ARN
<code>ssm:CreateAssociation</code>	*
<code>organizations:ListAWSServiceAccessForOrganization</code>	*
<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 as permissões dessa política no AWS Management Console, consulte [AWSLicenseManagerServiceRolePolicy](#).

AWS política gerenciada: AWSLicenseManagerMasterAccountRolePolicy

Essa política é anexada à função vinculada ao serviço nomeada `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` para permitir que o License Manager chame ações de API que realizam o gerenciamento de licenças para uma conta de gerenciamento central em seu nome. Para obter mais informações sobre a função vinculada ao serviço, consulte [License Manager: perfil da conta de gerenciamento](#).

A política de permissões do perfil permite que o License Manager execute as ações a seguir nos atributos especificados.

Ação	Atributo ARN
<code>s3:GetBucketLocation</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>

Ação	Atributo ARN
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:GetLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*
s3:PutLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*
s3:GetBucketPolicy	arn:aws:s3:::aws-license-manager-service-*
s3:PutBucketPolicy	arn:aws:s3:::aws-license-manager-service-*
s3:AbortMultipartUpload	arn:aws:s3:::aws-license-manager-service-*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
s3:GetObject	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucketMultipartUploads	arn:aws:s3:::aws-license-manager-service-*
s3:ListMultipartUploadParts	arn:aws:s3:::aws-license-manager-service-*
s3>DeleteObject	arn:aws:s3:::aws-license-manager-service-*/re-source-sync/*
athena:GetQueryExecution	*
athena:GetQueryResults	*

Ação	Atributo ARN
<code>athena:StartQueryExecution</code>	*
<code>glue:GetTable</code>	*
<code>glue:GetPartition</code>	*
<code>glue:GetPartitions</code>	*
<code>glue:CreateTable</code>	Consulte a nota de rodapé ¹
<code>glue:UpdateTable</code>	Consulte a nota de rodapé ¹
<code>glue>DeleteTable</code>	Consulte a nota de rodapé ¹
<code>glue:UpdateJob</code>	Consulte a nota de rodapé ¹
<code>glue:UpdateCrawler</code>	Consulte a nota de rodapé 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>	*

Ação	Atributo ARN
<code>ram:CreateResourceShare</code>	*
<code>ram:AssociateResourceShare</code>	*
<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>

Ação	Atributo ARN
<code>cloudformation:DescribeStacks</code>	<code>arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*</code>

¹ A seguir estão os recursos definidos para as AWS Glue ações:

- `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 as permissões dessa política no AWS Management Console, consulte [AWSLicenseManagerMasterAccountRolePolicy](#).

AWS política gerenciada: AWSLicenseManagerMemberAccountRolePolicy

Esta política é anexada à perfil vinculado ao serviço com nome de `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` para permitir que o License Manager chame ações de API para gerenciar licenças de uma conta de gerenciamento para você. Para ter mais informações, consulte [License Manager: perfil da conta-membro](#).

A política de permissões do perfil permite que o License Manager execute as ações a seguir nos atributos especificados.

Ação	Atributo ARN
<code>license-manager:UpdateLicenseSpecificationsForResource</code>	*

Ação	Atributo ARN
<code>license-manager:GetLicenseConfiguration</code>	*
<code>ssm:ListInventoryEntries</code>	*
<code>ssm:GetInventory</code>	*
<code>ssm:CreateAssociation</code>	*
<code>ssm:CreateResourceDataSync</code>	*
<code>ssm>DeleteResourceDataSync</code>	*
<code>ssm:ListResourceDataSync</code>	*
<code>ssm:ListAssociations</code>	*
<code>ram:AcceptResourceShareInvitation</code>	*
<code>ram:GetResourceShareInvitations</code>	*

Para ver as permissões dessa política no AWS Management Console, consulte [AWSLicenseManagerMemberAccountRolePolicy](#).

AWS política gerenciada: AWSLicenseManagerConsumptionPolicy

É possível anexar a política `AWSLicenseManagerConsumptionPolicy` a suas identidades do IAM. Essa política concede permissões que permitem acesso às ações da API do License Manager necessárias para consumir licenças. Para ter mais informações, consulte [Uso da licença](#).

Para visualizar as permissões para esta política, consulte [AWSLicenseManagerConsumptionPolicy](#) no AWS Management Console.

AWS política gerenciada:

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Esta política é anexada ao perfil vinculado ao serviço com nome de política da `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` para permitir que o

License Manager chama ações de API para gerenciar atributos de licenças baseadas no usuário. Para ter mais informações, consulte [License Manager: perfil de assinatura baseado no usuário](#).

A política de permissões do perfil permite que o License Manager execute as ações a seguir nos atributos especificados.

Ação	Atributo ARN
<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 O License Manager só pode criar tags e encerrar instâncias que tenham os códigos de produto [bz0vcy31ooqlzk5tsash4r1ik](#), [77yzkpa7kvee1y1tt7wnsdwoc](#) ou [d44g89hc0gp9jdzm99rznthpw](#).

² O License Manager só pode executar um comando SSM Run com o documento do AWS-RunPowerShellScript em instâncias com o nome da tag `AWSLicenseManager` e um valor de `UserSubscriptions`.

Para ver as permissões dessa política no AWS Management Console, consulte [AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#).

AWS política gerenciada:

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Esta política é anexada à perfil vinculado ao serviço com nome de política da `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` para permitir que o License Manager chame ações da API para gerenciar atributos de licenças Linux. Para ter mais informações, consulte [License Manager: perfil de assinaturas Linux](#).

A política de permissões do perfil permite que o License Manager execute as ações a seguir nos atributos especificados.

Ação	Condições	Recurso
<code>ec2:DescribeInstances</code>	N/D	*
<code>ec2:DescribeRegions</code>	N/D	*
<code>organizations:DescribeOrganization</code>	N/D	*
<code>organizations:ListAccounts</code>	N/D	*
<code>organizations:DescribeAccount</code>	N/D	*
<code>organizations:ListChildren</code>	N/D	*
<code>organizations:ListParents</code>	N/D	*
<code>organizations:ListAccountsForParent</code>	N/D	*
<code>organizations:ListRoots</code>	N/D	*

Ação	Condições	Recurso
<code>organizations:ListAWSServiceAccessForOrganization</code>	N/D	*
<code>organizations:ListDelegatedAdministrators</code>	N/D	*
<code>gerente de segredos: GetSecret Value</code>	StringEquals: “aws:ResourceTag/LicenseManagerLinuxSubscriptions”: “ativado” “aws:ResourceAccount “: “\${aws:PrincipalAccount}”	<code>arn:aws:secretsmanager:*:*:secret:*</code>
<code>kms:Decrypt</code>	StringEquals: “aws:ResourceTag/LicenseManagerLinuxSubscriptions”: “ativado”, “aws:ResourceAccount “: “\${aws:PrincipalAccount}” StringLike: “kms: “[ViaService“secret smanager.*.amazonaws.com”]	<code>arn:aws:kms:*:*:key/*</code>

Para ver as permissões dessa política no AWS Management Console, consulte [AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#).

Atualizações do License Manager para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do License Manager desde que esse serviço começou a rastrear essas alterações.

Alteração	Descrição	Data
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy : atualizar para uma política existente	<p>O License Manager adicionou permissões para armazenar e recuperar segredos e usar AWS KMS chaves para descriptografar segredos de AWS Secrets Manager token de acesso para assinatura as Bring Your Own License (BYOL).</p>	<p>22 de maio de 2024</p>
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy – Nova política	<p>O License Manager adicionou uma permissão para criar o perfil vinculado ao serviço chamado de <code>AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService</code>. Essa função fornece ao License Manager permissão para listar AWS Organizations recursos do Amazon EC2.</p>	<p>21 de dezembro de 2022</p>
AWSLicenseManagerUserSubscriptionsServiceRolePolicy : atualizar para uma política existente	<p>O License Manager adicionou a permissão do <code>ec2:DescribeVpcPeeringConnections</code>.</p>	<p>28 de novembro de 2022</p>
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – Nova política	<p>O License Manager adicionou uma permissão para criar o perfil vinculado ao serviço chamado de <code>AWSLicenseManagerUserSubscriptionsServiceRolePolicy</code>. Essa função fornece ao License Manager</p>	<p>18 de julho de 2022</p>

Alteração	Descrição	Data
	<p>permissão para listar AWS Directory Service recursos, utilizar recursos do Systems Manager e gerenciar recursos do Amazon EC2 criados para assinaturas baseadas em usuários.</p>	
<p>AWSLicenseManagerMasterAccountRolePolicy: atualizar para uma política existente</p>	<p>O License Manager adicionou a <code>resource-groups:PutGroupPolicy</code> permissão para grupos de recursos gerenciados por AWS Resource Access Manager.</p>	<p>27 de junho de 2022</p>
<p>AWSLicenseManagerMasterAccountRolePolicy: atualizar para uma política existente</p>	<p>O License Manager alterou a chave de AWSLicenseManagerMasterAccountRolePolicy condição da política AWS AWS Resource Access Manager gerenciada de usar <code>ram:ResourceTag</code> para <code>aws:ResourceTag</code>.</p>	<p>16 de novembro de 2021</p>
<p>AWSLicenseManagerConsumptionPolicy – Nova política</p>	<p>O License Manager adicionou uma nova política que concede permissões para consumir licenças.</p>	<p>11 de agosto de 2021</p>

Alteração	Descrição	Data
<p>AWSLicenseManagerServiceRolePolicy: atualizar para uma política existente</p>	<p>O License Manager adicionou uma permissão para listar administradores delegados e uma permissão para criar o perfil vinculado ao serviço chamado <code>AWSServiceRoleForAWSLicenseManagerMemberAccountRole</code>.</p>	<p>16 de junho de 2021</p>
<p>AWSLicenseManagerServiceRolePolicy: atualizar para uma política existente</p>	<p>O License Manager adicionou uma permissão para listar todos os atributos do License Manager, como configurações de licenças, licenças e concessões.</p>	<p>15 de junho de 2021</p>
<p>AWSLicenseManagerServiceRolePolicy: atualizar para uma política existente</p>	<p>O License Manager adicionou uma permissão para criar o perfil vinculado ao serviço chamado de <code>AWSServiceRoleForMarketplaceLicenseManagement</code>. Essa função AWS Marketplace fornece permissões para criar e gerenciar licenças no License Manager. Para obter mais informações, consulte perfis vinculados ao serviço para o AWS Marketplace no Guia do comprador do AWS Marketplace.</p>	<p>9 de março de 2021</p>

Alteração	Descrição	Data
O License Manager começou a rastrear as alterações	O License Manager começou a monitorar as alterações em suas políticas AWS gerenciadas.	9 de março de 2021

Assinatura criptográfica de licenças

O License Manager pode assinar criptograficamente licenças emitidas por um ISV ou AWS Marketplace em nome de um ISV. A assinatura permite que os fornecedores validem a integridade e a origem de uma licença dentro do próprio aplicativo, mesmo em um ambiente offline.

Para assinar licenças, o License Manager usa uma assimétrica AWS KMS key pertencente a um ISV e protegida em (). AWS Key Management Service AWS KMS Essa CMK gerenciada pelo cliente consiste em um par de chave pública e chave privada relacionadas matematicamente. Quando um usuário solicita uma licença, o License Manager gera um objeto JSON listando os direitos da licença e assina o objeto com a chave privada. A assinatura e o objeto JSON de texto simples são retornados ao usuário. Qualquer pessoa apresentada com esses objetos pode usar a chave pública para validar se o texto da licença não foi alterado e se a licença foi assinada pelo proprietário da chave privada. A parte privada do par de chaves nunca sai AWS KMS. Para obter mais informações sobre criptografia assimétrica em AWS KMS, consulte [Usando chaves simétricas e assimétricas](#).

Note

O License Manager chama as operações AWS KMS [Signe](#) a [Verify](#)API ao assinar e verificar licenças. A CMK deve ter um valor de uso de chave de [SIGN_VERIFY](#) para ser usada por essas operações. Essa variedade de CMK não pode ser usada para criptografia e descriptografia.

O fluxo de trabalho a seguir descreve a emissão de licenças assinadas criptograficamente:

1. No AWS KMS console, na API ou no SDK, o administrador da licença cria uma CMK assimétrica gerenciada pelo cliente. A CMK deve usar um sinal para a chave, verificar e dar suporte ao algoritmo de assinatura RSASSA-PSS SHA-256. Para obter mais informações, consulte [Criar CMKs assimétricas](#) e [Como escolher a configuração de CMK](#).

2. No License Manager, o administrador da licença cria uma configuração de consumo que inclui um AWS KMS ARN ou ID. A configuração pode especificar uma ou ambas as opções de Empréstimo e provisória. Para obter mais informações, consulte [Criar um bloco de licenças emitidas pelo vendedor](#).
3. Um usuário final obtém a licença usando a operação de API [CheckoutLicense](#) ou [CheckoutBorrowLicense](#). A operação CheckoutBorrowLicense é permitida somente em licenças com o Borrow configurado. Ela retorna uma assinatura digital como parte de sua resposta junto com o objeto JSON listando os direitos. O texto simples do JSON é semelhante ao seguinte:

```
{
  "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"
  }
}
```


Validação de conformidade para AWS License Manager

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte [Serviços da AWS Escopo por Programa de Conformidade](#) [Serviços da AWS](#) e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#) .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Guias de início rápido sobre segurança e conformidade](#) — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- [Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services](#) — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

 Note

Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a [Referência dos serviços qualificados pela HIPAA](#).

- AWS Recursos de <https://aws.amazon.com/compliance/resources/> de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- [AWS Guias de conformidade do cliente](#) — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#) — Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a [Referência de controles do Security Hub](#).
- [Amazon GuardDuty](#) — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.

- [AWS Audit Manager](#)— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no AWS License Manager

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte [Infraestrutura global da AWS](#).

Segurança da infraestrutura no AWS License Manager

Por ser um serviço gerenciado, o AWS License Manager é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte [Segurança na Nuvem AWS](#). Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte [Proteção de infraestrutura](#) em Pilar segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar o License Manager por meio da rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

AWS License Manager e VPC endpoints de interface (AWS PrivateLink)

Você pode estabelecer uma conexão privada entre a nuvem privada virtual (VPC) e o AWS License Manager criando um endpoint da VPC de interface. Os endpoints de interface são habilitados por [AWS PrivateLink](#), uma tecnologia que você pode usar para acessar de forma privada a API do License Manager sem um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. As instâncias na VPC não precisam de endereços IP públicos para a comunicação com o License Manager. O tráfego entre sua VPC e o License Manager não deixa a rede da Amazon.

Cada endpoint de interface é representado por uma ou mais [interfaces de rede elástica](#) nas sub-redes.

Para obter mais informações, consulte [Endpoints da interface da VPC\(AWS PrivateLink\)](#) no Manual do usuário do Amazon VPC.

Criar um endpoint da VPC de interface para o License Manager

Crie um endpoint de interface para o License Manager usando um dos seguintes nomes de serviço:

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

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API para o License Manager usando seu nome DNS padrão para a região. Por exemplo, `license-manager.region.amazonaws.com`.

Para obter mais informações, consulte [Criar um endpoint de interface](#) no Guia do usuário da Amazon VPC.

Criar uma política de endpoint da VPC para o License Manager

É possível anexar uma política ao endpoint da VPC para controlar o acesso ao License Manager. Essa política especifica as seguintes informações:

- A entidade principal que pode executar ações
- As ações que podem ser executadas

- O atributo no qual as ações podem ser executadas

Veja a seguir um exemplo de uma política de endpoint para o License Manager. Quando anexada a um endpoint, essa política concede acesso às ações indicadas do License Manager para todas as entidades principais em todos os atributos.

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

Para obter mais informações, consulte [Controlar o acesso a serviços com endpoints da VPC](#) no Guia do usuário da Amazon VPC.

Solução de problemas AWS License Manager

As informações a seguir podem ajudar você a solucionar problemas ao usar o AWS License Manager. Antes de começar, confirme se a configuração do License Manager atende aos requisitos estabelecidos em [Configurações em AWS License Manager](#).

Erro de descoberta entre contas

Enquanto configura a descoberta entre contas, você pode encontrar a seguinte mensagem de erro na página Pesquisar inventário:

Exceção do Athena: falha na consulta do Athena devido a permissões insuficientes para executar a consulta. Migre seu catálogo para habilitar o acesso a esse banco de dados.

Isso pode ocorrer quando o serviço do Athena usa o catálogo de dados gerenciado pelo Athena, em vez do AWS Glue Data Catalog. Para obter instruções de atualização, consulte Como [atualizar para o AWS Glue Data Catalog passo a passo](#).

A conta de gerenciamento não pode dissociar recursos de uma licença autogerenciada

Se uma conta-membro de uma organização excluir o perfil vinculado ao serviço (SLR) `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` da conta, e houver atributos pertencentes ao membro associados a uma licença autogerenciada, a gestão da conta será impedida de desassociar licenças desses atributos da conta-membro. Isso significa que os atributos da conta-membro continuarão a consumir licenças do grupo de contas de gerenciamento. Para permitir que a conta de gerenciamento desassocie atributos, restaure a SLR.

Esse comportamento é responsável por casos em que um cliente prefere não permitir que a conta de gerenciamento execute algumas ações que afetam os atributos da conta-membro.

O inventário do Systems Manager está desatualizado

O Systems Manager armazena dados nos dados de Inventário por 30 dias. Durante esse período, o License Manager conta uma instância gerenciada como ativa até mesmo se ela não for compatível

com ping. Assim que os dados de inventário forem eliminados do Systems Manager, o License Manager marcará a instância como inativa e atualizará os dados de inventário local. Para manter as contagens de instâncias gerenciadas precisas, recomendamos cancelar o registro das instâncias manualmente no Systems Manager, para que o License Manager possa executar operações de limpeza.

Persistência aparente de uma AMI de registro cancelado

O License Manager elimina associações obsoletas entre atributos e licenças autogerenciadas uma vez a cada algumas horas. Se uma AMI associada a uma licença autogerenciada tiver o registro cancelado por meio do Amazon EC2, a AMI poderá brevemente continuar a ser exibida no inventário de atributos do License Manager antes de ser removida.

Nova instância de conta filho demora a ser exibida no inventário de atributos

Quando o suporte entre contas está habilitado, o License Manager atualiza as contas do cliente às 13h diariamente por padrão. As instâncias adicionadas posteriormente no dia serão exibidas na conta de gerenciamento do inventário de atributos no dia seguinte. Você pode alterar a frequência com que o script de atualização é executado editando o `LicenseManagerResourceSynDataProcessJobTrigger` no AWS Glue console da conta de gerenciamento.

Após habilitar o modo entre contas, as instâncias de contas filho demoram a ser exibidas

Quando você habilita o modo entre contas no License Manager, as instâncias em contas filho podem levar de alguns minutos a algumas horas para serem exibidas no inventário de atributos. O tempo depende do número de contas filho e do número de instâncias em cada conta filho.

Não é possível desabilitar a descoberta entre contas

Após uma conta ser configurada para a descoberta entre contas, será impossível reverter para a descoberta em uma única conta.

O usuário de uma conta filho não consegue associar a licença autogerenciada compartilhada com uma instância

Quando isso ocorrer e a descoberta entre contas estiver habilitada, verifique o seguinte:

- Se a conta filho foi removida da organização.
- A conta filho foi removida do compartilhamento de atributos criado na conta de gerenciamento.
- A licença autogerenciada foi removida do compartilhamento de atributos.

Falha na vinculação de AWS Organizations contas

Se a página Settings (Configurações) relatar esse erro, isso indicará que uma conta não é membro de uma organização pelos seguintes motivos:

- Uma conta filho foi removida da organização.
- Um cliente desativou o acesso ao License Manager do console da organização da conta de gerenciamento.

Histórico do documento para AWS License Manager

A tabela a seguir descreve as versões do AWS License Manager.

Alteração	Descrição	Data
Recupere informações de assinatura BYOL do Red Hat Subscription Manager (RHSM)	O License Manager adicionou suporte para recuperar informações de assinatura do RHSM para licenças BYOL em instâncias do Red Hat Enterprise Linux. Isso inclui atualizações para AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy .	10 de julho de 2024
Suporte adicional para Amazon RDS para licenças BYOL baseadas em vCPUs do Db2	O License Manager adicionou suporte ao Amazon RDS para licenças BYOL baseadas em vCPUs do Db2.	20 de março de 2024
Adição do suporte ao Windows Server 2019 para assinaturas baseadas no usuário do Microsoft Office	AWS adicionou suporte para o Windows Server 2019 nas Amazon Machine Images (AMIs) com licenças fornecidas pela Amazon para o Microsoft Office LTSC Professional Plus 2021 no Amazon EC2.	4 de dezembro de 2023
Usuários do domínio autogerenciado (on-premises) podem utilizar assinaturas baseadas em usuários	O License Manager adicionou suporte para usuários no domínio autogerenciado do Active Directory utilizarem assinaturas baseadas em usuários quando uma relação de confiança com seu	6 de setembro de 2023

Alteração	Descrição	Data
	AWS Managed Microsoft AD diretório for criada.	
Conversões de tipo de licença para assinaturas do Ubuntu LTS	O License Manager adicionou suporte para as instâncias do Ubuntu LTS usarem a conversão de tipo de licença para adicionar uma assinatura do Ubuntu Pro.	20 de abril de 2023
Substituição de concessões ativas	O License Manager adicionou uma funcionalidade para substituir, opcionalmente, concessões ativas por uma licença concedida durante a ativação da concessão.	31 de março de 2023
Administração delegada para assinaturas Linux	O License Manager adicionou suporte a administradores delegados para assinaturas Linux.	3 de março de 2023
Assinaturas Linux	O License Manager adicionou o rastreamento para assinaturas comerciais Linux.	21 de dezembro de 2022
CloudWatch Métricas da Amazon	O License Manager agora emite CloudWatch métricas para o uso da configuração de licenças e assinaturas.	21 de dezembro de 2022
Microsoft Office para assinaturas baseadas em usuários	O License Manager adicionou o Microsoft Office como software compatível com assinaturas baseadas em usuários.	28 de novembro de 2022

Alteração	Descrição	Data
Distribuição de direitos às unidades organizacionais	Distribua direitos para uma OU específica em sua organização.	17 de novembro de 2022
Visualização organizacional (console)	Gerencie as licenças concedidas em suas contas AWS Organizations usando o console do License Manager.	11 de novembro de 2022
Conversão de tipo de licença	Utilize produtos com suporte a Conversão de tipo de licença Amazon EC2.	2 de agosto de 2022
Registro e envio de dados de uso da licença (console)	Registre e envie dados de uso da licença usando o console do License Manager.	28 de março de 2022
Conversão de tipo de licença (console)	Altere seu tipo de licença entre o AWS licenciamento fornecido e o modelo Bring Your Own License (BYOL) usando o console do License Manager sem reimplantar suas cargas de trabalho existentes.	9 de novembro de 2021
Conversão de tipo de licença (CLI)	Altere seu tipo de licença entre o AWS licenciamento fornecido e o modelo Bring Your Own License (BYOL) usando o AWS CLI sem reimplantar suas cargas de trabalho existentes.	22 de setembro de 2021

Alteração	Descrição	Data
Compartilhamento de direitos	Compartilhe direitos de licença gerenciada com toda a sua organização com uma única solicitação.	16 de julho de 2021
Relatórios de uso	Acompanhe o histórico das configurações do seu tipo de licença com os relatórios de uso do License Manager. Anteriormente, os relatórios de uso eram chamados de geradores de relatórios e relatórios de licenças.	18 de maio de 2021
Regras de exclusão da descoberta automática	Exclua instâncias da descoberta automática do License Manager com base em IDs e tags da AWS conta.	5 de março de 2021
Direitos gerenciados	Rastreie e distribua direitos de licença para produtos comprados AWS Marketplace e vendedores que usam o License Manager para distribuir licenças.	3 de dezembro de 2020
Contabilidade automática para software desinstalado	Configure a descoberta automática para interromper o rastreamento de instâncias quando o software for desinstalado.	3 de dezembro de 2020
Filtragem por tags	Pesquise no seu inventário de atributos usando tags.	3 de dezembro de 2020

Alteração	Descrição	Data
Escopo de associação do AMI	Associe suas licenças autogerenciadas e as AMIs compartilhadas com sua conta da AWS .	23 de novembro de 2020
Afinidade de licença com o host	Imponha a atribuição de licenças a hardware dedicado por um número específico de dias.	12 de agosto de 2020
Rastreamento de implantações do Oracle no Amazon RDS	Rastreie o uso da licença para edições de mecanismos e pacotes de licença da base de dados do Oracle no Amazon RDS.	23 de março de 2020
Grupos de atributos de host	Configure um grupo de recursos de host para permitir que o License Manager gerencie seus hosts dedicados.	1º de dezembro de 2019
Descoberta automática de software	Configure o License Manager para pesquisar sistemas operacionais ou aplicativos recém-instalados e anexar as licenças autogerenciadas correspondentes às instâncias.	1º de dezembro de 2019
Diferença entre a licença incluída e Bring Your Own License	Filtre os resultados de pesquisa com base no fato de você estar usando licenças fornecidas pela Amazon ou suas próprias licenças.	8 de novembro de 2019

Alteração	Descrição	Data
Anexar licenças a atributos on-premises	Depois de anexar licenças a uma instância on-premises, o License Manager coleta periodicamente o inventário de software, atualiza as informações de licenciamento e cria relatórios de uso.	8 de março de 2019
AWS License Manager lançamento inicial	Lançamento do serviço inicial	28 de novembro de 2018

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.