Guia do comprador

AWS Marketplace

AWS Marketplace: Guia do comprador

Table of Contents

O que é o AWS Marketplace?

O AWS Marketplace é um catálogo digital administrado que você pode usar para encontrar, comprar, implantar e gerenciar os softwares, dados e serviços de terceiros necessários para criar soluções e administrar seus negócios. O AWS Marketplace inclui milhares de ofertas de software de categorias populares, como segurança, redes, armazenamento, machine learning, IoT, business intelligence, banco de dados e DevOps. O AWS Marketplace também simplifica o licenciamento e a aquisição de software com opções flexíveis de definição de preço e vários métodos de implantação. Além disso, o AWS Marketplace inclui produtos de dados disponíveis no AWS Data Exchange.

Você pode iniciar rapidamente software pré-configurado com apenas alguns cliques e escolher soluções de software nos formatos de imagens de máquina da Amazon (AMIs) e software como serviço (SaaS), bem como outros formatos. Além disso, você pode navegar e assinar produtos de dados. As opções flexíveis de definição de preço incluem avaliação gratuita, por hora, mensal, anual, vários anos e um modelo Traga sua própria licença (BYOL). Todas essas opções de definição de preço são cobradas de uma fonte. A AWS lida com faturamento e pagamentos, e as cobranças aparecem na sua fatura da AWS.

É possível usar o AWS Marketplace como comprador (assinante), como vendedor (provedor) ou ambos. Qualquer pessoa com uma Conta da AWS pode usar o AWS Marketplace como um consumidor e se registrar para se tornar um vendedor. Um vendedor pode ser um provedor independente de software, um revendedor de valor agregado ou um indivíduo que tenha algo a oferecer que funcione com os produtos e serviços da AWS.

> **Note**
>
> Os fornecedores de produtos de dados precisam satisfazer os requisitos de elegibilidade do AWS Data Exchange. Para obter mais informações, consulte Fornecimento de produtos de dados no AWS Data Exchange no Guia do usuário do AWS Data Exchange.

Cada produto de software no AWS Marketplace passou por um processo de curadoria. Na página do produto, pode haver uma ou mais ofertas do produto. Ao enviar um produto no AWS Marketplace, o vendedor define o preço do produto, além dos termos e condições de uso. Os compradores concordam com a definição de preço e os termos e condições definidos para a oferta.

No AWS Marketplace, o produto pode ser de uso gratuito ou ter um custo associado. A cobrança se torna parte da fatura da AWS e, depois de você pagar, o AWS Marketplace pagará o vendedor.

> **Note**
>
> Ao comprar de alguns vendedores não americanos, você também pode receber uma fatura fiscal do vendedor. Para obter mais informações, consulte Vendedores do AWS Marketplace na Ajuda fiscal da Amazon Web Services.

Os produtos podem assumir muitas formas. Por exemplo, um produto pode ser oferecido como uma Imagem de máquina da Amazon (AMI) que é instanciada usando sua Conta da AWS. O produto também pode ser configurado para usar modelos do AWS CloudFormation na entrega para o consumidor. O produto também pode ser ofertas de Software como serviço (SaaS) de um ISV ou uma ACL da web, um conjunto de regras ou condições do AWS WAF.

Você pode comprar produtos de software pelo preço listado usando o contrato de licença de usuário final padrão (EULA) do ISV ou por uma oferta privada com definição de preço e EULA personalizados. Você também pode comprar produtos sob um contrato padrão com horário especificado ou limites de uso.

Depois que as assinaturas do produto estiverem implementadas, você poderá usar o AWS Service Catalog para copiar o produto e gerenciar como o produto é acessado e usado em sua organização. Para obter mais informações, consulte Adicionar produtos do AWS Marketplace ao portfólio no Guia do administrador do AWS Service Catalog.

Estrutura do contrato no AWS Marketplace

O uso do software, dos serviços e dos produtos de dados vendidos no AWS Marketplace é regido por acordos entre compradores e vendedores. A AWS não é uma parte desses acordos.

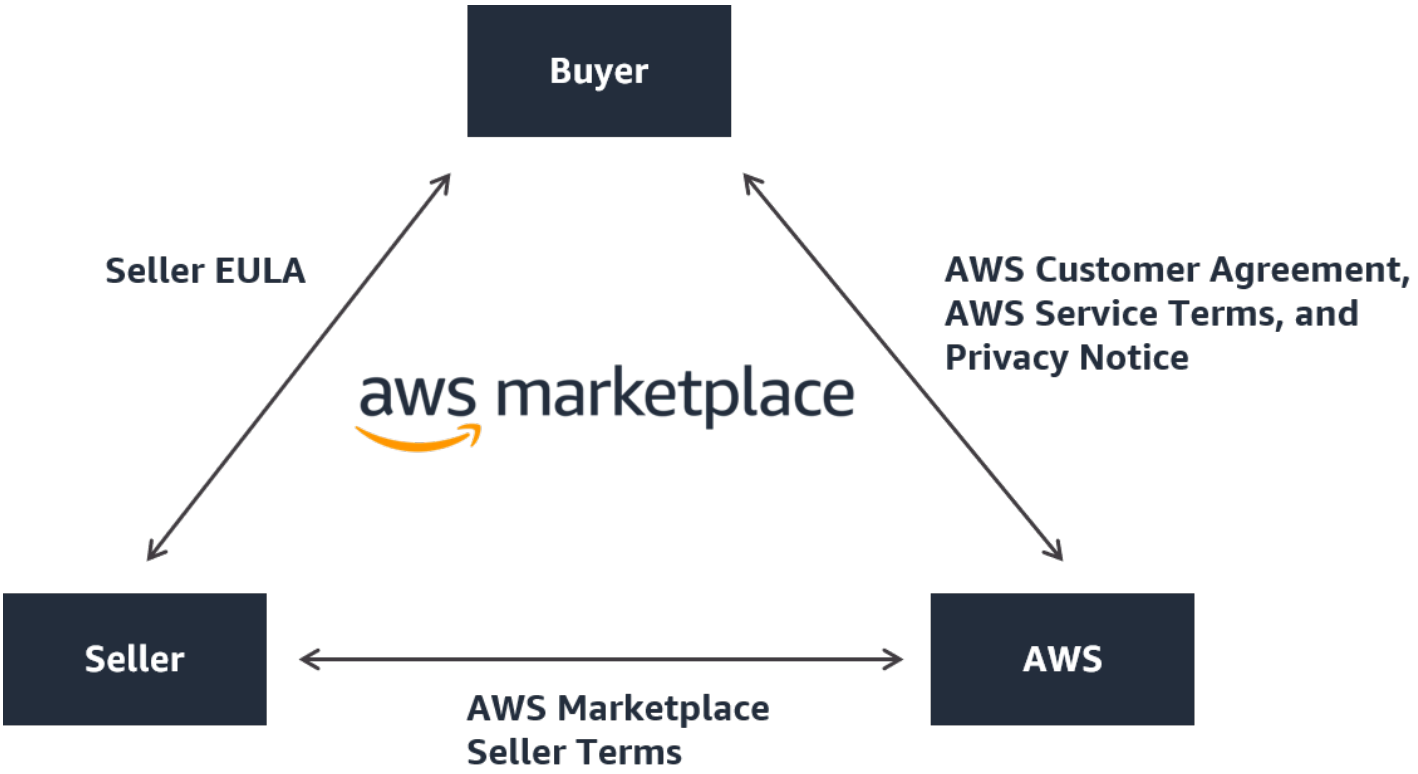
Como comprador, seu uso do AWS Marketplace é regido pelos Termos de Serviço da AWS, pelo Contrato de Cliente da AWS e pelo Aviso de Privacidade.

Os contratos do vendedor incluem o seguinte:

- O EULA do vendedor está localizado na página de listagem de produtos para listagens públicas de software no AWS Marketplace. Muitos vendedores usam o Contrato Padrão para AWS Marketplace (SCMP) como EULA padrão. Eles também podem usar o SCMP como base para negociações em ofertas privadas e usar o modelo de emenda para modificar o SCMP. As ofertas privadas também podem incluir termos contratuais personalizados negociados entre as partes.

- Os Termos do Vendedor do AWS Marketplace regem a atividade do vendedor no AWS Marketplace.

O gráfico a seguir mostra a estrutura do contrato do AWS Marketplace.



Atualizações do EULA

Os vendedores têm a opção de atualizar o EULA para cada um de seus produtos de software como serviço (SaaS). O momento em que essa atualização afeta o EULA depende do tipo de oferta e do modelo de preços.

A tabela a seguir fornece informações sobre quando o novo EULA entrará em vigor para produtos de SaaS.

Tipo de oferta	Modelo de definição de preços	Quando o EULA atualizado entra em vigor
Public	Uso	Você cancela sua assinatura e assina novamente.

Tipo de oferta	Modelo de definição de preços	Quando o EULA atualizado entra em vigor
Public	Contrato	Seu contrato atual termina e se renova em um novo contrato de oferta pública.
Public	Contrato com consumo	Seu contrato atual termina e se renova em um novo contrato de oferta pública.
Private	Uso	Sua oferta privada atual expira e é renovada automatic amente em um novo contrato de oferta pública. As renovações da oferta privada dependem da oferta privada específica.
Private	Contrato	Sua oferta privada atual expira e você assina novamente na oferta pública ou em uma nova oferta privada. As renovações da oferta privada dependem da oferta privada específica.
Private	Contrato com consumo	Sua oferta privada atual expira e você assina novamente na oferta pública ou em uma nova oferta privada. As renovações da oferta privada dependem da oferta privada específica.

Contratos padrão do AWS Marketplace

Ao se preparar para comprar um produto, revise o EULA associado ou o contrato padronizado. Muitos vendedores oferecem o mesmo contrato padronizado na listagens, o Contrato Padrão para AWS Marketplace (SCMP). O AWS Marketplace desenvolveu o SCMP em colaboração com as comunidades de compradores e vendedores para governar o uso e definir as obrigações dos compradores e vendedores em relação às soluções digitais. Exemplos de soluções digitais incluem software de servidor, software como serviço (SaaS) e algoritmos de inteligência artificial e machine learning (AI/ML).

Em vez de revisar EULAs personalizados para cada compra, basta revisar o SCMP uma vez. Os termos do contrato são os mesmos para todos os produtos que usam o SCMP.

Os vendedores também podem usar os seguintes adendos com o SCMP:

- Adendo de segurança aprimorado: oferece suporte a transações com requisitos elevados de segurança de dados.
- Adendo de associado comercial da HIPAA: apoia transações com os requisitos de conformidade da Lei de Portabilidade e Responsabilidade de Seguro de Saúde de 1996 dos EUA (HIPAA).

Para localizar ofertas de produtos que oferecem contratos padronizados, use o filtro Contrato padrão ao pesquisar produtos. Para ofertas privadas, pergunte ao vendedor se ele pode substituir o EULA pelo SCMP e aplicar as emendas acordadas conforme necessário para atender aos requisitos específicos da transação.

Para obter mais informações, consulte Contratos padronizados no AWS Marketplace.

Usar o AWS Marketplace como comprador

Como comprador, acesse o AWS Marketplace para pesquisar, filtrar e navegar até um produto que é executado na Amazon Web Services.

Quando você escolhe um produto de software, a página do produto é aberta. A página tem informações sobre o produto, definição de preço, uso, suporte e análises de produtos. Para assinar o produto de software, você faz login na Conta da AWS e é levado para uma página de assinatura com o EULA, os termos e condições de uso e todas as opções disponíveis para personalizar a assinatura.

As compras do AWS Marketplace feitas por suas contas baseadas na Europa, Oriente Médio e África (exceto Turquia e África do Sul) de vendedores qualificados da EMEA são facilitadas pela Amazon Web Services EMEA SARL.

Para clientes em determinados países, a Amazon Web Services EMEA SARL cobra imposto sobre valor agregado (IVA) local nas compras do AWS Marketplace. Para obter mais informações sobre impostos, consulte a página de ajuda sobre impostos para compradores do AWS Marketplace.

Para obter mais informações sobre a Amazon Web Services EMEA SARL, consulte as Perguntas frequentes da Amazon Web Services EMEA SARL.

Os clientes que negociam com vendedores qualificados da EMEA recebem uma fatura da Amazon Web Services EMEA SARL. Todas as outras transações continuam passando pela AWS Inc. Para obter mais informações, consulte Pagamento de produtos.

Assim que a assinatura for processada, será possível configurar as opções de cumprimento, as versões de software e as Regiões da AWS onde o produto de software será usado e, depois, iniciá-lo. Também encontre ou execute os produtos acessando Software Marketplace no site do AWS Marketplace, pelo AWS Marketplace ou pelo console do Amazon Elastic Compute Cloud (Amazon EC2) ou ainda por meio do Service Catalog.

Para obter mais informações sobre categorias de produtos disponíveis usando o AWS Marketplace, consulte Categorias de produtos.

Para obter mais informações sobre os métodos de entrega de produtos de software no AWS Marketplace, consulte:

- Produtos de servidor baseados em AMI
- Produtos de contêiner
- Produtos de machine learning
- Produtos de serviços profissionais
- Produtos de SaaS
- Produtos de dados: consulte O que é o AWS Data Exchange? no Guia do usuário do AWS Data Exchange

Software e serviços no AWS Marketplace

O AWS Marketplace conta com muitas categorias de software, inclusive bancos de dados, servidores de aplicativos, ferramentas de teste, ferramentas de monitoramento, gerenciamento de conteúdo e business intelligence. Selecione softwares comerciais de vendedores conhecidos, bem como muitas ofertas de código aberto amplamente usadas. Ao encontrar produtos desejados, você pode comprar e implantar esse software em sua própria instância do Amazon EC2 com 1 clique. Você também pode usar o AWS CloudFormation para implantar uma topologia do produto.

Qualquer cliente da AWS pode comprar no AWS Marketplace. Os preços de software e infraestrutura estimados são exibidos no site. Compre a maioria dos software imediatamente usando instrumentos de pagamento já registrado na AWS. As cobranças de software aparecem na mesma fatura mensal que as taxas de infraestrutura da AWS.

Observações

- Há muitos produtos comerciais disponíveis no AWS Marketplace, inclusive produtos de software como serviço (SaaS) e baseados no servidor. Os produtos baseados no servidor podem exigir conhecimento técnico ou suporte de TI para configurar e manter.
- As informações e os tutoriais em Tutorial: conceitos básicos das instâncias do Linux do Amazon EC2 podem ajudar você a conhecer os conceitos básicos do Amazon EC2.
- Se você planejar executar topologias complexas de produtos do AWS Marketplace por meio do AWS CloudFormation, Conceitos básicos do AWS CloudFormation poderá ajudar você a saber os conceitos básicos úteis do AWS CloudFormation.

O AWS Marketplace inclui as seguintes categorias de software:

- Software de infraestrutura
- Ferramentas de desenvolvedor
- Software comercial
- Machine learning
- IoT
- Serviços profissionais
- Aplicativos desktop

- Produtos de dados

Para obter mais informações, consulte Categorias de produtos.

Cada categoria de software principal contém mais subcategorias específicas. Por exemplo, a categoria de infraestrutura de software contém subcategorias como desenvolvimento de aplicativos, bancos de dados e armazenamento em cache e sistemas operacionais. O software está disponível como um dos sete tipos diferentes de produtos, incluindo imagens de máquina da Amazon (AMIs) e software como serviço (SaaS). Para obter informações sobre os tipos diferentes de software, consulte Tipos de produto.

Para ajudar você a escolher o software necessário, o AWS Marketplace fornece as seguintes informações:

- Detalhes do vendedor
- Versão do software
- Tipo de software (AMI ou SaaS) e informações sobre a AMI, se aplicáveis
- Avaliação do comprador
- Preço
- Informações do produto

Diferenças entre o AWS Marketplace e o Amazon DevPay

Há diferenças substanciais entre o AWS Marketplace e o Amazon DevPay. Ajude os clientes na compra de software executado na AWS, mas o AWS Marketplace oferece uma experiência mais abrangente do que o Amazon DevPay. Para compradores de software, as principais diferenças são as seguintes:

- O AWS Marketplace oferece uma experiência de compra mais parecida com Amazon.com, simplificando a descoberta dos softwares disponíveis.
- Os produtos do AWS Marketplace funcionam com outros recursos da AWS como a nuvem privada virtual (VPC) e podem ser executados em instâncias reservadas e instâncias spot do Amazon Elastic Compute Cloud (Amazon EC2), além de instâncias sob demanda.
- O AWS Marketplace oferece suporte a softwares compatíveis com o Amazon Elastic Block Store (Amazon EBS), e o Amazon DevPay não.

Além disso, os vendedores de software se beneficiam do alcance de marketing e da facilidade de descoberta do AWS Marketplace.

Conceitos básicos do trabalho de um comprador

Os tópicos a seguir descrevem o processo de começar a usar produtos de software como comprador do AWS Marketplace.

Tópicos

Para obter informações sobre como começar a usar produtos de dados, consulte Assinatura de produtos de dados no AWS Data Exchange no Guia do usuário do AWS Data Exchange.

Comprar produtos

No AWS Marketplace, comprar um produto significa que você aceitou os termos do produto como mostrado na página de listagem do produto. Isso inclui os termos de definição de preço e o contrato de licença de usuário final (EULA) do vendedor e que você concorda em usar esse produto de acordo com o Contrato do cliente da AWS. Você receberá uma notificação por e-mail no endereço de e-mail associado à sua Conta da AWS para as ofertas aceitas no AWS Marketplace.

Se o produto tiver uma taxa mensal ou tiver sido comprado mediante um contrato de assinatura, você receberá a cobrança da taxa mediante a assinatura. A assinatura é rateada com base no tempo restante do mês. Nenhuma outra cobrança é avaliada até que você execute uma das seguintes ações:

- Execute uma instância do Amazon Elastic Compute Cloud (Amazon EC2) com o produto de imagem de máquina da Amazon (AMI).
- Implante o produto usando um modelo do AWS CloudFormation.
- Registre o produto no site do vendedor.

Se o produto tiver uma opção de assinatura anual, você receberá a cobrança da taxa anual total mediante a assinatura. Essa cobrança abrange a base de uso do produto, com a renovação da assinatura devida no aniversário da data da assinatura original. Se você não renovar no final do

período da assinatura anual, ela será convertida em uma assinatura por hora de acordo com a taxa por hora atual.

Para obter mais informações sobre assinaturas de produtos de dados, consulte Assinatura de produtos de dados do AWS Data Exchange no Guia do usuário do AWS Data Exchange.

Iniciar software

Depois de comprar o software, você pode iniciar as imagens de máquina da Amazon (AMIs) que o contêm usando a visualização 1-Click Launch no AWS Marketplace. Você também pode executá-lo usando outras ferramentas de gerenciamento da Amazon Web Services (AWS), incluindo o AWS Management Console, o console do Amazon Elastic Compute Cloud (Amazon EC2), as APIs do Amazon EC2 ou o console do AWS CloudFormation.

Com a exibição Execução de 1 clique, é possível examinar, modificar e iniciar rapidamente uma única instância do software com configurações recomendadas pelo vendedor do software. A exibição Iniciar com console do EC2 oferece uma maneira fácil de encontrar o número de identificação da AMI e outras informações pertinentes obrigatórias para iniciar a AMI usando o AWS Management Console, as APIs do Amazon EC2 ou outras ferramentas de gerenciamento. A exibição Iniciar com console do EC2 também fornece mais opções de configuração do que a inicialização a partir do AWS Management Console, como marcar uma instância.

Para produtos do AWS Marketplace com topologias complexas, a exibição Execução personalizada fornece um botão Iniciar com o console do CloudFormation que carrega o produto no console do AWS CloudFormation com o modelo do AWS CloudFormation. Em seguida, siga as etapas no assistente do console do AWS CloudFormation para criar o cluster de AMIs e recursos da AWS associados desse produto.

Tutorial: Comprar um produto de software baseado em AMI

O tutorial a seguir descreve como comprar um produto de imagem de máquina da Amazon (AMI) com o AWS Marketplace.

Etapas

- Etapa 1: criar uma Conta da AWS
- Etapa 2: escolher o software
- Etapa 3: configurar o software

- Etapa 4: executar o software no Amazon EC2
- Etapa 5: gerenciar o software
- Etapa 6: encerrar a instância

Etapa 1: criar uma Conta da AWS

Você pode navegar no site do AWS Marketplace (https://aws.amazon.com/marketplace) sem estar conectado à Conta da AWS. No entanto, você precisa fazer login para assinar ou executar produtos.

É necessário estar conectado à sua Conta da AWS para acessar o console do AWS Marketplace. Para obter informações sobre como criar uma Conta da AWS, consulte Criação de uma Conta da AWS no Guia de referência do AWS Account Management.

Etapa 2: escolher o software

Como escolher o software

1. Navegue até o site do AWS Marketplace.

   > **Note**
   >
   > Você pode comprar, assinar e executar novas instâncias no site público do AWS Marketplace, em https://aws.amazon.com/marketplace, ou por meio do AWS Marketplace no AWS Management Console, em https://console.aws.amazon.com/marketplace/home#/subscriptions.
   > As experiências nos dois locais são semelhantes. Esse procedimento usa o site do AWS Marketplace, mas observa as principais diferenças ao usar o console.

2. O painel Shop All Categories (Todas as categorias de compra) contém a lista de categorias à disposição. Também escolha o software em destaque no painel intermediário. Neste tutorial, no painel Todas as categorias de compra, escolha Gerenciamento de conteúdo.
3. Na lista Gerenciamento de conteúdo, escolha WordPress Certified by Bitnami and Automattic.
4. Na página de detalhes do produto, examine as informações. A página de detalhes do produto inclui informações adicionais como:

   - Avaliação do comprador
   - Oferta de suporte

- Destaques
- Descrição detalhada do produto
- Detalhes de preço dos tipos de instância em cada Região da AWS (para AMIs)
- Recursos adicionais para ajudar você a dar os primeiros passos

5. Escolha Continue to Subscribe (Continuar para assinar).
6. Se você ainda não tiver feito login, será direcionado para fazer login no AWS Marketplace. Se já tiver uma Conta da AWS, você poderá usar essa conta para fazer login. Se você ainda não tiver configurado uma Conta da AWS, consulte Etapa 1: criar uma Conta da AWS.
7. Leia os termos da oferta da Bitnami e escolha Aceitar contrato para concordar com a oferta de assinatura.
8. Pode levar alguns minutos para que a ação de assinatura seja concluída. Quando isso acontecer, você receberá uma mensagem de e-mail sobre os termos da assinatura e poderá continuar. Escolha Continuar com a configuração para configurar e executar seu software.

Assinar um produto significa que você aceitou os termos do produto. Se o produto tiver uma taxa mensal, a assinatura será cobrada mediante a taxa, que será pro rata com base no tempo restante no mês. Nenhuma outra cobrança será avaliada até você executar uma instância do Amazon Elastic Compute Cloud (Amazon EC2) com a AMI escolhida.

> **Note**
>
> Como assinante de um produto, sua conta receberá mensagens de e-mail quando uma nova versão do software que você assinou for publicada.

Etapa 3: configurar o software

Como escolhemos o software como AMI, sua próxima etapa é configurar o software, incluindo a seleção do método de entrega, da versão e da Região da AWS da qual você deseja usar o software.

Para configurar o software

1. Na página Configurar este software, selecione Imagem de máquina da Amazon (AMI) de 64 bits (x86) para o Método de entrega.
2. Escolha a versão mais recente disponível para a Versão do software.

3. Escolha a Região na qual você deseja lançar o produto, por exemplo, Leste dos EUA (Norte da Virgínia).

> **Note**
>
> Ao fazer alterações na configuração, você pode notar que o ID da AMI na parte inferior da tela é atualizado. O ID da AMI tem o formato ami-<identificador>, por exemplo, *ami-123example456*. Cada versão de cada produto em cada região tem uma AMI diferente. Esse ID da AMI permite que você especifique a AMI correta a ser usada ao executar o produto. O Alias da AMI é um ID semelhante que é mais fácil de usar na automação.
> Para obter mais informações sobre o alias da AMI, consulte Sobre aliases de AMI.

4. Selecione Continue para executar.

Etapa 4: executar o software no Amazon EC2

Antes de iniciar a instância do Amazon EC2, você precisa decidir se deseja iniciar com a execução com 1 clique ou executar usando o console do Amazon EC2. A execução com 1 clique ajuda a iniciar rapidamente com opções padrão recomendadas, como grupos de segurança e tipos de instância. Com a execução com 1 clique, também é possível ver a cobrança mensal estimada. Se preferir mais opções, como iniciar em uma Amazon Virtual Private Cloud (Amazon VPC) ou usar instâncias spot, você deverá iniciar usando o console do Amazon EC2. Os procedimentos a seguir orientam você em meio à assinatura do produto e à execução de uma instância do EC2 usando a execução com 1 clique ou o console do Amazon EC2.

Execução no Amazon EC2 usando a execução com 1 clique

Para executar no Amazon EC2 usando a execução com 1 clique

1. Na página Iniciar este software, escolha Iniciar a partir do site na lista suspensa Escolher ação e revise as configurações padrão. Se você quiser alterar alguma delas, faça o seguinte:

   - Na lista suspensa Tipo de instância do EC2, escolha um tipo de instância.
   - Nas listas suspensas Configurações de VPC e Configurações de sub-rede, selecione as configurações de rede que você deseja usar.
   - Em Configurações de grupo de segurança, escolha um grupo de segurança existente ou escolha Criar com base nas configurações do vendedor para aceitar as configurações padrão.

Para obter mais informações sobre os grupos de segurança, consulte Grupos de segurança do Amazon EC2 para instâncias do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux.

- Expanda Key Pair (Par de chaves) e escolha um par de chaves existente, se você tiver um. Se ainda não tiver um par de chaves, você precisará criar um. Para obter mais informações sobre pares de chaves do Amazon EC2, consulte Pares de chaves do Amazon EC2.

2. Quando você estiver satisfeito com as configurações, escolha Executar.

   Sua nova instância é executada com o software WordPress Certified by Bitnami e Automattic em execução nela. A partir daqui, você pode ver os detalhes da instância, criar outra instância ou visualizar todas as instâncias do software.

Execução no Amazon EC2 usando a execução com o console do EC2

Para Iniciar no Amazon EC2 usando a execução com o console do EC2

1. Na página Iniciar no EC2, escolha a exibição Iniciar com console do EC2 e selecione uma versão da AMI na lista Selecionar uma versão.
2. Examine as Firewall Settings (Configurações do firewall), as Installation Instructions (Instruções de instalação), Release Notes (Notas de release) e escolha Launch with EC2 Console (Iniciar com console do EC2).
3. No console do EC2, execute a AMI usando o assistente de solicitação da instância. Siga as instruções em Conceitos básicos das instâncias do Linux do Amazon EC2 para navegar pelo assistente.

Etapa 5: gerenciar o software

A qualquer momento, você pode gerenciar suas assinaturas de software no AWS Marketplace usando a página Gerenciar assinaturas do console do AWS Marketplace.

Como gerenciar o software

1. Navegue até o console do AWS Marketplace e escolha Gerenciar assinaturas.
2. Na página Gerenciar assinaturas:

   - Exibir o status da instância por produto
   - Exibir as cobranças mensais atuais

- Executar uma nova instância
- Exibir perfis do vendedor da instância
- Gerenciar instâncias
- Vincular diretamente à instância do Amazon EC2 para configurar o software

Etapa 6: encerrar a instância

Ao perceber que você não necessita mais de sua instância, você pode encerrá-la.

> **Note**
>
> Não reinicie uma instância encerrada. No entanto, inicie instâncias adicionais da mesma AMI.

Para encerrar sua instância

1. Navegue até o console do AWS Marketplace e escolha Gerenciar assinaturas.
2. Na página Gerenciar assinaturas, escolha a assinatura de software da qual você deseja encerrar uma instância e selecione Gerenciar.
3. Na página de assinatura específica, escolha Exibir instâncias na lista suspensa Ações.
4. Selecione a Região em que a instância que você deseja encerrar está. Isso abre o console do Amazon EC2 e mostra as instâncias nessa região em uma nova guia. Se necessário, você pode retornar a essa guia para ver o ID da instância a ser fechada.
5. No console do Amazon EC2, escolha o ID da instância para abrir a página Detalhes da instância.
6. Na lista suspensa Estado da instância, escolha Encerrar instância.
7. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

   O encerramento leva alguns minutos para ser concluído.

Para obter mais informações

Para obter mais informações sobre categorias e tipos de produto, consulte Categorias de produtos e Tipos de produto.

Para obter mais informações sobre o Amazon EC2, consulte a documentação do serviço em Documentação do Amazon Elastic Compute Cloud.

Para saber mais sobre a AWS, consulte https://aws.amazon.com/.

Regiões da AWS compatíveis no AWS Marketplace

Para produtos de software, o vendedor escolhe em quais Regiões da AWS disponibilizar o software, bem como os tipos de instância. Incentivamos a disponibilização de produtos em todas as regiões e em todos os tipos de instância que façam sentido. O site do AWS Marketplace está disponível em todo o mundo, e é compatível com as seguintes regiões:

- América do Norte
  - Leste dos EUA (Ohio)
  - Leste dos EUA (N. da Virgínia)
  - Oeste dos EUA (N. da Califórnia)
  - Oeste dos EUA (Oregon)
  - AWS GovCloud (Leste dos EUA)
  - AWS GovCloud (Oeste dos EUA)
  - Canadá (Central)
  - Oeste do Canadá (Calgary)

- África
  - África (Cidade do Cabo)

- América do Sul
  - América do Sul (São Paulo)

- EMEA
  - Europa (Frankfurt)
  - Europa (Irlanda)
  - Europa (Londres)
  - Europa (Milão)
  - Europa (Paris)
  - Europa (Espanha)
  - Europa (Estocolmo)
  - Europa (Zurique)

- APAC
  - Ásia-Pacífico (Hong Kong)
  - Ásia-Pacífico (Hyderabad)
  - Ásia-Pacífico (Jacarta)
  - Ásia-Pacífico (Melbourne)
  - Ásia-Pacífico (Mumbai)
  - Ásia-Pacífico (Osaka)
  - Ásia-Pacífico (Seul)
  - Ásia-Pacífico (Singapura)
  - Ásia-Pacífico (Sydney)
  - Ásia-Pacífico (Tóquio)

- Oriente Médio
  - Israel (Tel Aviv)
  - Oriente Médio (Barém)
  - Oriente Médio (Emirados Árabes Unidos)

Para obter mais informações sobre regiões compatíveis com produtos de dados, consulte Endpoints e cotas do AWS Data Exchange na Referência geral da AWS.

Categorias de produtos

O site do AWS Marketplace está organizado em quatro categorias, com subcategorias em cada uma. Você pode pesquisar e filtrar com base nas categorias e nas subcategorias.

Tópicos

Software de infraestrutura

Os produtos nessa categoria oferecem soluções relacionadas à infraestrutura.

Backup e recuperação

: Produtos usados em soluções de armazenamento e backup.

Análise de dados

: Produtos usados para análise de dados.

Computação de alta performance

: Produtos de computação de alta performance.

Migração

: Produtos usados em projetos de migração.

Infraestrutura de rede

: Produtos usados para criar soluções de rede.

Sistema operacional

Sistemas operacionais Linux e Windows empacotados.

Segurança

Produtos de segurança para a infraestrutura.

Storage (Armazenamento)

Aplicações concentradas em cargos envolvidos em armazenamento.

DevOps

Os produtos nessa categoria fornecem ferramentas concentradas em desenvolvedores e equipes de desenvolvedores.

Gerenciamento de ciclo de vida Agile

Produtos usados para o Agile SDLM.

Desenvolvimento de aplicativos

Produtos usados no desenvolvimento de aplicativos.

Servidores de aplicativos

Servidores usados no desenvolvimento de aplicativos.

Pilhas de aplicativos

Pilhas usadas no desenvolvimento de aplicativos.

Integração contínua e entrega contínua

Produtos usados para CI/CD.

Infraestrutura como código

Produtos usados para infraestrutura.

Rastreamento de problemas e bugs

Produtos usados por equipes de desenvolvedores para rastrear e gerenciar bugs de software.

Monitoramento

Produtos usados para monitorar o software operacional.

Análise de logs

Produtos usados no registro em log e na análise de logs.

Controle de origem

Ferramentas usadas para gerenciar e manter o controle de origem.

no dispositivo

Produtos usados em testes automatizados de produtos de software.

Aplicativos de negócios

Os produtos nessa categoria ajudam a administrar a empresa.

Blockchain

Produtos usados para blockchain.

Colaboração e produtividade

Produtos usados para habilitar a colaboração na empresa.

Central de atendimento

Produtos usados para habilitar centrais de atendimento em sua organização.

Gerenciamento de conteúdo

Produtos concentrados no gerenciamento de conteúdo.

CRM

Ferramentas concentradas no gerenciamento de relações com o cliente.

Comércio eletrônico

Produtos que fornecem soluções de comércio eletrônico.

eLearning

Produtos que fornecem soluções de eLearning.

Recursos humanos

Produtos usados para habilitar recursos humanos em sua organização.

Gerenciamento de negócios de TI

Produtos usados para habilitar gerenciamento de negócios de TI em sua organização.

Business Intelligence

Produtos usados para habilitar business intelligence na organização.

Gerenciamento de projetos

Ferramentas para gerenciamento de projetos.

Machine Learning

Os produtos nessa categoria fornecem algoritmos de machine learning e pacotes de modelos que funcionam com o Amazon SageMaker.

Soluções ML

Soluções de machine learning.

Serviços de identificação de dados

Produtos que oferecem capacidade de identificação de dados.

Visão computacional

Produtos que habilitam visão computacional.

Processamento de linguagem natural

Produtos que habilitam a capacidade de processamento de linguagem natural.

Reconhecimento de voz

Produtos que habilitam a capacidade de reconhecimento de voz.

Texto

Produtos que habilitam a capacidade de aprendizado de texto. Entre os exemplos estão classificação, agrupamento, edição/processamento, incorporação, geração, gramática/análise, identificação, nomes e reconhecimento de entidades, análise de sentimento, resumo, texto para fala e tradução.

Imagem

Produtos que habilitam a capacidade de análise da imagem. Entre os exemplos estão 3D, legenda, classificação, edição/processamento, incorporação/extração de recursos, geração,

gramática/análise, reconhecimento de letra manuscrita, humano/face, detecção de objetos, segmentação/identificação de pixels e texto/OCR.

Vídeo

Produtos que habilitam a capacidade de análise do vídeo. Entre os exemplos estão classificação, detecção de objetos, edição/processamento, detecção de anomalias, identificação do falante, movimento, reindentificação, resumo, texto/legenda e rastreamento.

Áudio

Produtos que habilitam a capacidade de análise do áudio. Entre os exemplos estão identificação do falante, fala para texto, classificação, identificação da música e segmentação.

Estruturados

Produtos que habilitam a capacidade de análise estruturada. Entre os exemplos estão classificação, agrupamento, redução de dimensionalidade, modelos de fatorização, engenharia de recursos, classificação, regressão e previsão de série temporal.

IoT

Produtos usados para criar soluções relacionadas a IoT.

Análise

Produtos analíticos para soluções de IoT.

Aplicativos

Produtos de aplicativo para o espaço de soluções de IoT.

Conectividade do dispositivo

Produtos usados para gerenciar a conectividade do dispositivo.

Gerenciamento de dispositivos

Produtos usados para gerenciar dispositivos.

Segurança do dispositivo

Produtos usados para gerenciar a segurança dos dispositivos de IoT.

IoT industrial

Produtos concentrados em fornecer soluções de IoT relacionadas à indústria.

Casa e cidade inteligentes

Produtos usados para habilitar soluções de casa e cidade inteligentes.

Serviços profissionais

Os produtos desta categoria fornecem serviços de consultoria relacionados a produtos do AWS Marketplace.

Avaliações

Avaliação do seu ambiente operacional atual para encontrar as soluções certas para sua organização.

Implementação

Ajuda para instalação, configuração e implantação de software de terceiros.

Serviços gerenciados

Gerenciamento de ponta a ponta do ambiente em seu nome.

Premium Support

Acesso a orientação e assistência de especialistas, projetadas para suas necessidades.

Treinamento

Workshops, programas e ferramentas educacionais personalizados fornecidos por especialistas para ajudar seus funcionários a aprender as práticas recomendadas.

Aplicativos desktop

Os produtos nessa categoria oferecem soluções relacionadas à infraestrutura.

Aplicativos desktop

Aplicativos e utilitários desktop para produtividade geral e habilitação de função específica.

AP e faturamento

Aplicativos usados para cargos concentrados em contas a pagar e faturamento.

Aplicativo e a web

Aplicativos de uso geral e de ambiente da web.

Desenvolvimento

Aplicativos usados no desenvolvimento.

Business Intelligence

Aplicativos usados por cargos concentrados no gerenciamento de business intelligence.

CAD e CAM

Aplicativos usados por cargos concentrados em design auxiliado por computador e fabricação.

GIS e mapeamento

Aplicativos usados por cargos concentrados em GIS e mapeamento.

Ilustração e design

Aplicativos para cargos concentrados em ilustração e design.

Mídia e codificação

Aplicativo usado em cargos envolvidos em mídia e codificação.

Produtividade e colaboração

Aplicativos concentrados em habilitar produtividade e colaboração.

Gerenciamento de projetos

Aplicativo para cargos de gerente de projetos.

Segurança/armazenamento/arquivamento

Aplicativos concentrados em cargos envolvidos em segurança, armazenamento e arquivamento de dados.

Utilitários

Aplicativos concentrados em utilitários para cargos variados.

Produtos de dados

Os produtos nesta categoria são conjuntos de dados baseados em arquivo. Para obter mais informações, consulte o Guia do usuário do AWS Data Exchange.

Indústrias

Educação e pesquisa

Produtos destinados a fornecer soluções de educação e pesquisa.

Serviços financeiros

Produtos que habilitam serviços financeiros na organização.

Saúde e ciências biológicas

Produtos usados nos setores de saúde e ciências biológicas.

Mídia e entretenimento

Produtos e soluções relacionados à mídia.

Industrial

Produtos e soluções relacionados à indústria.

Energia

Produtos e soluções relacionados à energia.

Tipos de produto

O AWS Marketplace inclui software popular de código aberto e comercial, bem como produtos de dados gratuitos e pagos. Esses produtos estão disponíveis de maneiras diferentes: como imagens de máquina da Amazon (AMIs) individuais, como um cluster de AMIs implantadas por meio de um modelo do AWS CloudFormation, como software como serviço (SaaS) e como produtos de dados do AWS Data Exchange.

Para obter mais informações sobre esses tipos de produtos, consulte os seguintes tópicos:

- Produtos de servidor baseados em AMI (incluindo produtos de AMI e imagem privada)
- Produtos de contêiner
- Produtos de machine learning
- Produtos de serviços profissionais
- Produtos de SaaS
- Produtos de dados

Produtos de servidor baseados em AMI

A imagem de máquina da Amazon (AMI) é uma imagem de um servidor, inclusive um sistema operacional e normalmente um software adicional, executado na AWS.

O software listado no AWS Marketplace está disponível somente para execução no Amazon Elastic Compute Cloud (Amazon EC2). Ele não está disponível para download.

No AWS Marketplace, procure AMIs (com sugestões de pesquisa), exiba análises de produtos enviadas por outros clientes, assine e inicie AMIs, além de gerenciar as assinaturas. Todos os produtos do AWS Marketplace foram verificados em termos de qualidade e pré-configurados para o recurso de execução com 1 clique na infraestrutura da Amazon Web Services (AWS).

As listagens de produtos de AMI e software como serviço (SaaS) vêm de vendedores confiáveis. Os produtos de AMI executados na Conta da AWS de um cliente. Você mantém mais controle sobre a configuração de software e os servidores que executam o software, mas você também tem responsabilidades adicionais relacionadas à configuração e à manutenção do servidor.

O catálogo do AWS Marketplace contém uma seleção gerenciada de software comerciais e de código aberto de vendedores conhecidos. Muitos produtos no AWS Marketplace podem ser comprados por hora.

Catálogo AMI é um recurso da comunidade em que as pessoas e as equipes de desenvolvimento podem listar e trocar software ou projetos em desenvolvimento sem a necessidade de passar por uma ampla inspeção. As listagens no catálogo AMI da comunidade podem ou não ser de vendedores conhecidos e normalmente não passam por investigações adicionais.

Um produto do AWS Marketplace contém uma AMI para cada Região da AWS na qual o produto está disponível. Essas AMIs são idênticas, exceto pelo local. Além disso, quando atualizam os produtos com os patches e as atualizações mais recentes, os vendedores podem adicionar outro conjunto de AMIs ao produto.

Alguns produtos do AWS Marketplace podem iniciar várias instâncias de uma AMI, porque eles são implantados como um cluster usando modelos do AWS CloudFormation. Esse cluster de instâncias, além de outros serviços de infraestrutura da AWS configurados pelo modelo do CloudFormation, funciona como uma única implantação de produto.

Modelo AWS CloudFormation

> **Important**
>
> O AWS Marketplace interromperá o método de entrega de vários produtos de imagem de máquina da Amazon (AMI) usando modelos do AWS CloudFormation em agosto de 2024. Outros produtos do AWS Marketplace que usam o CloudFormation, como uma única AMI com o CloudFormation, não serão afetados.
>
> Até agosto de 2024, os assinantes existentes podem executar novas instâncias de seus vários produtos de AMI usando os modelos do CloudFormation no AWS Marketplace. Após a descontinuação, eles não poderão executar novas instâncias. Todas instâncias existentes lançadas e executadas anteriormente no Amazon Elastic Compute Cloud (Amazon EC2) não serão afetadas e continuarão sendo executadas.
>
> Se tiver dúvidas, entre em contato com o AWS Support.

O AWS CloudFormation é um serviço que ajuda você a modelar e configurar seus recursos da AWS para despender menos tempo gerenciando esses recursos e mais tempo se concentrando em seus aplicativos executados AWS. Um modelo do CloudFormation descreve os vários recursos da AWS

que você deseja, como instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou instâncias de banco de dados do Amazon Relational Database Service (Amazon RDS). O CloudFormation se encarrega de provisionar e configurar esses recursos para você. Para obter mais informações, consulte Conceitos básicos do AWS CloudFormation.

Uso de modelos do AWS CloudFormation

Os vendedores de software podem oferecer modelos do CloudFormation para definir uma topologia de implantação preferida que consiste em várias instâncias da AMI e outros recursos da AWS. Se estiver disponível para um produto, um modelo do CloudFormation será listado como uma opção de implantação na página de listagem de produtos.

Use uma AMI para implantar uma única instância do Amazon EC2. Use um modelo do CloudFormation para implantar várias instâncias de uma AMI que funcionem como um cluster, além de recursos da AWS, como o Amazon RDS, o Amazon Simple Storage Service (Amazon S3) ou qualquer outro serviço da AWS, como uma única solução.

Tópicos

- Assinaturas de AMI no AWS Marketplace
- Produtos da AMI com preços contratuais
- Produtos de AMI habilitados para medição
- Marcação de alocação de custos em produtos de AMI
- Criação de imagens privadas
- Sobre aliases de AMI

Assinaturas de AMI no AWS Marketplace

No AWS Marketplace, alguns produtos de software baseados na imagem de máquina da Amazon (AMI) oferecem um modelo anual de preços por assinatura. Com esse modelo de preços, você faz um pagamento adiantado único e não paga nenhuma taxa de uso por hora nos próximos 12 meses. Você pode aplicar uma assinatura anual a um produto de software do AWS Marketplace em uma instância do Amazon Elastic Compute Cloud (Amazon EC2).

> **Note**
>
> Para AMI por hora com preço anual, a assinatura anual cobre somente os tipos de instância que você especifica ao comprar. Por exemplo, `t3.medium`. A execução de qualquer

outro tipo de instância incorrerá na taxa horária desse tipo de instância com base na assinatura ativa. Você não pode alterar o tipo de instância de uma assinatura anual depois de comprada.

Também continue iniciando e executando produtos de software do AWS Marketplace usando a definição de preço por hora. As cobranças para usar o Amazon EC2 e outros serviços da AWS são separadas e adicionais ao que você paga para comprar produtos de software do AWS Marketplace.

Se você alterar o tipo de instância do Amazon EC2 para uso por hora, a infraestrutura do Amazon EC2 será cobrada de acordo com o plano de economia assinado. No entanto, a licença da AMI do AWS Marketplace mudará automaticamente para o preço por hora.

Se um produto da AMI por hora não oferecer suporte ao preço anual, o comprador não poderá comprar uma assinatura anual. Se um produto por hora da AMI oferecer suporte ao preço anual, o comprador poderá acessar a página do produto do AWS Marketplace e comprar contratos anuais. Cada contrato anual permite que o comprador execute uma instância sem a cobrança da taxa horária. Os contratos variam de acordo com o tipo de instância.

Produtos da AMI com preços contratuais

Alguns vendedores oferecem produtos de software públicos baseados na imagem de máquina da Amazon (AMI) com um modelo de preços contratuais. Nesse modelo, você concorda em fazer um pagamento adiantado único por quantidades discretas de licenças para acessar o produto de software pelo período de sua escolha. Você recebe a cobrança, antecipadamente, por meio da Conta da AWS. Por exemplo, você pode comprar 10 licenças de acesso de usuário e cinco licenças administrativas por um ano. Você pode optar por renovar as licenças automaticamente.

Além disso, algumas empresas oferecem produtos de software privados baseados na AMI com um modelo de preços contratuais. Uma oferta privada normalmente tem uma duração fixa que não pode ser alterada.

Você pode comprar um contrato de produto de software baseado na AMI usando a página de detalhes do produto no AWS Marketplace. Se essa opção estiver disponível, AMI com preço contratual será exibido para Método de entrega na página de detalhes do produto. Quando fizer a compra, você será direcionado para o site do produto para instalação e configuração da conta. As cobranças de uso acabarão sendo exibidas no relatório de faturamento da Conta da AWS regular.

Assinatura de um produto de AMI com oferta pública de preços contratuais

Para assinar uma oferta pública de produto baseado na AMI com um modelo de preço contratual

1. Faça login no AWS Marketplace e encontre um produto de software baseado em contêineres com um modelo de preços contratuais.
2. Na página Compras, veja as Informações de preços.

   Você pode ver as Unidades e a taxa de cada duração (em meses).
3. Escolha Continue para assinar para iniciar a assinatura.

   Para salvar este produto sem assinar, escolha Salvar na lista.
4. Crie um contrato revisando as informações de preços e configurando os termos do produto de software.

   a. Escolha a duração do contrato: 1 mês, 12 meses, 24 meses ou 36 meses
   b. Em Configurações de renovação, escolha se deseja renovar automaticamente o contrato.
   c. Em Opções de contrato, escolha uma quantidade para cada unidade.

   O preço total do contrato é exibido em Detalhes do preço.
5. Depois de fazer todas as seleções, escolha Create Contract (Criar contrato).

O Preço total do contrato é cobrado na Conta da AWS. Uma licença é gerada no AWS License Manager.

> **Note**
>
> Pode levar até 10 minutos para que a assinatura seja processada e uma licença seja gerada na conta do AWS License Manager para o produto de software.

Assinatura de um produto de AMI com oferta privada de preços contratuais

Para assinar uma oferta privada de produto baseado na AMI com um modelo de preço contratual

1. Faça login no AWS Marketplace com sua conta de comprador.
2. Veja a oferta privada.

3. Na página Compras, veja as Informações de preços.

   Você pode ver as Unidades e a taxa de cada duração (em meses).
4. Escolha Continue para assinar para iniciar a assinatura.
5. Crie um contrato revisando as informações de preços e configurando os termos do produto de software.

   A duração do contrato já foi definida pelo vendedor e não pode ser modificada.
6. Em Opções de contrato, escolha uma quantidade para cada unidade.
7. Veja o preço total do contrato em Detalhes do preço.

   Você também pode ver a oferta pública escolhendo Exibir oferta em Outras ofertas disponíveis.
8. Depois de fazer todas as seleções, escolha Create Contract (Criar contrato).

> **Note**
>
> Pode levar até 10 minutos para que a assinatura seja processada e uma licença seja gerada na conta do AWS License Manager para o produto de software.

Acesso ao software

Para acessar o produto de software baseado na AMI

1. No console do AWS Marketplace, navegue até Exibir assinatura e veja a licença do produto de software.
2. Na página Compras:
   a. Escolha Gerenciar licença para visualizar, conceder acesso e monitorar o uso de seus direitos no AWS License Manager.
   b. Escolha Continue to Configuration (Continuar para configuração).
3. Na página Iniciar, revise a configuração e escolha como você deseja iniciar o software em Escolher ação.
4. Em Escolha um tipo de instância, escolha uma instância do Amazon Elastic Compute Cloud (Amazon EC2) e, em seguida, escolha Avançar: Configurar detalhes da instância.

5. Na página Configurar detalhes da instância, em Perfil do IAM, escolha um perfil existente do AWS Identity and Access Management (IAM) na sua Conta da AWS.

   Se você não tiver um perfil do IAM, escolha o link Criar novo perfil do IAM manualmente e siga as instruções.

   > **Note**
   >
   > Quando você compra um produto com preços contratuais, uma licença é criada pelo AWS Marketplace na Conta da AWS que o software pode verificar usando a API do Gerenciador de licenças. Você precisará de um perfil do IAM para iniciar uma instância do produto baseado na AMI.
   > As seguintes permissões do IAM são obrigatórias na política do IAM.
   >
   > ```
   > {
   >    "Version":"2012-10-17",
   >    "Statement":[
   >       {
   >          "Sid":"VisualEditor0",
   >          "Effect":"Allow",
   >          "Action":[
   >             "license-manager:CheckoutLicense",
   >             "license-manager:GetLicense",
   >             "license-manager:CheckInLicense",
   >             "license-manager:ExtendLicenseConsumption",
   >             "license-manager:ListReceivedLicenses"
   >          ],
   >          "Resource":"*"
   >       }
   >    ]
   > }
   > ```

6. Depois que os detalhes da instância estiverem configurados, escolha Revisar e iniciar.
7. Na página Revisar execução da instância, selecione um par de chaves existente ou crie um novo e escolha Executar instâncias.

   A janela de progresso Iniciando execuções de instância é exibida.
8. Depois que a instância for iniciada, acesse o painel do EC2 e, em Instâncias, veja se o Estado da instância exibe Executando.

Visualização de uma licença gerada

Para visualizar uma licença gerada

1. Faça login no AWS License Manager com sua Conta da AWS.
2. Em Licenças concedidas, veja todas as licenças concedidas.
3. Pesquise licenças inserindo o SKU, o destinatário ou o status do produto na barra Pesquisar.
4. Escolha o ID da licença e veja os Detalhes da licença.
5. Você pode visualizar o Emissor (AWS/Marketplace) e os Direitos (as unidades às quais a licença concede o direito de usar, acessar ou consumir uma aplicação ou recurso).

Modificação de um contrato existente

Se já tiverem um compromisso inicial com um produto da AMI, os compradores do AWS Marketplace podem modificar alguns aspectos de um contrato. Um contrato de AMI é suportado por meio de ofertas baseadas em termos contratuais, em vez de ofertas de preços flexíveis de consumo (FCP) por hora ou por ano. Esse recurso está disponível somente para aplicações integradas ao AWS License Manager. Os compradores podem comprar licenças adicionais dentro do direito à mesma oferta no contrato atual. No entanto, os compradores não podem reduzir o número de direitos adquiridos no contrato. Os compradores também poderão cancelar a renovação automática da assinatura se a opção for habilitada pelo vendedor.

> **Note**
>
> Uma oferta de contrato de cronograma de pagamento flexível (FPS) não pode ser modificada. Não há alterações de direito disponíveis para o comprador de um contrato adquirido por FPS. Um direito é o direito de usar, acessar ou consumir uma aplicação ou recurso. As ofertas de FPS não podem ser alteradas.

Gerenciar sua assinatura

1. No console do AWS Marketplace, navegue até Exibir assinatura e veja a licença do produto de software.
2. Na página Compras, selecione Gerenciar licença.
3. Na lista, selecione Visualizar termos.

4. Na seção Opções de contrato, aumente seus direitos usando as setas. Não é possível reduzir a contagem de direitos abaixo dos direitos adquiridos.
5. Os detalhes do contrato e o preço total são exibidos na seção Detalhes do preço.

Para cancelar a renovação automática da assinatura

1. No console do AWS Marketplace, navegue até Exibir assinatura e veja a licença do produto de software.
2. Na página Compras, selecione Gerenciar licença.
3. Na página Assinatura, localize a seção Configurações de renovação.
4. Entenda os termos e condições com o cancelamento.
5. Marque a caixa de seleção para cancelar a renovação automática.

Produtos de AMI habilitados para medição

Alguns produtos listados no AWS Marketplace são cobrados por uso medidos pelo aplicativo de software. Entre os exemplos de dimensões de uso estão uso de dados, de host/agente ou largura de banda. Esses produtos exigem configuração extra para funcionar corretamente. Um perfil do IAM com a permissão para medir o uso deve ser associada à instância do AWS Marketplace Amazon Elastic Compute Cloud (Amazon EC2) no momento da execução. Para obter mais informações sobre perfis do IAM para o Amazon EC2, consulte Perfis do IAM para o Amazon EC2.

Marcação de alocação de custos em produtos de AMI

O AWS Marketplace oferece suporte à marcação de alocação de custos para produtos de software baseados em imagem de máquina da Amazon (AMI). As tags de instância novas e existentes do Amazon Elastic Compute Cloud (Amazon EC2) são preenchidas automaticamente com base no uso correspondente da AMI do AWS Marketplace. Você pode usar tags de alocação de custos ativadas para identificar e rastrear o uso da AMI por meio do AWS Cost Explorer, do Relatório de custos e uso da AWS, de Orçamentos da AWS ou de outras ferramentas de análise de gastos na nuvem.

O fornecedor que forneceu a AMI também pode registrar outras tags personalizadas na medição de produtos baseados em AMI, com base nas informações específicas do produto. Para obter mais detalhes, consulte Marcação de alocação de custo.

Você pode usar tags para organizar os seus recursos e tags de alocação de custos para acompanhar os custos da AWS em um nível detalhado. Depois de ativar as tags de alocação de custos, a AWS as usa para organizar seus custos de recursos no relatório de alocação de custos, para facilitar a categorização e o controle dos custos da AWS.

A marcação de alocação de custos só rastreará os custos a partir do momento em que as tags foram ativadas no console do Billing and Cost Management. Somente os proprietários de Conta da AWS, os proprietários de contas de gerenciamento do AWS Organizations e usuários com as permissões apropriadas podem acessar o console do Billing and Cost Management de uma conta. Independentemente de você usar a marcação de alocação de custos, não há alteração no valor cobrado. Usar ou não tags de alocação de custos não afeta a funcionalidade de seus produtos de software baseados em AMI.

Rastrear tags de alocação de custos para uma AMI em várias instâncias

Cada instância do Amazon EC2 executada para uma assinatura de AMI do AWS Marketplace tem um item de linha de uso de software do AWS Marketplace correspondente no Relatório de custos e uso da AWS. O uso que você fizer do AWS Marketplace sempre refletirá as tags específicas aplicadas à instância correspondente do Amazon EC2. Isso permite que você diferencie seus custos de uso do AWS Marketplace com base nos diferentes valores de tag que foram atribuídos, no nível de instância.

Também é possível somar seus custos de uso baseados em tag para igualar a cobrança de uso de software da AMI refletida na sua fatura com o Cost Explorer ou o Relatório de custos e uso da AWS.

Encontrar orçamentos com instâncias marcadas de custos alocados

Se você já tem orçamentos ativos filtrados por tags de alocação de custos em várias instâncias do Amazon EC2 no console do Billing and Cost Management , pode ser difícil encontrar todos eles. O script Python a seguir retorna uma lista de orçamentos que contêm instâncias do Amazon EC2 do AWS Marketplace na Região da AWS atual.

Você pode usar esse script para estar ciente de um possível impacto em seu orçamento e onde excedentes podem ocorrer com essa alteração. Observe que o valor faturado não muda, mas as alocações de custos serão refletidas com mais precisão, o que pode afetar os orçamentos.

```
#! /usr/bin/python

import boto3
```

```
session = boto3.Session()
b3account=boto3.client('sts').get_caller_identity()['Account']
print("using account {} in region {}".format(b3account,session.region_name))


def getBudgetFilters(filtertype):
    '''
    Returns budgets nested within the filter values [filter value][budeget name].
    The filtertype is the CostFilter Key such as Region, Service, TagKeyValue.
    '''
    budget_client = session.client('budgets')
    budgets_paginator = budget_client.get_paginator('describe_budgets')
    budget_result = budgets_paginator.paginate(
        AccountId=b3account
    ).build_full_result()
    returnval = {}
    if 'Budgets' in budget_result:
        for budget in budget_result['Budgets']:
            for cftype in budget['CostFilters']:
                if filtertype == cftype:
                    for cfval in budget['CostFilters'][cftype]:
                        if cfval in returnval:
                            if not budget['BudgetName'] in returnval[cfval]:
                                returnval[cfval].append(budget['BudgetName'])
                        else:
                            returnval[cfval] = [ budget['BudgetName'] ]
    return returnval

def getMarketplaceInstances():
    '''
    Get all the AWS EC2 instances which originated with AWS Marketplace.
    '''
    ec2_client = session.client('ec2')
    paginator = ec2_client.get_paginator('describe_instances')
    returnval = paginator.paginate(
        Filters=[{
            'Name': 'product-code.type',
            'Values': ['marketplace']
        }]
    ).build_full_result()
    return returnval


def getInstances():
```

```
    mp_instances = getMarketplaceInstances()
    budget_tags = getBudgetFilters("TagKeyValue")
    cost_instance_budgets = []
    for instance in [inst for resrv in mp_instances['Reservations'] for inst in
 resrv['Instances'] if 'Tags' in inst.keys()]:
        for tag in instance['Tags']:
            # combine the tag and value to get the budget filter string
            str_full = "user:{}${}".format(tag['Key'], tag['Value'])
            if str_full in budget_tags:
                for budget in budget_tags[str_full]:
                    if not budget in cost_instance_budgets:
                        cost_instance_budgets.append(budget)
    print("\r\nBudgets containing tagged Marketplace EC2 instances:")
    print( '\r\n'.join([budgetname for budgetname in cost_instance_budgets]) )


if __name__ == "__main__":
    getInstances()
```

Exemplo de saída

```
Using account 123456789012 in region us-east-2

Budgets containing tagged Marketplace EC2 instances:
EC2 simple
MP-test-2
```

Tópicos relacionados

Para obter mais informações, consulte os tópicos a seguir:

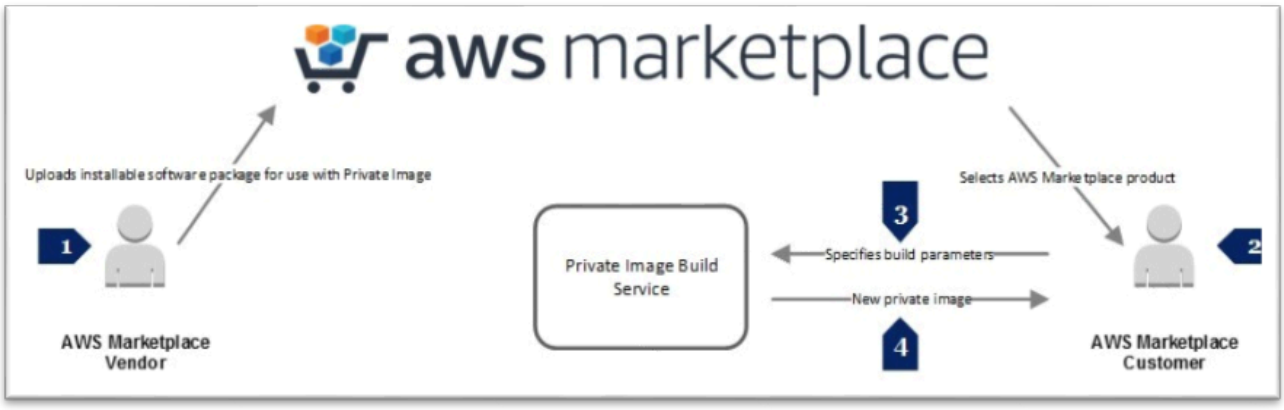
- Usar tags de alocação de custos no Guia do usuário do AWS Billing.
- Ativar as tags de alocação de custos geradas pela AWS no Guia do usuário do AWS Billing.
- Marcar recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias do Linux.

Criação de imagens privadas

> **Important**
>
> O AWS Marketplace interromperá o método de entrega do Private Image Build em abril de 2024.
>
> Até abril de 2024, os assinantes existentes do Private Image Build podem criar novas imagens de máquina da Amazon (AMIs) douradas ou atualizar a AMI dourada com o software fornecido no método de entrega do Private Image Build. Após a descontinuação, eles não poderão criar ou atualizar sua própria AMI com o software Private Image Build. As AMIs existentes criadas anteriormente usando o Private Image Build não são afetadas. Isso significa que as AMIs criadas usando o Private Image Build podem continuar sendo cobradas e executadas usando o Amazon Elastic Compute Cloud (Amazon EC2) e as instâncias ativas continuarão sendo executadas da mesma forma que funcionam atualmente.
>
> Além disso, o software anteriormente disponível apenas como Private Image Build agora está disponível por meio da opção autônoma de execução da AMI, que não será descontinuada. A AMI autônoma ainda pode ser usada com sua assinatura existente do Private Image Build após a descontinuação do Private Image Build. Em caso de dúvidas, entre em contato com AWS Support.

O AWS Marketplace Private Image Build permite comprar produtos de software instaláveis por meio do AWS Marketplace e instalá-los em uma imagem gold ou em uma AMI escolhida dentre as imagens disponíveis para a conta da AWS. Para fins deste conteúdo, imagem gold é uma imagem do servidor que inclui um Operating System (OS –Sistema operacional) base com modificações aplicadas, de maneira que cada servidor iniciado a partir dessa imagem siga os padrões de TI definidos. Escolha o software no AWS Marketplace que deseja instalar e a AMI base para a compilação. Em seguida, você usa o AWS Marketplace Image Build Service para criar e fornecer uma nova AMI como uma imagem privada disponível apenas para a conta da AWS.

Esse serviço ajuda a atender melhor aos requisitos internos de segurança, conformidade e gerenciamento, permitindo executar produtos do AWS Marketplace em um sistema operacional base que atenda aos padrões de TI.



Os vendedores participantes do AWS Marketplace Private Image Build criam versões instaláveis do produto para plataformas de sistema operacional, sistemas operacionais e versões de SO específicas. Quando um vendedor envia um conjunto de pacotes de software para o produto, o AWS Marketplace Image Build Service instala e verifica o produto no OS especificado antes da publicação do produto no AWS Marketplace. Ao comprar um produto habilitado para o AWS Marketplace Private Image Build, você pode escolher uma AMI existente para criar uma nova imagem privada. Assim que você tiver usado o AWS Marketplace Image Build Service para criar uma nova imagem, ele será disponibilizado no console do Amazon EC2 como uma imagem própria. Crie uma imagem usando o site do AWS Marketplace ou use a API do AWS Marketplace Image Build Service.

Há uma cobrança de software e infraestrutura para os Serviços da AWS usados para concluir o processo de compilação, o que pode levar de 1 a 2 horas, dependendo do produto. No entanto, não há custo adicional para usar o AWS Marketplace Image Build Service a fim de criar imagens privadas. Depois que a imagem for criada, você não incorrerá em cobranças de uso do recurso da AWS até usar o produto.

O AWS Marketplace Private Image Build usa o AWS Identity and Access Management (IAM) para criar perfis do IAM e políticas que concedam permissões limitadas a usuários finais para criar e exibir imagens privadas. Concluir as etapas obrigatórias exige privilégios de nível administrativo.

Concluir etapas de pré-requisito

> **Important**
>
> O AWS Marketplace interromperá o método de entrega do Private Image Build em abril de 2024. O método de entrega só está disponível para assinantes existentes até que seja descontinuado. Para obter mais informações, consulte Private image build.

As etapas de pré-requisito descritas aqui exigem permissões de nível administrativo que configuram o AWS Identity and Access Management (IAM) de maneira que seja possível conceder a capacidade de criar imagens privadas a outros usuários. Depois que as políticas e os perfis do IAM forem criados, anexe-os às contas de grupo (ou usuário), de maneira que os usuários associados possam criar imagens privadas.

O IAM é um serviço da Web que ajuda você a controlar o acesso aos recursos da AWS de forma segura. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos. Crie identidades (usuários, grupos e funções) e adicione os usuários aos grupos, de maneira que seja possível gerenciar grupos, em vez de usuários individuais. Um perfil do IAM é semelhante a um usuário por ser uma identidade com políticas de permissões que determinam o que a identidade pode e não pode fazer na AWS. No entanto, uma função não tem credenciais (senha ou chaves de acesso) associadas. Em vez de ser exclusivamente associada a uma pessoa, uma função destina-se a ser assumível por qualquer pessoa que precisar. Um usuário pode assumir temporariamente uma função para adquirir permissões diferentes para uma tarefa específica.

A parte de gerenciamento de acesso do IAM ajuda a definir o que um usuário ou outra entidade pode fazer em uma conta, normalmente conhecido como autorização. As permissões são concedidas por meio de políticas. Uma política é uma entidade da AWS que, quando associada a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma principal, como um usuário, faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. As políticas são armazenadas na AWS como documentos JSON anexados a entidades principais como políticas baseadas em identidade ou a recursos como políticas baseadas em recursos. Você concede permissões definindo políticas de permissão e atribuindo a política a um grupo.

Políticas baseadas em identidade são políticas de permissão que você pode anexar a uma entidade principal (ou identidade), como um usuário, função ou grupo. As políticas baseadas em recursos são documentos de política JSON anexados a um recurso, como um bucket do Amazon Simple Storage Service (Amazon S3). As políticas baseadas em identidade controlam quais ações cada identidade pode realizar, em quais recursos e em que condições. As políticas baseadas em identidade podem ser categorizadas em políticas gerenciadas pela AWS, políticas gerenciadas pelo cliente e políticas em linha.

As Políticas baseadas em recurso controlam quais ações uma entidade principal pode realizar nesses recursos, e em que condições. As políticas baseadas em recursos são políticas em linha, e não há políticas gerenciadas que sejam baseadas em recurso. Embora as identidades do IAM sejam tecnicamente recursos da AWS, não é possível anexar uma política baseada em recurso

a uma identidade do IAM. Use políticas baseadas em identidade no IAM. Políticas de confiança são políticas baseadas em recursos anexadas a uma função que define quais entidades principais podem assumir a função. Quando você cria uma função no IAM, ela deve ter dois itens: uma política de confiança que indique quem pode assumir a função e uma política de permissão que indique o que pode ser feito com essa função. Lembre-se de que adicionar uma conta à política de confiança de uma função é apenas metade da tarefa de estabelecer o relacionamento de confiança. Por padrão, nenhum usuário nas contas confiáveis pode assumir a função até que o administrador da conta em questão conceda aos usuários a permissão para assumir a função.

O serviço de criação de imagens do AWS Marketplace usa duas funções do IAM, e cada função tem uma política de permissões e uma política de confiança. Se você tiver usuários com acesso ao site do AWS Marketplace para criar imagens privadas, esses usuários também precisarão de permissões do IAM para listar e atribuir as funções necessárias para criar e exibir as imagens privadas criadas por eles.

Como administrador, você cria duas funções obrigatórias e as políticas associadas. A primeira função é um perfil de instância anexado à instância criada durante o processo de criação de imagens. Perfil de instância é um contêiner para uma função do IAM que pode ser usada para passar informações da função para uma instância do Amazon EC2 quando a instância é iniciada. A segunda é um perfil do IAM que dá acesso ao AWS Systems Manager e ao Amazon EC2. Para configurar o perfil de instância, anexe uma política de permissão que ofereça as permissões obrigatórias. Em seguida, edite a política de confiança da função para conceder permissão para o Amazon EC2 e o Systems Manager assumirem a função.

Criar uma função de perfil de instância

Para criar a função de perfil de instância por meio do console do IAM

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, escolha Roles (Funções) e Criar função (Create role).
3. Em Select type of trusted entity (Selecionar tipo de entidade confiável), escolha AWS service (Serviço da AWS).
4. Em Choose the service that will use this role (Escolher o serviço que usará esta função), selecione EC2 e Next: Permissions (Próximo: permissões).
5. Em Create policy (Criar política), escolha Next: Review (Próximo: examinar).

6. Em Nome da função, digite o nome de uma função ou o sufixo de nome de uma função para ajudar a identificar a finalidade dessa função, por exemplo, **`MyInstanceRole`**. Os nomes de função devem ser exclusivos em sua Conta da AWS.
7. Revise a função e escolha Create role (Criar função).
8. Na página Roles (Funções), escolha a função criada.
9. Em Permissions (Permissões), escolha Add inline policy (Adicionar política em linha).
10. Escolha a guia JSON e substitua todo o texto pelo seguinte texto `InstanceRolePermissionsPolicy`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:GetDocument",
                "ssm:GetManifest",
                "ssm:GetParameters",
                "ssm:ListAssociations",
                "ssm:ListInstanceAssociations",
                "ssm:PutConfigurePackageResult",
                "ssm:UpdateAssociationStatus",
                "ssm:UpdateInstanceAssociationStatus",
                "ssm:UpdateInstanceInformation"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2messages:AcknowledgeMessage",
                "ec2messages:DeleteMessage",
                "ec2messages:FailMessage",
                "ec2messages:GetEndpoint",
                "ec2messages:GetMessages",
                "ec2messages:SendReply"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
```

```
            "Action": [
                "ec2:DescribeInstanceStatus"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> Antes de começar esse processo, você deve criar o bucket do S3, *DOC-EXAMPLE-BUCKET*.

11 Escolha Review policy (Revisar política).

12 Em Nome da política, digite um nome para ajudar a identificar a finalidade dessa política, por exemplo, **`MyInstanceRolePolicy`** e escolha Criar política.

Para editar a relação de confiança da função

1. Na página Roles (Funções), escolha a função criada.
2. Escolha a guia Trust relationships (Relações de confiança) e Edit trust relationship (Editar relação de confiança).
3. Selecione todo o texto na caixa de texto Documento de política e o substitua pelo seguinte `InstanceRoleTrustPolicy`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": [
          "ssm.amazonaws.com",
          "ec2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Escolha Update Trust Policy.

Criação de uma função de automação do AWS Systems Manager

Para criar a função de automação do AWS Systems Manager

1. No painel de navegação do console do IAM, escolha Roles (Funções) e Criar função (Create role).
2. Em Select type of trusted entity (Selecionar tipo de entidade confiável), escolha AWS service (Serviço da AWS).
3. Em Choose the service that will use this role (Escolher o serviço que usará esta função), selecione EC2 e Next: Permissions (Próximo: permissões).
4. Em Create policy (Criar política), escolha Next: Review (Próximo: examinar).
5. Em Nome da função, digite o nome de uma função ou o sufixo de nome de uma função para ajudar a identificar a finalidade dessa função, por exemplo, **`MyAutomationRole`**. Os nomes de função devem ser exclusivos em sua Conta da AWS.
6. Revise a função e escolha Create role (Criar função).
7. Na página Roles (Funções), escolha a função criada.
8. Em Permissions (Permissões), escolha Add inline policy (Adicionar política em linha).
9. Escolha a guia JSON e substitua todo o texto pelo seguinte texto `AutomationRolePermissionsPolicy`.

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:*"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:CreateImage",
                "ec2:DescribeImages",
                "ec2:StartInstances",
                "ec2:RunInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:CreateTags",
                "ec2:DescribeTags"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "{{ Instance Profile }}"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Note

Substitua `{{ Instance Profile }}` pelo nome do recurso da Amazon (ARN) da função de política da instância criada anteriormente. Localize a função no console de gerenciamento do IAM e a escolha. Na página de resumo da função, ARN da função

é o primeiro item listado, por exemplo, `arn:aws:iam::123456789012:role/MyInstanceRole`.

Para editar a relação de confiança da função

1. Na página Roles (Funções), escolha a função criada.
2. Escolha a guia Trust relationships (Relações de confiança) e Edit trust relationship (Editar relação de confiança).
3. Substitua todo o texto na caixa de texto Documento de política pelo seguinte `InstanceRoleTrustPolicy`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm.amazonaws.com",
          "ec2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Escolha Update Trust Policy.

Você já criou as duas funções e as políticas associadas que você usará durante o processo de criação da imagem privada.

Usar uma política para acessar o site do AWS Marketplace

A maioria das organizações não permite que os usuários façam login usando credenciais da conta raiz. Em vez disso, elas criam usuários com permissões limitadas com base em funções organizacionais ou tarefas que somente determinadas pessoas podem realizar. O AWS Marketplace fornece duas políticas principais gerenciadas pelo IAM para trabalhar com ferramentas do AWS

Marketplace. Use essas duas políticas gerenciadas para oferecer a capacidade de realizar as tarefas descritas:

- `AWSMarketplaceFullAccess`: oferece a capacidade de assinar e cancelar a assinatura do software IAM, permite que os usuários gerenciem instâncias de software do AWS Marketplace na página Seu software do AWS Marketplace e fornece acesso administrativo ao Amazon EC2.
- `AWSMarketplaceRead-only`: oferece a capacidade de revisar assinaturas da AWS.

Adicione a política gerenciada chamada `AWSMarketplaceFullAccess` a um usuário, grupo ou função para fornecer todas as permissões necessárias para acessar o site do AWS Marketplace e executar as tarefas associadas à criação de imagens privadas do AWS Marketplace.

Para fornecer o 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.

Na próxima vez em que acessar o site do AWS Marketplace, um usuário ou um membro de um grupo ou função selecionada poderá realiza as tarefas associadas ao processo de criação da imagem privada.

Criar uma imagem privada

> **Important**
>
> O AWS Marketplace interromperá o método de entrega do Private Image Build em abril de 2024. O método de entrega só está disponível para assinantes existentes até que seja descontinuado. Para obter mais informações, consulte Private image build.

Ao criar uma imagem privada, selecione o pacote de software no AWS Marketplace e a imagem de máquina da Amazon (AMI) base no console do Amazon Elastic Compute Cloud (Amazon EC2) que você usará para criar a nova imagem privada. Antes de iniciar o processo de criação, configure o ambiente da AWS de maneira que possa fornecer:

- O ID da AMI da imagem base em que você instalará o produto do AWS Marketplace.
- O nome de um bucket do Amazon Simple Storage Service (Amazon S3) no qual armazenar os logs de criação. O bucket do S3 deve estar na Região da AWS onde a AMI estará disponível.
- O perfil de instância do Amazon EC2 com que o pacote será instalado (consulte a seção anterior).
- A função de automação do AWS Identity and Access Management (IAM) que o processo de criação de imagem usará para criar a AMI (consulte a seção anterior).
- O nome da nova imagem privada.

Se tiver experiência usando os Serviços da AWS, você provavelmente terá familiaridade com a escolha de Regiões da AWS, a localização do ID da AMI no painel do Amazon EC2 e o trabalho com buckets do Amazon S3.

Para encontrar um produto que oferece suporte à criação de uma imagem privada, acesse a página de pesquisa de produtos do AWS Marketplace e, para o filtro de pesquisa do Método de entrega, escolha Imagem de máquina da Amazon privada. Na página de detalhes do produto, você configura opções de aquisição, configuração e cumprimento. O produto criado é adicionado à Conta da AWS.

Além dos pré-requisitos especificados na seção anterior, a AMI base deve atender aos seguintes requisitos:

- As AMIs do Linux devem ter `Wget` ou `cURL` instalado e configurado. Windows As AMIs devem ter o PowerShell instalado.

- As AMIs do Linux devem ser capazes de executar Scripts de dados do usuário do EC2 ou ter o agente AWS Systems Manager (SSM Agent) pré-instalado.
- As AMIs do Windows devem ter o SSM Agent pré-instalado.

Para criar uma imagem privada

1. No AWS Marketplace, na página de detalhes do produto, escolha Continuar para assinatura.
2. Na página Subscribe to this software (Assinar este software), em Terms and Conditions (Termos e condições), escolha Show Details (Mostrar detalhes) para exibir o tipo de instância do produto, os custos de uso do software e o End User License Agreement (EULA – Contrato de licença do usuário final). Dependendo do produto, convém ver vários tipos de assinaturas. Depois que você escolher o tipo de assinatura, escolha Aceitar termos.
3. Escolha Continue to Configuration (Continuar para configuração).
4. Na página Configure this software (Configurar este software), em Fulfillment Option (Opção de cumprimento), escolha Private Amazon Machine Image (Imagem de máquina da Amazon privada).
5. Na seção Imagem privada, em 1. Escolher uma região, escolha a região. Em 2. Escolher uma imagem privada para execução, escolha Criar nova imagem privada.
6. Na seção Create New Private Image (Criar nova imagem privada), em Select a base AMI to use (Selecionar uma AMI base a ser usada), escolha Owned by me (Minha propriedade), Public Images (Imagens públicas) ou Private images (Imagens privadas).
   a. Minha propriedade: AMIs especificamente pertencentes à Conta da AWS
   b. Imagens públicas: AMIs que foram compartilhadas com todas as Contas da AWS
   c. Imagens privadas: AMIs que foram compartilhadas com a Conta da AWS
7. Em ID da AMI base pública de entrada ou ID da AMI base privada de entrada, insira o ID da AMI ou use o console do Amazon EC2 para copiar e colar o ID da AMI da imagem que você deseja usar como a AMI base.
8. Em Instance Profile (Perfil da instância), escolha a função da instância criada como uma etapa de pré-requisito.
9. Em Automation Role (Função da automação), escolha a função da automação criada como uma etapa de pré-requisito.
10. Em Build Logs (Logs de criação), digite o nome de um bucket do Amazon S3 em que você deseja armazenar. Este é o nome do bucket simples; por exemplo, *DOC-EXAMPLE-BUCKET*, em vez de todo o nome DNS.
11. Em Private Image Name (Nome da imagem privada), digite o nome da nova imagem privada.

Recomendamos usar uma convenção de nomenclatura para as imagens privadas criadas a fim de facilitar a identificação de imagens. Além disso, ao criar uma nova imagem privada, o AWS Marketplace Image Building Service adiciona uma tag AWSMarketplaceFulfillmentID, que poderá ser útil depois para identificar as imagens privadas posteriormente. Também conclua as etapas opcionais a seguir para fornecer detalhes adicionais ou iniciar o processo de criação escolhendo Start Build (Iniciar criação).

(Opcional) Para fornecer detalhes adicionais sobre a imagem privada

1. Em Observações da descrição, insira todas as informações relevantes que você deseja incluir na instância que será usada durante a criação da imagem privada.
2. Em Instance Type (Tipo de instância), escolha o tipo de instância que você deseja usar ao criar a imagem privada.
3. Em VPC, escolha a VPC que você deseja que a instância use ao criar a imagem privada e o grupo de segurança e a sub-rede.
4. Em Enable Simple Notification System (Habilitar sistema de notificação simples), escolha um tópico existente ou criar um novo tópico para receber notificações quando o status da alteração mudar.
5. Escolha Start Build (Iniciar criação).

O processo de criação leva de 1 a 2 horas para ser concluído. Observe as seguintes informações sobre o processo:

- As cobranças de serviços usados durante o processo de criação serão exibidas na Conta da AWS usada para iniciar o processo de criação da imagem privada. Isso inclui a instância executada enquanto o produto do AWS Marketplace está sendo instalado na imagem privada e o bucket do S3 usado em logs.
- Exiba o status do processo de criação ou receba mensagens do Amazon Simple Notification Service (Amazon SNS).
- Depois que a criação for concluída, a nova imagem privada será adicionada à Conta da AWS e estará disponível por meio do console do Amazon EC2 como uma AMI listada em Minha propriedade.
- Os repositórios usados para concluir o processo de criação devem ser locais.
- Durante a criação, o processo bloqueia o acesso à Internet.

Sobre aliases de AMI

Uma imagem de máquina da Amazon (AMI) é identificada com um `AMI ID`. Você pode usar o `AMI ID` para indicar qual AMI deseja usar ao executar um produto. O `AMI ID` tem o formato `ami-<identifier>`, por exemplo, ami-123example456. Cada versão de cada produto em cada Região da AWS tem uma AMI diferente (e um `AMI ID` diferente).

Quando você executa um produto no AWS Marketplace, o `AMI ID` é preenchido automaticamente. Você pode usar `AMI ID` se quiser automatizar a execução de produtos no AWS Command Line Interface (AWS CLI) ou usando o Amazon Elastic Compute Cloud (Amazon EC2). Você pode encontrar o `AMI ID` ao configurar o software no momento da inicialização. Para obter mais informações, consulte Etapa 3: configurar o software.

O `Ami Alias` também está no mesmo local do `AMI ID`, ao configurar o software. O `Ami Alias` é um ID semelhante ao `AMI ID`, mas é mais fácil de usar na automação. Um `AMI alias` tem o formato `aws/service/marketplace/prod-<identifier>/<version>`, por exemplo, `aws/service/marketplace/prod-1234example5678/12.2`. Você pode usar esse ID do `Ami Alias` em qualquer região e a AWS vai mapeá-lo automaticamente para o `AMI ID` regional correto.

Se você quiser usar a versão mais recente de um produto, use o termo **`latest`** no lugar da versão no `AMI alias` para que a AWS escolha a versão mais recente do produto para você, por exemplo, **`aws/service/marketplace/prod-1234example5678/latest`**.

> **Warning**
>
> O uso da opção **`latest`** fornece a versão mais recente do software. No entanto, use esse recurso com cuidado. Por exemplo, se um produto tiver as versões 1.x e 2.x disponíveis, você talvez esteja usando 2.x. No entanto, a versão mais recente do produto pode ser uma correção de bug para 1.x.

Exemplos de uso de aliases de AMI

Os aliases da AMI são úteis na automação. Você pode usá-los no AWS CLI ou em modelos do AWS CloudFormation.

O exemplo a seguir mostra como usar um alias de AMI para executar uma instância usando o AWS CLI.

```
aws ec2 run-instances
--image-id resolve:ssm:/aws/service/marketplace/<identifier>/version-7.1
--instance-type m5.xlarge
--key-name MyKeyPair
```

O exemplo a seguir mostra um modelo do CloudFormation que aceita o alias da AMI como parâmetro de entrada para criar uma instância.

```
AWSTemplateFormatVersion: 2010-09-09

Parameters:
    AmiAlias:
        Description: AMI alias
        Type: 'String'

Resources:
    MyEC2Instance:
        Type: AWS::EC2::Instance
        Properties:
            ImageId: !Sub "resolve:ssm:${AmiAlias}"
            InstanceType: "g4dn.xlarge"
            Tags:
                -Key: "Created from"
                 Value: !Ref AmiAlias
```

Produtos de contêiner

Os produtos de contêiner são produtos autônomos fornecidos como imagens de contêineres. Os produtos de contêiner podem ser gratuitos ou devem ser pagos usando uma opção de preço fornecida pelo vendedor. Os produtos de contêiner podem ser usados com vários runtimes e serviços de contêineres, incluindo Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) e até mesmo serviços executados em sua própria infraestrutura. Para obter uma lista completa de serviços e runtimes compatíveis com mais informações sobre cada um, consulte Serviços compatíveis para produtos de contêiner.

Você pode descobrir, assinar e implantar produtos de contêiner no site do AWS Marketplace ou no console do Amazon ECS. Você pode implantar vários produtos no Amazon ECS ou no Amazon EKS usando modelos de implantação fornecidos pelo vendedor, como definições de tarefas ou charts do Helm. Ou você pode acessar imagens de contêiner diretamente dos repositórios privados do Amazon Elastic Container Registry (Amazon ECR) depois de assinar esses produtos.

Se um produto habilitou o QuickLaunch, você pode usá-lo para testar rapidamente produtos de contêiner em um cluster do Amazon EKS com apenas algumas etapas. O QuickLaunch usa o AWS CloudFormation para criar um cluster do Amazon EKS e executar software de contêiner nele. Para obter mais informações sobre como executar com o QuickLaunch, consulte QuickLaunch no AWS Marketplace.

Esta seção fornece informações sobre como encontrar, assinar e lançar produtos de contêiner no AWS Marketplace.

Modelos de definição de preço para produtos de contêiner pagos

Os produtos de contêiner pagos devem ter um ou mais modelos de preços. Como acontece com qualquer outro produto pago no AWS Marketplace, você recebe uma cobrança da AWS pelos produtos de contêiner pagos de acordo com o modelo de preços. O modelo de preços pode ser uma taxa mensal fixa ou um preço por hora, monitorado em segundos e rateado. Os detalhes de preço serão exibidos na página de detalhes e quando você assinar o produto.

Os modelos de preço aceitos para produtos de contêiner no AWS Marketplace são os seguintes:

- Uma cobrança mensal fixa que oferece uso ilimitado.
- Um pagamento adiantado para uso do produto durante um contrato em longo prazo.
- Um modelo de pagamento conforme o uso (normalmente por hora) com base no uso do produto.
- Um modelo de pagamento adiantado com preços contratuais.

Para obter mais informações sobre cada modelo, consulte Preços dos produtos de contêiner no Guia do vendedor do AWS Marketplace.

Visão geral dos contêineres e do Kubernetes

Os contêineres, como os do Docker, são uma tecnologia de software de código aberto que fornece uma camada adicional de abstração e automação em sistemas operacionais virtualizados como Linux e Windows Server. Assim como máquinas virtuais são instâncias de imagens de servidor, os contêineres são instâncias de imagens de contêiner do Docker. Elas encapsulam o software de aplicativo do servidor em um sistema de arquivos que contém todo o necessário para execução: código, tempo de execução, ferramentas de sistema, bibliotecas de sistema etc. Com contêineres, o software sempre funciona da mesma forma, independentemente do ambiente.

De maneira análoga a máquinas virtuais Java, os contêineres exigem uma plataforma subjacente para fornecer uma camada de conversão e orquestração ao mesmo tempo em que permanecem isoladas do mesmo sistema operacional e entre si. Existem runtimes compatíveis com o Docker diferentes e serviços de orquestração que é possível usar com contêineres do Docker, inclusive Amazon ECS, que é um serviço de orquestração altamente dimensionável e de alto desempenho para a AWS, e o Amazon EKS, que facilita implantar, gerenciar e escalar aplicações em contêineres usando Kubernetes, um serviço de gerenciamento de código aberto e orquestração.

Encontrar e assinar produtos de contêiner

Produtos de contêiner são produtos do AWS Marketplace que podem ser executados em imagens de contêiner. Os produtos de contêiner incluem qualquer produto do AWS Marketplace no qual o vendedor tenha fornecido uma opção de execução com um método de entrega Imagem do contêiner, Chart do Helm ou Complemento do Amazon EKS. Para obter mais informações sobre os métodos de entrega de produtos de contêiner, consulte Métodos de entrega de produtos de contêiner.

Muitos ambientes de execução, também conhecidos como serviços suportados, estão disponíveis para opções de execução em produtos de contêiner. Os ambientes de execução incluem serviços como o Amazon Elastic Container Service (Amazon ECS), o Amazon Elastic Kubernetes Service (Amazon EKS) e até sua própria infraestrutura autogerenciada. Para obter uma lista completa dos ambientes de execução de produtos de contêiner disponíveis, consulte Serviços compatíveis para produtos de contêiner.

Procurar produtos de contêiner usando o site do AWS Marketplace

Você pode procurar produtos de contêiner usando o site do AWS Marketplace.

Para procurar produtos de contêiner usando o site do AWS Marketplace

1. Navegue até a página de pesquisa do AWS Marketplace.
2. Filtre o Método de entrega por Imagem do contêiner ou Chart do Helm.
3. (Opcional) Filtre os Serviços compatíveis para restringir os resultados da pesquisa pelos serviços com os quais o produto pode ser executado.

Depois de encontrar um produto de seu interesse, escolha o título para navegar até a página de detalhes do produto.

Página de detalhes do produto de contêiner

Na página de detalhes do produto no AWS Marketplace, você pode encontrar detalhes sobre o produto, incluindo as seguintes informações:

- Visão geral do produto: a visão geral inclui uma descrição do produto e as seguintes informações:
  - A versão do produto que você está visualizando.
  - Um link para o perfil do vendedor.
  - As categorias de produtos às quais esse produto pertence.
  - Os sistemas operacionais compatíveis para executar este software.
  - Os métodos de entrega que estão disponíveis para executar o software.
  - Os serviços suportados nos quais este produto pode ser executado.
- Informações sobre preços: os produtos têm níveis gratuitos, traga a sua própria licença (BYOL), pagamento adiantado com preços contratuais ou pagamento conforme o uso com um preço fixo mensal ou anual ou um preço por hora. Para obter mais informações sobre os modelos de definição de preço, consulte Definição de preço do produto de contêiner.
- Informações de uso: aqui estão incluídas as opções de execução fornecidas pelo vendedor com instruções para iniciar e executar o software. Cada produto deve ter pelo menos uma opção de execução e pode ter até cinco. Cada opção de execução inclui um método de entrega e instruções a serem seguidas para iniciar e executar o software.
- Informações de suporte: esta seção inclui detalhes sobre como obter suporte para o produto e sua política de reembolso.
- Avaliações de clientes: encontre avaliações de outros clientes sobre o produto ou escreva suas próprias.

Para assinar um produto, escolha Continue para assinar na página de detalhes do produto. Para obter mais informações sobre assinatura de produtos, consulte Assinatura de produtos no AWS Marketplace.

Assinatura de produtos no AWS Marketplace

Para usar um produto, você deve assiná-lo primeiro. Na página de assinatura, você pode exibir informações de definição de preço para produtos pagos e acessar o contrato de licença do usuário final (EULA) do software.

Para um produto com preço de contrato de contêiner, selecione o preço do contrato e escolha Aceitar contrato para continuar. Isso cria uma assinatura do produto, que fornece um direito de usar o software. Vai levar um ou dois minutos para a assinatura ser concluída. Depois que receber um direito a um produto pago, você será cobrado quando começar a usar o software. Se cancelar a assinatura sem encerrar todas as instâncias em execução do software, você continuará sendo cobrado por um eventual uso de software. Você também pode incorrer em custos de infraestrutura relacionados ao uso do produto. Por exemplo, se criar um novo cluster do Amazon EKS para hospedar o produto de software, você será cobrado por esse serviço.

> **Note**
>
> Para ver um passo a passo sobre como assinar e implantar um produto baseado em contêiner, você também pode consultar os vídeos a seguir:
>
> - Implantação de contêineres do AWS Marketplace em clusters do Amazon ECS (3:34)
> - Implantação de produtos do AWS Marketplace baseados em contêineres usando o Amazon ECS Anywhere (5:07)
> - Gerenciamento de complementos do Amazon EKS

Métodos de entrega de produtos de contêiner

Um produto do AWS Marketplace será considerado um produto de contêiner se o vendedor tiver fornecido uma opção de execução com um método de entrega Imagem do contêiner, Chart do Helm ou Complemento do Amazon EKS.

Método de entrega Imagem do contêiner

Para uma opção de execução com um método de entrega Imagem de contêiner, use as instruções fornecidas pelo vendedor para executar o produto. Isso é feito ao extrair imagens do Docker diretamente do registro do AWS Marketplace no Amazon Elastic Container Registry. Para obter mais informações sobre como executar com esse método de entrega, consulte Execução com uma opção de execução de imagens de contêiner.

Método de entrega Chart do Helm

Para uma opção de execução com um método de entrega Chart do Helm, use as instruções fornecidas pelo vendedor ou o modelo de implantação para executar o produto. Isso é feito instalando um chart do Helm usando a CLI do Helm. Você pode executar a aplicação em um cluster

existente do Amazon EKS ou um cluster autogerenciado no EKS Anywhere, no Amazon Elastic Compute Cloud (Amazon EC2) ou on-premises. Para obter mais informações sobre como executar com esse método de entrega, consulte Execução com a opção Helm.

Método de entrega Complemento do Amazon EKS

Para uma opção de execução com um método de entrega Complemento do Amazon EKS, use o console do Amazon EKS ou a CLI do Amazon EKS para executar o produto. Para obter mais informações sobre os complementos do Amazon EKS, consulte Complementos do Amazon EKS.

Serviços compatíveis para produtos de contêiner

A lista a seguir inclui todos os serviços compatíveis com produtos de contêiner no AWS Marketplace. Um serviço compatível é um serviço ou ambiente de contêiner em que o produto pode ser executado. Um produto de contêiner deve incluir pelo menos uma opção de execução que inclua um método de entrega com instruções para ser executado em um ou mais ambientes.

Amazon ECS

O Amazon Elastic Container Service (Amazon ECS) é um serviço de gerenciamento de contêineres altamente escalável e rápido que pode ser usado para execução, interrupção e gerenciamento de contêineres em um cluster. Os contêineres são definidos em uma definição de tarefa que você usa para executar tarefas individuais ou tarefas em um serviço. Nesse contexto, um serviço é uma configuração que permite executar e manter simultaneamente um número especificado de tarefas em um cluster. Você pode executar tarefas e serviços em uma infraestrutura sem servidor gerenciada pelo AWS Fargate. Como alternativa, para ter mais controle da infraestrutura, é possível executar tarefas e serviços em um cluster de instâncias do Amazon EC2 que você gerencia.

Para obter mais informações sobre o Amazon ECS, consulte O que é o Amazon Elastic Container Service no no Guia do desenvolvedor do Amazon Elastic Container Service.

Amazon EKS

O Amazon Elastic Kubernetes Service (Amazon EKS) é um serviço gerenciado que você pode usar para executar o Kubernetes na AWS, eliminando a necessidade de instalar e manter seus próprios nós ou painel de controle do Kubernetes. O Kubernetes é um sistema de código aberto para automatizar a implantação, a escalabilidade e o gerenciamento de aplicações em contêineres.

Você pode pesquisar, assinar e implantar software Kubernetes de terceiros usando o console do Amazon EKS. Para obter mais informações, consulte Gerenciamento de complementos do Amazon EKS, no Guia do usuário do Amazon EKS.

Kubernetes autogerenciados

Você pode executar produtos de contêiner em clusters Kubernetes autogerenciados executados no EKS Anywhere, no Amazon ECS Anywhere, no Amazon EC2 ou na infraestrutura on-premises.

O Amazon ECS Anywhere é um recurso do Amazon ECS que você pode usar para executar e gerenciar workloads de contêineres na infraestrutura gerenciada pelo cliente. O Amazon ECS Anywhere se baseia no Amazon ECS para fornecer uma experiência consistente de ferramentas e API em aplicações baseadas em contêiner.

Para obter mais informações, consulte Amazon ECS Anywhere.

EKS Anywhere é um serviço que você pode usar para criar um cluster do Amazon EKS na infraestrutura gerenciada pelo cliente. Você pode implantar o EKS Anywhere como um ambiente local sem suporte ou como um ambiente de qualidade de produção que pode se tornar uma plataforma Kubernetes on-premises compatível.

Para obter mais informações sobre o EKS Anywhere, consulte a documentação do EKS Anywhere.

Procurar produtos de contêiner usando o console do Amazon ECS

Também encontre produtos de contêiner no console do Amazon ECS. O painel de navegação tem links para descobrir novos produtos do AWS Marketplace e para ver as assinaturas existentes.

Cancelar uma assinatura

Para cancelar a assinatura de um produto, use a página Your Software (Seu software).

Produtos de contêiner com preços contratuais

Alguns vendedores oferecem produtos de software baseados em contêineres públicos com um modelo de preços contratuais, no qual você concorda em fazer um pagamento adiantado único por quantidades discretas de licenças para acessar o produto de software pelo período de sua preferência, que são cobradas antecipadamente na sua Conta da AWS.

Example de comprar diferentes tipos de licenças em quantidades diferentes

Por exemplo, você pode comprar 10 licenças de acesso de usuário e cinco licenças administrativas por um ano. Você pode optar por renovar as licenças automaticamente.

Além disso, algumas empresas oferecem produtos de software privados baseados em contêiner com um modelo de preços contratuais. Uma oferta privada normalmente tem uma duração fixa que não pode ser alterada.

Você pode comprar um contrato de produto de software baseado em contêiner usando a página de detalhes do produto no AWS Marketplace. Se essa opção estiver disponível, AMI com preço contratual será exibido para Método de entrega na página de detalhes do produto. Quando fizer a compra, você será direcionado para o site do produto para instalação e configuração da conta. As cobranças de uso acabarão sendo exibidas no relatório de faturamento da Conta da AWS regular.

Assinatura de um produto de contêiner com oferta pública de preços contratuais no AWS Marketplace

Para assinar uma oferta pública de produto baseado em contêiner com um modelo de preço contratual

> **Note**
>
> Para obter informações sobre a assinatura usando o Amazon EKS, consulte Gerenciamento de complementos do Amazon EKS.

1. Faça login no AWS Marketplace e encontre um produto de software baseado em contêineres com um modelo de preços contratuais.
2. Na página Compras, veja as Informações de preços.

   Você pode ver as Unidades e a taxa de cada duração (em meses).
3. Para iniciar a assinatura, escolha Continue para assinar.

   Para salvar este produto sem assinar, escolha Salvar na lista.
4. Crie um contrato revisando as informações de preços e configurando os termos do produto de software.

   a. Escolha a duração do contrato: 1 mês, 12 meses, 24 meses ou 36 meses.
   b. Em Configurações de renovação, escolha se deseja renovar automaticamente o contrato.
   c. Em Opções de contrato, escolha uma quantidade para cada unidade.

   O preço total do contrato é exibido em Detalhes do preço.

5. Depois de fazer todas as seleções, escolha Criar contrato.

O Preço total do contrato é cobrado na sua Conta da AWS e uma licença é gerada no AWS License Manager.

> **Note**
>
> Pode levar até 10 minutos para que a assinatura seja processada e uma licença seja gerada na conta do Gerenciador de licença para o produto de software.

Assinatura de um produto de contêiner com oferta privada de preços contratuais no AWS Marketplace

Para assinar uma oferta privada de produto baseado em contêiner com um modelo de preço contratual

> **Note**
>
> Para obter informações sobre a assinatura usando o Amazon EKS, consulte Gerenciamento de complementos do Amazon EKS.

1. Faça login no AWS Marketplace com sua conta de comprador.
2. Veja a oferta privada.
3. Na página Compras, veja as Informações de preços.

   Você pode ver as Unidades e a taxa de cada duração (em meses).
4. Escolha Continue para assinar para iniciar a assinatura.
5. Crie um contrato revisando as informações de preços e configurando os termos do produto de software.

   A duração do contrato já foi definida pelo vendedor e não pode ser modificada.
6. Em Opções de contrato, escolha uma quantidade para cada unidade.
7. Veja o preço total do contrato em Detalhes do preço.

   Você também pode ver a oferta pública escolhendo Exibir oferta em Outras ofertas disponíveis.

8. Depois de fazer todas as seleções, escolha Criar contrato.

> **Note**
>
> Pode levar até 10 minutos para que a assinatura seja processada e uma licença seja gerada na conta do Gerenciador de licença para o produto de software.

Acesso ao software

Para acessar o produto de software baseado em contêiner

1. No console do AWS Marketplace, navegue até Exibir assinatura e veja a licença do produto de software.
2. Na página Compras:
   a. Escolha Gerenciar licença para visualizar, conceder acesso e monitorar o uso de seus direitos no AWS License Manager.
   b. Escolha Continue to Configuration (Continuar para configuração).
3. Na página Executar, veja os detalhes da imagem do contêiner e siga as instruções fornecidas.

   Ao criar um cluster do Amazon Elastic Container Service (Amazon ECS), você deve adicionar as seguintes permissões do AWS Identity and Access Management (IAM) à política do IAM.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "license-manager:CheckoutLicense",
            "license-manager:GetLicense",
            "license-manager:CheckInLicense",
            "license-manager:ExtendLicenseConsumption",
            "license-manager:ListReceivedLicenses"
         ],
         "Resource":"*"
      }
```

```
    ]
}
```

Visualização de uma licença gerada

Para visualizar uma licença gerada

1. Faça login no AWS License Manager com sua Conta da AWS.
2. Em Licenças concedidas, veja todas as licenças concedidas.
3. Pesquise licenças inserindo o SKU, o destinatário ou o status do produto na barra Pesquisar.
4. Escolha o ID da licença e veja os Detalhes da licença.
5. Você pode visualizar o Emissor (AWS/Marketplace) e os Direitos (as unidades às quais a licença concede o direito de usar, acessar ou consumir uma aplicação ou recurso).

Modificação de um contrato existente

Se já tiverem um compromisso inicial com um produto de contêiner, os compradores do AWS Marketplace podem modificar alguns aspectos de um contrato. Um contrato de contêiner é suportado por meio de ofertas baseadas em termos contratuais, em vez de ofertas de preços flexíveis de consumo (FCP) por hora ou por ano. Esse recurso está disponível somente para aplicações integradas ao AWS License Manager. Os compradores podem comprar licenças adicionais dentro do direito à mesma oferta no contrato atual. No entanto, os compradores não podem reduzir o número de direitos adquiridos no contrato. Os compradores também poderão cancelar a renovação automática da assinatura se a opção for habilitada pelo vendedor.

> **Note**
>
> Uma oferta de contrato de cronograma de pagamento flexível (FPS) não pode ser modificada. Não há alterações de direito disponíveis para o comprador de um contrato adquirido por FPS. Um direito é o direito de usar, acessar ou consumir uma aplicação ou recurso. As ofertas de FPS não podem ser alteradas.

Gerenciar sua assinatura

1. No console do AWS Marketplace, navegue até Exibir assinatura e veja a licença do produto de software.

2. Na página Compras, selecione Gerenciar licença.
3. Na lista, selecione Visualizar termos.
4. Na seção Opções de contrato, aumente seus direitos usando as setas. Não é possível reduzir a contagem de direitos abaixo dos direitos adquiridos.
5. Os detalhes do contrato e o preço total são exibidos na seção Detalhes do preço.

Para cancelar a renovação automática da assinatura

1. No console do AWS Marketplace, navegue até Exibir assinatura e veja a licença do produto de software.
2. Na página Compras, selecione Gerenciar licença.
3. Na página Assinatura, localize a seção Configurações de renovação.
4. Entenda os termos e condições com o cancelamento.
5. Marque a caixa de seleção para cancelar a opção de renovação automática.

Execução do software de contêiner no AWS Marketplace

Depois de ter uma assinatura ativa de um produto de contêiner no AWS Marketplace, a próxima etapa é executar o software. Para executar o software, siga as instruções incluídas em uma das opções de execução fornecidas pelo vendedor. No AWS Marketplace, uma opção de execução é um procedimento opcional fornecido pelo vendedor para executar o produto em seu ambiente. Para os produtos de contêiner, o vendedor pode fornecer até quatro opções de execução, que podem usar métodos de entrega diferentes e representam configurações diferentes do software. Por exemplo, um vendedor pode criar uma opção de execução usada para testar o produto e outra opção que deve ser implantada em escala dentro de uma empresa.

Você pode ver quais opções de execução estão disponíveis na seção Informações de uso da página de detalhes do produto no AWS Marketplace. Cada opção de execução inclui informações sobre quais serviços são compatíveis e fornece detalhes da versão do software. Exemplos de serviços incluem o Amazon Elastic Container Service (Amazon ECS) e o Amazon Elastic Kubernetes Service (Amazon EKS). Escolha Instruções de uso para ver a documentação do vendedor sobre como usar o produto, como a maneira de fazer login em um servidor da Web ou a configuração de pós-execução.

> **Note**
>
> Para ver um passo a passo sobre como assinar e implantar um produto baseado em contêiner, você também pode consultar os vídeos a seguir:
>
> - Implantação de contêineres do AWS Marketplace em clusters do Amazon ECS (3:34)
> - Implantação de produtos do AWS Marketplace baseados em contêineres usando o Amazon ECS Anywhere (5:07)

Implantação de produtos baseados em contêineres do AWS Marketplace usando o ECS Anywhere

Executar o software de contêiner no AWS Marketplace

Para executar o software de contêiner no AWS Marketplace

1. Faça login no AWS Marketplace.
2. Acesse o AWS Marketplace e encontre o produto que contém o software que você deseja executar. Você deve ter uma assinatura do produto para executar o software. Para obter informações sobre como encontrar e assinar produtos de contêiner no AWS Marketplace, consulte Encontrar e assinar produtos de contêiner.
3. Escolha Continue para assinar na página de detalhes do produto.
4. Escolha Continue to Configuration (Continuar para configuração). Se você não vir o botão, talvez seja necessário aceitar os termos primeiro ou talvez não tenha uma assinatura do produto.
5. Em Opção de execução, selecione uma opção de execução na lista de opções fornecida pelo vendedor. Depois de selecionar uma opção de execução, você pode ver os serviços que podem ser executados em Serviços suportados. Para obter mais informações sobre as opções de execução, consulte Opções de execução de produtos de contêiner.
6. Escolha Continue para executar.
7. Siga as instruções fornecidas pelo vendedor para executar o produto. As instruções variam para cada opção de execução. Para ter mais informações, consulte Execução com uma opção de execução de imagens de contêiner ou Execução com a opção Helm.
8. Opcional: escolha Instruções de uso para obter a documentação do vendedor sobre como configurar e usar o produto após a execução.

Opções de execução de produtos de contêiner

Você pode ver as opções de execução que estão disponíveis na seção Informações de uso da página de detalhes de um produto. Junto com as opções de execução fornecidas pelo vendedor, o AWS Marketplace inclui instruções para extrair imagens do Docker diretamente no Amazon Elastic Container Registry (Amazon ECR).

Como as opções de execução são fornecidas pelo vendedor, seus nomes e conteúdo serão diferentes para cada produto no AWS Marketplace. Embora os métodos sejam exclusivos para cada produto e vendedor, cada opção de execução deve ter um método de entrega. Você pode pensar em um método de entrega como um tipo de opção de execução. Os três métodos de entrega disponíveis para produtos de contêineres são Imagem de contêiner, Chart do Helm e Complemento do Amazon EKS.

Execução com uma opção de execução de imagens de contêiner

Para uma opção de execução com um método de entrega Imagem de contêiner, use as instruções fornecidas pelo vendedor para executar o produto. Isso é feito extraindo imagens do Docker diretamente do Amazon ECR. As etapas gerais para executar o produto são as seguintes:

1. Verifique se você instalou as versões mais recentes do AWS Command Line Interface (AWS CLI) e do Docker. Para obter mais informações, consulte Usar o Amazon ECR com o AWS CLI no Guia do usuário do Amazon Elastic Container Registry.
2. Autentique o cliente do Docker no seu registro do Amazon ECR. As etapas para fazer isso dependerão do sistema operacional.
3. Extraia todas as imagens do Docker usando a imagem fornecida do nome do recurso da Amazon (ARN) do Amazon ECR. Para obter mais informações, consulte Extrair uma imagem no Guia do usuário do Amazon Elastic Container Registry.
4. Revise todas as instruções de uso ou links externos fornecidos pelo vendedor para obter informações sobre o uso do produto.

Execução com a opção Helm

Para uma opção de execução com um método de entrega Helm, use as instruções fornecidas pelo vendedor para executar o produto. Isso é feito instalando um chart do Helm usando a CLI do Helm. Você pode executar a aplicação em um cluster existente do Amazon EKS ou um cluster autogerenciado no EKS Anywhere, no Amazon Elastic Compute Cloud (Amazon EC2) ou on-premises.

> **Note**
>
> O ambiente de execução deve usar a CLI do Helm versão 3.7.1. Para ver uma lista das versões do Helm, consulte Versões do Helm no GitHub.

Se o vendedor tiver habilitado o QuickLaunch, você poderá usá-lo para executar a aplicação. O QuickLaunch é um recurso no AWS Marketplace que usa o AWS CloudFormation para criar um cluster do Amazon EKS e executar a aplicação. Para obter mais informações sobre QuickLaunch, consulte QuickLaunch no AWS Marketplace.

As instruções são fornecidas pelo vendedor e são diferentes para cada vendedor e produto. As etapas gerais para executar um produto com a opção de execução Helm são as seguintes:

Para executar um produto com a opção Helm

1. Siga as etapas de 1 a 6 de Executar o software de contêiner no AWS Marketplace e escolha uma opção de execução com um método de entrega Chart do Helm.
2. Em Destino de execução, escolha o ambiente em que você deseja implantar:
   - Escolha o Kubernetes gerenciado pela Amazon para implantar a aplicação no Amazon EKS. Se o vendedor tiver habilitado o QuickLaunch, você poderá usá-lo para criar um novo cluster do Amazon EKS e executá-lo.
   - Escolha Kubernetes autogerenciado para implantar a aplicação no EKS Anywhere ou em qualquer cluster Kubernetes executado no Amazon EC2 ou on-premises.
3. Se estiver executando em um cluster Kubernetes gerenciado pela Amazon:
   a. Para executar em um cluster existente no Amazon EKS, em Método de execução, escolha Executar no cluster existente e siga as Instruções de execução. As instruções incluem a criação de um perfil do AWS Identity and Access Management (IAM) e a execução da aplicação. Verifique se você está usando a CLI do Helm versão 3.7.1.
   b. Para usar o QuickLaunch para criar um novo cluster do Amazon EKS e executá-lo, em Método de execução, escolha Executar em um novo cluster EKS com o QuickLaunch. Escolha Executar para ser redirecionado para criar uma pilha no console do AWS CloudFormation. Essa pilha criará um cluster do Amazon EKS e implantará a aplicação instalando o chart do Helm fornecido pelo vendedor.
   c. Na página Criação rápida da pilha, em Nome da pilha, forneça um nome para essa pilha.

d. Revise as informações no bloco Parâmetros e forneça as informações necessárias. Analise e selecione as confirmações em Capacidades e escolha Criar pilha.

> **Note**
>
> Para obter mais informações sobre o QuickLaunch, incluindo informações sobre AWS CloudFormation, pilhas e o cluster do Amazon EKS criado, consulte QuickLaunch no AWS Marketplace.

4. Se estiver executando em um cluster Kubernetes autogerenciado:

   a. Verifique se você está usando a CLI do Helm versão 3.7.1.

   b. Escolha Criar token para gerar um token de licença e um perfil do IAM. Esse token e esse perfil são usados para se comunicar com o AWS License Manager e validar os direitos do produto.

   > **Note**
   >
   > O número máximo de tokens de licença para uma conta é 10.

   c. Escolha Baixar como CSV para baixar um arquivo .csv com as informações do token gerado. Como acontece com todos os segredos e senhas, armazene o arquivo .csv em um local seguro.

   d. Execute os comandos em Salvar como segredo do Kubernetes para salvar o token de licença e o perfil do IAM como um segredo no seu cluster do Kubernetes. Esse segredo é usado quando você instala o chart do Helm e executa a aplicação. O AWS Marketplace usa o segredo para verificar o direito a esse produto.

   e. Execute os comandos em Executar aplicação usando o token para instalar o chart do Helm que implanta a implantação no cluster.

   f. Escolha Instruções de uso para obter a documentação do vendedor sobre como configurar e usar o produto após a execução.

   g. Opcional: use os comandos fornecidos em [Opcional] Baixar artefatos para baixar localmente as imagens do contêiner e os charts do Helm localmente.

Execução com a opção Amazon EKS

Para uma opção de execução com um método de entrega Complemento do Amazon EKS, use o console do Amazon EKS para implantar o software no cluster do Amazon EKS. As etapas gerais para executar o produto são as seguintes:

Para executar um produto com a opção Amazon EKS

1. Depois de assinar o produto, navegue até a página de configuração e escolha Continuar no console do Amazon EKS para acessar o console do Amazon EKS.
2. No console do Amazon EKS, escolha a Região da AWS onde o cluster será implantado. Selecione o cluster em que deseja implantar o software.
3. Escolha a guia Add-ons (Complementos).
4. Escolha Obter mais complementos, role para localizar o complemento que você deseja implantar e escolha Próximo.
5. Selecione a versão que você deseja implantar e escolha Próximo. Para obter mais informações sobre a implantação do Amazon EKS, consulte Complementos do EKS.
6. Verifique suas seleções e escolha Criar.

QuickLaunch no AWS Marketplace

Se o vendedor habilitou o QuickLaunch em uma opção de execução, você pode usá-lo para criar um cluster do Amazon EKS e implantar uma aplicação de contêiner nele. Com o QuickLaunch, você usará o AWS CloudFormation para configurar e criar um cluster do Amazon EKS e executar uma aplicação de contêiner nele. Com o QuickLaunch, você pode executar uma aplicação de contêiner para fins de teste. Para usar o QuickLaunch, siga as etapas em Execução com a opção Helm.

Para criar um cluster do Amazon EKS no qual a aplicação possa ser implantada, crie uma pilha do CloudFormation. Uma pilha é um conjunto de recursos da AWS que você pode gerenciar como uma unidade. Todos os recursos em uma pilha são definidos pelo modelo CloudFormation dela. No QuickLaunch, os recursos da pilha incluem as informações necessárias para criar o cluster do Amazon EKS e executar a aplicação. Para obter mais informações sobre pilhas no AWS CloudFormation, consulte Trabalho com pilhas no Guia do usuário do AWS CloudFormation.

Depois que o cluster é criado, o QuickLaunch executa a aplicação nele instalando o chart do Helm fornecido pelo vendedor no cluster. O QuickLaunch trata disso para você como parte da criação da pilha que também cria o cluster do Amazon EKS.

Produtos de machine learning

O AWS Marketplace tem uma categoria para produtos de machine learning que é possível assinar por meio do AWS Marketplace. A categoria de produto é machine learning. Os produtos nessa categoria incluem algoritmos e pacotes de modelos de machine learning (ML).

Navegue em e procure centenas de algoritmos e pacotes de modelos de ML de uma grande variedade de subcategorias, como visão computadorizada, processamento de linguagem natural, reconhecimento de voz, texto, dados, voz, imagem, análise de vídeo, detecção de fraudes e análise preditiva.

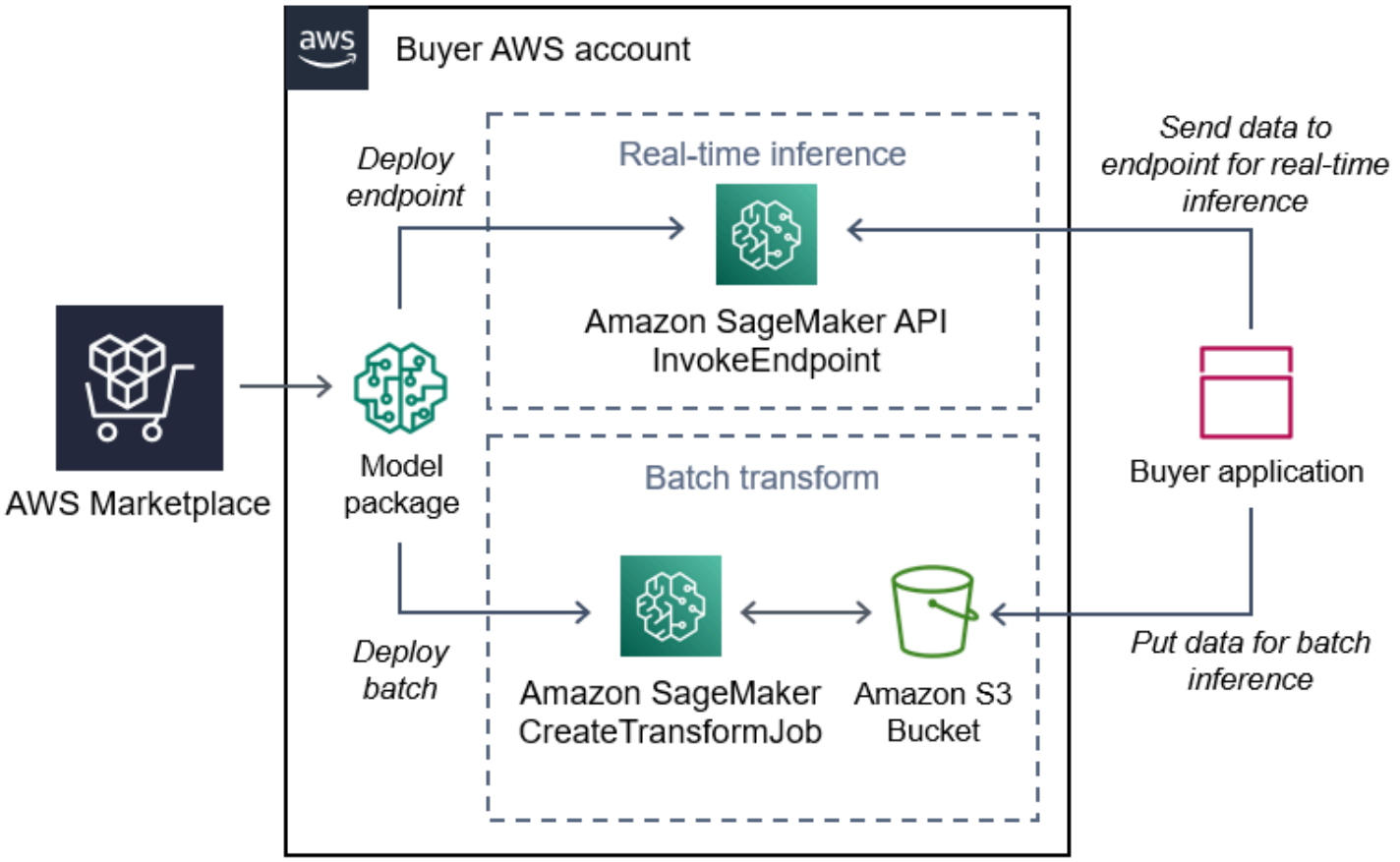
Para avaliar a qualidade e a adequação de um modelo, examine descrições de produtos, instruções de uso, avaliações de clientes, notebooks Jupyter de amostras, definição de preços e informações de suporte. Você implanta modelos diretamente do console do Amazon SageMaker, por meio de um caderno Jupyter, com o SDK do Amazon SageMaker ou usando o AWS Command Line Interface AWS CLI. O Amazon SageMaker fornece um ambiente seguro para executar trabalhos de treinamento e inferência executando uma verificação estática em todos os produtos do marketplace.

Pacote de modelos do Amazon SageMaker

Um pacote de modelos do Amazon SageMaker é um modelo exclusivo de ML pré-treinado que é identificado por um nome do recurso da Amazon (ARN) no Amazon SageMaker. Os clientes usam um pacote de modelos para criar um modelo no Amazon SageMaker. Depois, o modelo poderá ser usado com os serviços de hospedagem para executar inferência em tempo real ou com transformação em lote para executar a inferência em lote no Amazon SageMaker.

O diagrama a seguir mostra um fluxo de trabalho para usar os produtos de pacote de modelo.

1. No AWS Marketplace, você encontra e assina um produto de pacote de modelo.
2. Você implanta o componente de inferência do produto no SageMaker para realizar inferência (ou previsão) em tempo real ou em lotes.



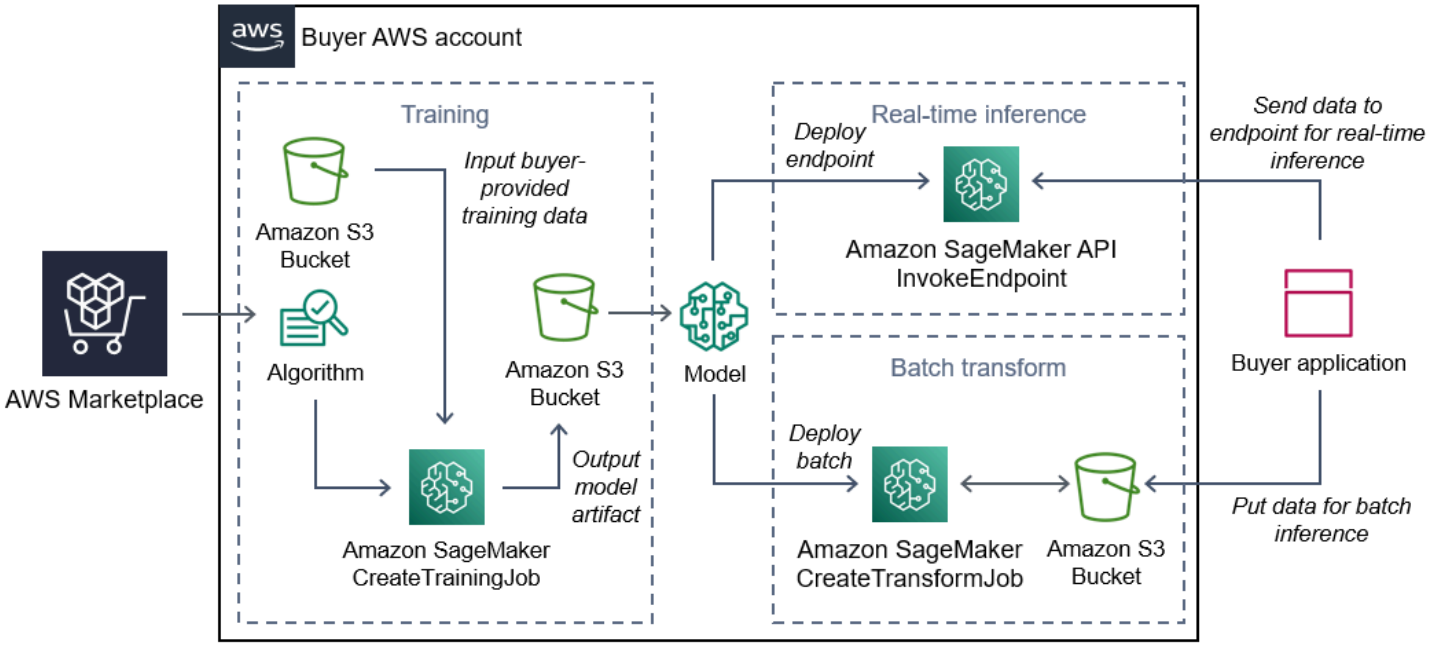
Algoritmo do Amazon SageMaker

Um algoritmo do Amazon SageMaker é uma entidade exclusiva do Amazon SageMaker identificada por um ARN. Um algoritmo tem dois componentes lógicos: treinamento e inferência.

O diagrama a seguir mostra um fluxo de trabalho para usar os produtos de algoritmo.

1. No AWS Marketplace, você encontra e assina um produto de algoritmo.
2. Você usa o componente de treinamento do produto para criar um trabalho de treinamento ou de ajuste usando o conjunto de dados de entrada no Amazon SageMaker para criar modelos de machine learning.
3. Quando o componente de treinamento do produto é concluído, ele gera os artefatos do modelo de machine learning.
4. O SageMaker salva os artefatos do modelo no bucket do Amazon Simple Storage Service (Amazon S3).

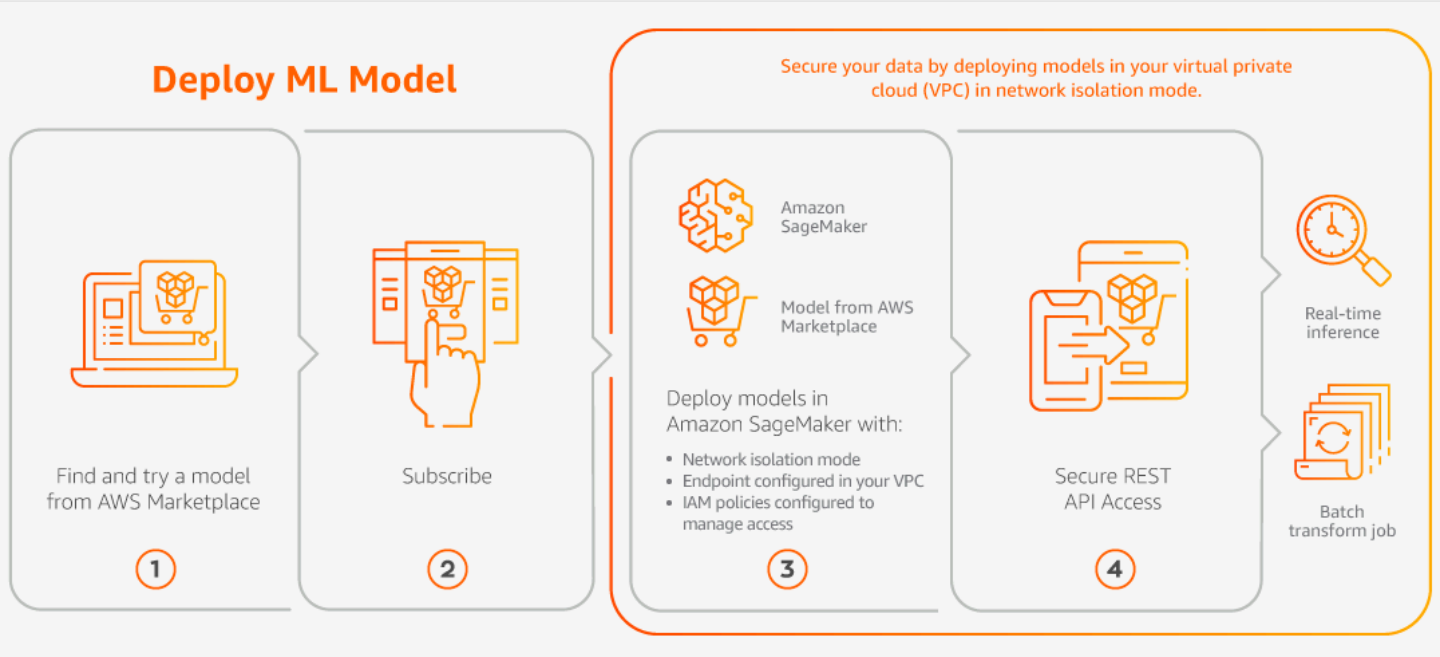
5. No SageMaker, você pode implantar o componente de inferência do produto usando esses artefatos de modelo gerados para realizar inferência (ou previsão) em tempo real ou em lotes.



Encontrar, assinar e implantar

O diagrama a seguir mostra uma visão geral do processo para encontrar, assinar e implantar um produto de machine learning no Amazon SageMaker.

1. Encontrar e experimentar um modelo do AWS Marketplace
2. Assinar o produto de ML
3. Implantar modelos no Amazon SageMaker
4. Usar APIs REST seguras
5. Executar
   - Inferência em tempo real
   - Trabalho de transformação em lotes



Você paga apenas pelo uso, sem taxas mínimas nem compromissos antecipados. O AWS Marketplace oferece um faturamento consolidado para algoritmos e pacotes de modelos e as cobranças de uso da infraestrutura da AWS.

As seções a seguir explicam como encontrar, assinar e implantar um produto de ML.

Tópicos

- Como encontrar um produto de machine learning
- Assinatura de um produto de machine learning
- Implantação de um produto de machine learning

Como encontrar um produto de machine learning

Para encontrar algoritmos ou pacotes de modelos no Amazon SageMaker

1. Faça login no site do AWS Marketplace.
2. Em Encontrar produtos do AWS Marketplace que atendam às necessidades, use o menu suspenso Categorias para encontrar a subcategoria em Machine Learning em que você tem interesse.
3. Refine os resultados de pesquisa aplicando tipo de recurso, categoria e filtros de definição de preço.

4. Nos resultados da pesquisa, acesse a página de detalhes do produto.
5. Revise descrições de produtos, instruções de uso, avaliações de clientes, cadernos Jupyter de amostras, definição de preços e informações de suporte.

Assinatura de um produto de machine learning

Para assinar algoritmos ou pacotes de modelos no Amazon SageMaker

1. Na página de detalhes do produto, escolha Continue para assinar.
2. Na página de compras, revise as informações de preço do produto e o contrato de licença do usuário final (EULA).
3. Escolha Continue para assinar.

Implantação de um produto de machine learning

Para implantar algoritmos ou pacotes de modelos no Amazon SageMaker

1. Confirme se você tem uma assinatura válida do algoritmo ou pacote de modelos navegando até o Software Marketplace.
2. Configure o produto (por exemplo, selecionando uma versão específica ou uma região de implantação) no site do AWS Marketplace.

   Depois de assinar um pacote de modelos ou um produto de algoritmo, ele é adicionado à lista de produtos no console do SageMaker. Você também pode usar SDKs da AWS, o AWS Command Line Interface (AWS CLI) ou o console do SageMaker para criar um endpoint de inferência REST totalmente gerenciado ou realizar inferência em lotes de dados.
3. Veja a página de detalhes do produto Amazon SageMaker escolhendo Exibir no Amazon SageMaker.
4. No console do Amazon SageMaker, implante os algoritmos e os pacotes de modelos usando o console do Amazon SageMaker, o caderno Jupyter, os comandos de CLI do Amazon SageMaker ou as operações de API.

Para obter mais informações sobre como implantar no Amazon SageMaker, consulte Conceitos básicos.

Produtos de serviços profissionais

O AWS Marketplace inclui produtos que são serviços profissionais de vendedores do AWS Marketplace. Você pode encontrar esses produtos na categoria Serviços profissionais ao pesquisar no AWS Marketplace. Você assina e compra esses produtos por meio do AWS Marketplace, mas trabalhará com o vendedor para configurar os serviços profissionais que atendam às suas necessidades.

Compra de serviços profissionais

Você pode pesquisar serviços profissionais usando a categoria Serviços profissionais no AWS Marketplace. Quando você encontrar um produto que lhe interessa, solicite uma oferta do vendedor. Como os serviços profissionais geralmente envolvem o trabalho em conjunto, você deve fornecer algumas informações adicionais ao vendedor para concluir a compra. Você também pode usar isso como uma oportunidade para negociar preços e quaisquer outros detalhes do serviço que precisem ser resolvidos. Você receberá uma oferta privada para o produto. Para obter mais informações sobre ofertas privadas, consulte Ofertas privadas.

Para comprar um produto de serviços profissionais

1. Acesse AWS Marketplace e faça login em sua conta da AWS. Depois, pesquise e encontre um produto de serviços profissionais que você deseja comprar.
2. Na página de detalhes do produto, escolha Continuar.
3. Na página Solicitar serviço, inclua as informações adicionais necessárias para que o vendedor crie a oferta, incluindo seu nome, endereço de e-mail, nome da empresa e qualquer informação adicional que possa ser útil para o vendedor, incluindo necessidades comerciais, cronogramas e requisitos contratuais.
4. O vendedor entrará em contato por meio do endereço de e-mail que você forneceu para descobrir os detalhes da sua oferta. Depois de concordar, o vendedor enviará um link para a oferta no AWS Marketplace. Abra o link em um navegador e faça login na sua conta da AWS.
5. Analise os detalhes da oferta na página de compras que você abriu com o vendedor. Certifique-se de que a oferta seja para o serviço e para o preço que você espera. Verifique também os termos: se você paga uma quantia fixa ou uma série de cobranças. Se a oferta estiver correta, continue. Caso contrário, entre em contato com o vendedor para fazer alterações.
6. Em Configurar contrato, escolha a configuração que você gostaria de usar para seu contrato. Por exemplo, se você estiver comprando um contrato de suporte, pode haver opções para contratos Silver, Gold ou Platinum, com preços diferentes.

7. Selecione Criar contrato para comprar o serviço. O vendedor deve entrar em contato com você em até 2 dias úteis com instruções para usar o serviço.

Produtos de SaaS

Para produtos de software como serviço (SaaS), assine os produtos usando o AWS Marketplace, mas acesse o produto no ambiente do vendedor do software.

Tópicos

Modelos de preços

O AWS Marketplace oferece os seguintes modelos de definição de preço.

Assinaturas baseadas no uso de SaaS

Com as assinaturas baseadas no uso de SaaS, o vendedor de software rastreia seu uso e você só paga pelo que usar. Esse modelo de preço conforme o uso é semelhante ao de muitos Serviços da AWS. O faturamento do uso de um produto SaaS é gerenciado por meio da fatura AWS.

Para assinar usando a assinatura baseada em uso de SaaS

1. Na página de detalhes do produto, escolha Exibir opções de compra para iniciar o processo de assinatura.
2. Revise a assinatura e escolha Assinar na página de assinatura.

> **Note**
>
> Alguns produtos oferecem uma opção de implantação de início rápido, que reduz o tempo e os recursos necessários para configurar, implantar e iniciar o software. Esses produtos são identificados por meio de uma badge de início rápido. Para obter mais informações, consulte the section called “Início rápido”.

Compromissos iniciais de SaaS

Algumas empresas disponibilizam antes contratos de SaaS para compra por meio do AWS Marketplace. Com essa opção, você pode comprar quantidades discretas de licenças ou ingestão de dados para esses produtos. Então, você pode faturar esses produtos, com antecedência, em sua Conta da AWS. Por exemplo, convém comprar 10 licenças de acesso de usuário para um ano ou comprar 10 GB de dados adicionados por dia por um ano.

Ao fazer a compra, você será direcionado ao site do produto para configuração da conta, a menos que o início rápido esteja habilitado. As cobranças por uso acabam sendo exibidas no relatório de faturamento da Conta da AWS regular.

> **Note**
>
> Para obter informações sobre a experiência de início rápido, consulte the section called “Início rápido”.

Para assinar usando um contrato de SaaS

1. Na página de detalhes do produto, escolha Exibir opções de compra para iniciar o processo de assinatura. Escolha as quantidades ou as unidades desejadas, a duração da assinatura (se várias opções estiverem disponíveis) e a renovação automática.
2. Depois de fazer todas as seleções, escolha Criar contrato.
3. Escolha Configurar a conta, o que leva você para o site da empresa. Enquanto a conta estiver sendo configurada e o pagamento verificado, você verá que o contrato está pendente na página de detalhes do AWS Marketplace do produto.

   > **Note**
   >
   > Alguns produtos oferecem uma opção de implantação de início rápido, que reduz o tempo e os recursos necessários para configurar, implantar e iniciar o software. Esses produtos são identificados por meio de uma badge de início rápido. Para obter mais informações, consulte the section called “Início rápido”.

Depois que a configuração for concluída, um link para configurar sua conta estará disponível na página do produto. O software será exibido em Software de sua loja quando você tiver feito login

na conta do AWS Marketplace. Já é possível começar a usar o software. Se você não concluir o processo de configuração da conta, você será solicitado a concluí-la quando acessar o produto novamente no AWS Marketplace.

Acesse a assinatura do software pelo site da empresa de software usando a conta criada no site. Também encontre links do site para as assinaturas de software compradas por meio do AWS Marketplace em Seu software da loja quando você fizer login na conta do AWS Marketplace.

Avaliações gratuitas de SaaS

Alguns fornecedores oferecem avaliações gratuitas para os produtos de SaaS no AWS Marketplace para fins de avaliação. Você pode pesquisar produtos de SaaS no AWS Marketplace e filtrar os resultados para mostrar apenas aqueles com avaliações gratuitas. Os resultados da pesquisa indicam quais produtos oferecem avaliações gratuitas. Todos os produtos com esse recurso exibem a badge de Avaliação gratuita ao lado do logotipo do produto. Na página de aquisição do produto, você pode encontrar a duração do período de avaliação gratuita e quanto uso de software gratuito está incluído no teste.

Durante a avaliação gratuita ou após o término da avaliação gratuita, você pode tomar uma decisão de compra negociando uma oferta privada ou assinando uma oferta pública. As avaliações gratuitas de SaaS não serão convertidas automaticamente em contratos pagos. Se você não desejar mais a avaliação gratuita, poderá deixá-la expirar.

Você pode ver suas assinaturas selecionando Gerenciar assinaturas no console do AWS Marketplace.

> **Note**
>
> Cada Conta da AWS está qualificada apenas para uma avaliação gratuita por produto.

Assinatura de uma oferta de avaliação gratuita de um contrato de SaaS

Para assinar uma oferta de avaliação gratuita de um contrato de SaaS

1. Faça login no console do AWS Marketplace e escolha Descobrir produtos no menu AWS Marketplace.
2. No painel Refinar resultados, acesse Avaliação gratuita e selecione Avaliação gratuita.
3. Em Métodos de entrega, selecione SaaS.

4. Em Modelo de preços, selecione Compromisso antecipado para ver todos os produtos que oferecem avaliações gratuitas. Todos os produtos qualificados exibem uma badge de Avaliação gratuita.
5. Em SaaS, selecione o produto de SaaS que deseja.
6. Escolha Testar gratuitamente na página de detalhes do produto.
7. Em Tipo de oferta, selecione uma opção de Avaliação gratuita.
8. Em Compra, escolha Criar contrato e, em seguida, Aceitar contrato.
9. Escolha Configurar sua conta para concluir seu registro e começar a usar seu software.

Assinatura de uma oferta de avaliação gratuita de assinatura de SaaS

Para assinar uma oferta de avaliação gratuita de assinatura de SaaS

1. Faça login no console do AWS Marketplace e escolha Descobrir produtos no menu AWS Marketplace.
2. No painel Refinar resultados, acesse Avaliação gratuita e selecione Avaliação gratuita.
3. Em Métodos de entrega, selecione SaaS.
4. Em Modelo de preços, selecione Baseado no uso para ver todos os produtos que oferecem avaliações gratuitas. Todos os produtos qualificados exibem uma badge de Avaliação gratuita.
5. Em SaaS, selecione o produto de SaaS que deseja.
6. Escolha Testar gratuitamente na página de detalhes do produto.
7. Em Tipo de oferta, selecione uma opção de Avaliação gratuita.
8. Em Comprar, escolha Assinar.

Início rápido

O início rápido é uma opção de implantação do AWS Marketplace disponível para produtos SaaS que possuem o início rápido habilitado. Reduz o tempo, os recursos e as etapas necessárias para configurar, implantar e iniciar seu software. Para produtos que oferecem esse recurso, você pode optar por usar o início rápido ou configurar manualmente seus recursos.

Para encontrar, assinar e lançar um produto SaaS usando a experiência de início rápido

1. Navegue até a página de pesquisa do AWS Marketplace.

2. Acesse o AWS Marketplace e encontre o produto que contém o software que você deseja executar. Os produtos que oferecem a experiência de início rápido têm uma badge de início rápido na descrição do produto.

   > **Tip**
   >
   > Para encontrar produtos com a experiência de início rápido habilitada, use os filtros SaaS e Modelo do CloudFormation no painel Refinar resultados.

3. Depois de assinar o produto, navegue até a página Configurar e iniciar escolhendo o botão Configurar sua conta.
4. Na página Configurar e iniciar na Etapa 1: verifique se você tem as permissões necessárias da AWS, certifique-se de ter as permissões necessárias para usar a experiência de início rápido. Entre em contato com seu administrador da AWS para solicitar as permissões.

   Para usar a experiência completa de início rápido, você deve ter as seguintes permissões:

   - `CreateServiceLinkedRole`: permite que o AWS Marketplace crie a função vinculada ao serviço `AWSServiceRoleForMarketplaceDeployment`. Essa função vinculada ao serviço permite ao AWS Marketplace gerenciar parâmetros relacionados à implantação, que são armazenados como segredos no AWS Secrets Manager, em seu nome.
   - `DescribeSecrets`: permite ao AWS Marketplace obter informações sobre parâmetros de implantação passados pelos vendedores.
   - `GetRole`: permite ao AWS Marketplace determinar se a função vinculada ao serviço foi criada na conta.
   - `ListSecrets`: permite ao AWS Marketplace obter o status dos parâmetros de implantação.
   - `ListRegions`: permite ao AWS Marketplace obter Regiões da AWS que estejam optados pela conta corrente.
   - `ReplicateSecrets`: permite ao AWS Marketplace iniciar a replicação de segredos para a região selecionada onde você implantará o software.
5. Para a Etapa 2: Fazer logon em uma conta de fornecedor nova ou existente, escolha o botão Fazer logon ou criar uma conta. O site do vendedor abre em uma nova guia, onde você pode fazer logon ou criar uma conta. Quando terminar, retorne à página Configurar e iniciar.
6. Para a Etapa 3: Configurar seu software e integração da AWS, escolha como você deseja configurar o produto:

- AWS CloudFormation: escolha o botão Modelo de execução para implantar um modelo predefinido do CloudFormation para configurar seu produto. Use o CloudFormation para revisar os parâmetros do modelo e preencher todos os campos obrigatórios adicionais. Quando terminar, retorne à página Configurar e iniciar para iniciar seu software.
- Manual: use as instruções fornecidas pelo vendedor para configurar seu software.

7. Para a Etapa 4: Iniciar seu software, escolha o botão Iniciar software para iniciar seu software.

Produtos de dados

Você pode usar o AWS Marketplace para localizar e assinar produtos de dados disponíveis por meio do AWS Data Exchange. Para obter mais informações, consulte Assinatura de produtos de dados no AWS Data Exchange no Guia do usuário do AWS Data Exchange.

Pagar por produtos

No início do mês, você recebe uma fatura da Amazon Web Services (AWS) com as cobranças do AWS Marketplace. Para produtos de software, a fatura inclui um cálculo da tarifa horária do software multiplicada pelo número de horas em que qualquer instância da imagem de máquina da Amazon (AMI) com este software é executada. Você também recebe uma fatura pelo uso de produtos da infraestrutura da AWS como o Amazon Elastic Compute Cloud (Amazon EC2), o Amazon Simple Storage Service (Amazon S3), o Amazon Elastic Block Store (Amazon EBS) Block Store (Amazon EBS) e a largura de banda.

Se a Conta da AWS estiver sediada na Europa, Oriente Médio e África (EMEA), exceto Turquia e África do Sul, e sua compra for de um vendedor qualificado para EMEA, você receberá uma fatura da Amazon Web Services EMEA SARL (AWS Europe). Caso contrário, você receberá uma fatura da AWS Inc.

> **Note**
>
> Para compras por contrato, a fatura das taxas de assinatura ocorre no momento da assinatura, e não na fatura mensal consolidada. Pagamentos flexíveis em contratos são faturados no momento do pagamento programado. Para contratos que têm componentes de uso (como um modelo de pagamento conforme o uso), o uso aparece na fatura mensal consolidada.

Os produtos do AWS Marketplace que usam topologias complexas podem incorrer em cobranças de clusters de AMIs e outros serviços de infraestrutura da AWS executados pelo modelo do AWS CloudFormation fornecido.

Por exemplo, suponha que você execute um software por 720 horas em um tipo de instância pequena do EC2. A taxa do vendedor pelo uso de software é 0,12 USD/h e as cobranças do EC2 são 0,085 USD/h. No final do mês, você receberá a cobrança de US$ 147,60.

Para obter mais informações sobre como assinar produtos de dados, consulte Assinatura de produtos de dados do AWS Data Exchange no Guia do usuário do AWS Data Exchange.

Para mais informações sobre a conta da AWS, consulte o Guia do usuário do AWS Billing.

Para obter mais informações sobre como gerenciar seus pagamentos na Amazon Web Services EMEA SARL (AWS Europe), consulte Gerenciamento de pagamentos na AWSEurope no Guia do usuário do AWS Billing.

Tópicos

Ordens de compra

Ao usar ordens de compra no AWS Marketplace e no console do AWS Billing, você recebe faturas da AWS que incluem o número da ordem de compra definido pelo cliente. Essa abordagem simplifica o processamento de pagamentos e a alocação de custos. No AWS Marketplace, as faturas fora do ciclo incluem compras que são cobradas imediatamente ou de acordo com um pagamento definido programado em uma oferta privada. Geralmente, cobranças de pagamento conforme o uso aparecem em uma fatura de uso mensal consolidada do AWS Marketplace.

Uso de ordens de compra para transações do AWS Marketplace

Você pode adicionar uma ordem de compra no momento da transação, que se aplicará a todas as faturas subsequentes fora do ciclo relacionadas a essa transação.

Os produtos a seguir oferecem suporte a ordens de compra:

- Contratos de software como serviço (SaaS)
- Produtos de serviços profissionais
- Produtos de servidor (incluindo instâncias de AMI, contêineres, modelos do AWS CloudFormation e charts do Helm) com um modelo de preços anual ou contratual

> **Note**
>
> O suporte a ordens de compra para o modelo de preços anuais só está disponível para ofertas privadas com um cronograma de pagamento flexível.

As ordens de compra para o modelo de preços anuais só são aceitas para ofertas privadas com um cronograma de pagamento flexível. A ordem de compra especificada não se aplica às faturas mensais do AWS Marketplace consolidadas para cobranças de pagamento conforme o uso.

> **Note**
>
> Para usar ordens de compra no AWS Marketplace, a conta de gerenciamento em sua organização da AWS deve habilitar a integração do AWS Billing. Essa tarefa de configuração única cria uma função vinculada ao serviço, que permite que contas em sua organização com permissão se inscrevam para usar ordens de compra. Se você não habilitar a integração, as contas em sua organização não poderão adicionar uma ordem de compra durante a aquisição. Para obter mais informações sobre a integração, consulte Criação de uma função vinculada ao serviço para o AWS Marketplace.

Para especificar uma ordem de compra no AWS Marketplace

1. Encontre e prepare-se para comprar um produto compatível do AWS Marketplace.
2. Durante o processo de compra, na página Configurar sua assinatura de software (para SaaS), em Ordem de compra, escolha Adicionar número da ordem de compra.
3. Insira o número da ordem de compra no campo Número da ordem de compra.

   O número da ordem de compra é o número ou texto que você usa para rastrear a ordem de compra em seu sistema. Geralmente é emitido por um sistema ou processo interno. Ele pode ter até 200 caracteres de comprimento.

Para obter detalhes sobre uma ordem de compra, incluindo ordens de compra fornecidas durante as transações do AWS Marketplace, use o painel de ordens de compra no console do AWS Billing.

Uso de ordens de compra de uso geral

Para separar cobranças do AWS Marketplace de outras ordens de compra, você pode criar uma ordem de compra com um item de linha de uso geral do AWS Marketplace no console do AWS Billing. As transações de fatura do AWS Marketplace incluirão a ordem de compra de uso geral que você especifica se determinados critérios e parâmetros correspondem (por exemplo, entidades de cobrança). Uma exceção são as faturas fora do ciclo que especificaram uma ordem de compra da transação do AWS Marketplace. Para obter mais informações, consulte Gerenciamento de ordens de compra no Guia do usuário do Gerenciamento de Faturamento e Custos da AWS.

Solução de problemas das ordens de compra

As informações na tabela a seguir podem ajudar a solucionar problemas com ordens de compra ou entender o que acontece em diferentes cenários.

Cenário	Detalhes
Permissões insuficientes	A nota é exibida perto do campo Entrada da ordem de compra se você não tiver a permissão `aws-marketplace:Subscribe` para se inscrever. A conta de gerenciamento também deve habilitar a integração do AWS Billing. Para obter informações sobre como habilitar a integração, consulte Criação de uma função vinculada ao serviço para o AWS Marketplace.
A ordem de compra não existe	O AWS Marketplace cria uma nova ordem de compra para você. A nova ordem de compra tem informações padrão, sem informações de contato.
Notificações sobre ordem de compra ausente	Ordens de compra sem informações de contato (incluindo as ordens de compra criadas pelo AWS Marketplace) não recebem notificações por e-mail. Você pode adicionar informações de contato a uma ordem de compra no painel

Cenário	Detalhes
	Ordens de compra no console do Billing and Cost Management.
Número de ordem de compra incorreto adicionado	Se você inserir um número de ordem de compra incorreto e precisar atualizá-lo, entre em contato com AWS Support para atualizar o número da ordem de compra.
A conta assinante é transferida para uma organização diferente	Para que as ordens de compra funcionem na nova organização, a integração deve ser concluída na nova organização. Se a integração tiver sido concluída e o suporte para ordens de compra estiver funcionando na nova organização, quando a conta assinante for transferida entre organizações, novas faturas mostrarão o número da ordem de compra na nova organização (e uma nova ordem de compra será criada, se necessário).
Opção de ordem de compra não disponível ao finalizar a compra	A integração do AWS Billing está disponível apenas para contratos de SaaS, produtos de serviços profissionais e produtos de servidor com preços contratuais e produtos de servidor com preços anuais para ofertas privadas com um cronograma de pagamento flexível.
Contratos com pagamento conforme o uso	A fatura do contrato mostra o número da ordem de compra, mas a fatura de consumo (pagamento conforme o uso) não mostra o número da ordem de compra. O modelo de pagamento conforme o uso, não permite adicionar números da ordem de compra. Considere adicionar uma ordem de compra com um item de linha de uso geral do AWS Marketplace no console do AWS Billing.

Cenário	Detalhes
Ordem de compra suspensa	Quando um número de ordem de compra é fornecido e a ordem de compra é marcada como suspensa no painel Ordens de compra no console do Billing and Cost Management, o novo item de linha é adicionado à ordem de compra, mas a fatura não inclui a ordem de compra. O administrador de cobrança da Conta da AWS precisa ativar a ordem de compra e entrar em contato com AWS Support para gerar novamente a fatura com a ordem de compra ativa.
Ordem de compra expirada	Quando um número de ordem de compra é fornecido e a ordem de compra expira, o novo item de linha é criado e a ordem de compra é marcada como ativa. A data de término do item de linha é usada como a data de vencimento da nova ordem de compra.
Acompanhamento do saldo	O acompanhamento do saldo não está habilitado para itens de linha do AWS Marketplace.
Integração a sistemas de compras	A ordem de compra fornecida por um sistema de compras integrado é exibida nas faturas.
Cronograma de pagamento flexível: compra inicial	Um contrato que tem datas específicas para faturamento (cronograma de pagamento flexível) gera um item de linha inicial na ordem de compra por zero dólares. Itens de linha adicionais com preços aplicáveis são criados para cada fatura.

Cenário	Detalhes
Cronograma de pagamento flexível: várias ordens de compra	Se você precisar que pagamentos individuais para um cronograma de pagamento flexível apareçam com diferentes ordens de compra, entre em contato com AWS Support para alterar o número da ordem de compra em faturas futuras.

Informações sobre reembolsos

Os clientes podem solicitar diferentes tipos de reembolso para produtos do AWS Marketplace. Para produtos do AWS Marketplace vendidos pela AWS, consulte a página da política de reembolso e, em seguida, envie o formulário de contato com o suporte usando o AWS Support Center Console. Se o produto for vendido por terceiros, revise as políticas de reembolso na página de detalhes do produto. As taxas de assinatura do software do AWS Marketplace são pagas ao vendedor do produto, e os reembolsos devem ser solicitados diretamente ao vendedor. Cada vendedor do AWS Marketplace deve incluir uma política de reembolso na página do AWS Marketplace.

Para obter mais informações sobre reembolsos relacionados às compras do AWS Marketplace, consulte os seguintes tópicos no Guia do vendedor do AWS Marketplace:

- Refunds
- Definição de preço do produto

> **Note**
>
> Para todos os reembolsos relacionados a ofertas privadas, entre em contato com o vendedor.

Cancelar a assinatura do produto

Você pode cancelar a assinatura do produto ou a renovação automática no AWS Marketplace. As etapas a seguir fornecem instruções para produtos de software como serviço (SaaS), machine learning (ML) e imagem de máquina da Amazon (AMI) no AWS Marketplace.

Tópicos

Cancelar a assinatura de SaaS

1. Faça login no AWS Management Console e abra o AWS Marketplace console.
2. Acesse a página Gerenciar assinaturas.
3. Para o método de entrega, escolha SaaS na lista suspensa.
4. Selecione a assinatura do produto que você deseja cancelar.
5. Escolha Cancel subscription.

Cancelar a assinatura de machine learning

Antes de cancelar sua assinatura de machine learning, realize as seguintes ações:

- Para algoritmos de ML: faça login no AWS Management Console e abra o console do Amazon SageMaker. Encerre qualquer trabalho de treinamento em execução para o algoritmo. Se você criou um pacote de modelo no algoritmo, não poderá iniciar um endpoint em tempo real nem criar um trabalho de inferência em lote depois que sua assinatura de machine learning for cancelada.
- Para pacotes de modelos de ML ou modelos criados nos algoritmos, faça login no AWS Management Console e abra o console do Amazon SageMaker. Encerre qualquer endpoint em execução em tempo real para os modelos ou encerre qualquer trabalho de inferência em lote em execução.

> **Note**
>
> Os trabalhos e endpoints existentes que não foram encerrados continuarão em execução e serão cobrados até serem encerrados.

Para cancelar uma assinatura de machine learning

1. Faça login no AWS Management Console e abra o AWS Marketplace console.
2. Acesse a página Minhas assinaturas.
3. Selecione a assinatura do produto que você deseja cancelar.
4. Escolha Cancel subscription. Depois de cancelar a assinatura, você não poderá iniciar seu algoritmo ou modelo.

Cancelar a assinatura de AMI

1. Faça login no AWS Management Console e abra o AWS Marketplace console.
2. Acesse a página Gerenciar assinaturas.
3. Para o método de entrega, escolha Imagem de máquina da Amazon na lista suspensa.
4. Selecione a assinatura do produto que você deseja cancelar.
5. Na lista suspensa Ações, escolha Cancelar assinatura.
6. Leia as informações fornecidas para Confirmar que as instâncias em execução são cobradas em sua conta e marque a caixa de seleção. Escolha Yes, cancel subscription.
7. Abra Gerenciar no console da AWS em uma nova guia.
8. Encerre a instância em execução no console do Amazon EC2. Se você tiver várias instâncias em execução, deverá encerrar todas elas. Além disso, você deve excluir as pilhas do AWS CloudFormation, se aplicável.
9. Volte para a guia Gerenciar assinaturas e escolha Sim, cancelar assinatura. Depois de cancelar a assinatura, você perderá o acesso ao software e não será mais cobrado por ele.

Cancelar a renovação automática de sua assinatura de contrato de SaaS

1. Faça login no AWS Management Console e abra o AWS Marketplace console.
2. Acesse a página Detalhes do produto.
3. Escolha Continuar para acessar a página de pedidos.
4. Escolha a guia Modificar renovação e, em seguida, escolha Cancelar renovação.

Métodos de pagamento

Quando criou a Conta da AWS, você definiu a forma de pagamento para essa conta. É possível gerenciar as formas de pagamento no console de Gerenciamento de Faturamento e Custos da AWS. Para obter instruções, consulte Gerenciamento de pagamentos no Guia do usuário do AWS Billing.

Erros de pagamento

Se ocorrer um erro ao processar o pagamento por meio de sua conta de pagador, atualize a forma de pagamento e tente novamente. Podem ocorrer erros porque:

- A forma de pagamento está ausente, é inválida ou não é suportada.
- O pagamento foi recusado.
- Sua conta da Amazon Internet Services Private Limited (AISPL) limita o uso de cartões de débito ou crédito para novas compras com um modelo de preços contratuais. Se você tiver uma conta da AISPL, entre em contato com o serviço de atendimento ao cliente da AWS para atualizar a forma de pagamento padrão. Para obter mais detalhes, consulte Restrição às compras com cartão de crédito e débito para clientes da AISPL que usam o AWS Marketplace no site do Blog do AWS Marketplace.
- Sua oferta privada inclui um cronograma de pagamento. No entanto, sua forma de pagamento padrão não está definida com os termos de faturamento.

As formas de pagamento atualizadas podem levar até sete dias para serem disponibilizadas para novas compras. Para obter ajuda com a solução de problemas, entre em contato com AWS Support.

Moedas aceitas

As listas a seguir incluem todas as moedas existentes aceitas pela AWS e pela Amazon Web Services EMEA SARL.

> **Note**
>
> A rupia indiana (INR) não é uma moeda aceita porque a Amazon Internet Services Private Limited (AISPL) não tem suporte atualmente no AWS Marketplace. Para obter mais informações, consulte Quais são as diferenças entre as Contas da AWS e as contas da AISPL.

As moedas aceitas pela Amazon Web Services são as seguintes:

- Dólar australiano (AUD)
- Libra esterlina (GBP)
- Dólar canadense (CAD)
- Coroa dinamarquesa (DKK)
- Euro (EUR)
- Dólar de Hong Kong (HKD)
- Iene japonês (JPY)
- Dólar neozelandês (NZD)
- Coroa norueguesa (NOK)
- Dólar de Cingapura (SGD)
- Rand sul-africano (ZAR)
- Coroa sueca (SEK)
- Franco suíço (CHF)
- Dólar americano (USD)

As moedas aceitas pela Amazon Web Services EMEA SARL são as seguintes:

- Libra esterlina (GBP)
- Coroa dinamarquesa (DKK)
- Euro (EUR)
- Coroa norueguesa (NOK)
- Rand sul-africano (ZAR)
- Coroa sueca (SEK)
- Franco suíço (CHF)
- Dólar americano (USD)

Alteração da moeda preferida

As compras do AWS Marketplace são exibidas na moeda que você especificou para a Conta da AWS. Você pode alterar a moeda preferida da sua conta no console do AWS Billing and Cost

Management. Para obter instruções, consulte Alteração da moeda que você usa para pagar sua fatura no Guia do usuário do AWS Billing.

> **Note**
>
> Alterar a moeda preferida altera as instruções de remessa. Para ver as instruções de remessa atualizadas, consulte sua fatura do AWS Marketplace ou acesse a página Configurações da conta no console do AWS Billing and Cost Management.

Atualização das instruções de remessa

Os clientes com Contas da AWS localizadas na Europa, Oriente Médio e África (EMEA), exceto Turquia e África do Sul, que compraram produtos de software de vendedores qualificado para EMEA, recebem uma fatura da Amazon Web Services EMEA SARL. As faturas da Amazon Web Services EMEA SARL (AWS Europe) têm instruções de remessa diferentes das da AWS, Inc. Você pode encontrar informações de remessa nas faturas quando estiver conectado ao console do AWS Billing and Cost Management. As contas bancárias listadas na parte de informações de remessa da fatura são diferentes das compras de serviços da Nuvem AWS por meio da Amazon Web Services EMEA SARL. A Amazon Web Services EMEA SARL usa a Amazon Payments Europe, S.C.A., uma instituição de dinheiro eletrônico licenciada em Luxemburgo, como processador de pagamento para faturas do AWS Marketplace. Todas as faturas devem ser pagas integralmente. Todos os pagamentos que não cubram o valor total da fatura serão reembolsados em sua conta bancária.

A tabela a seguir descreve os tipos de transação, a entidade de transação e as instruções de remessa correspondentes (Nome da conta listado em Detalhes da transferência eletrônica de fundos na fatura).

Tipo de transação	Entidade de transação	Instruções de remessa
Compras de serviços da Nuvem AWS	Amazon Web Services EMEA SARL	Amazon Web Services EMEA SARL
Vendedor qualificado do AWS Marketplace	Amazon Web Services EMEA SARL	Amazon Payments Europe, S.C.A.
Vendedor não qualificado do AWS Marketplace	AWS Inc.	AWS

Para solicitar uma carta bancária com as instruções de remessa, selecione Faturamento ou suporte de conta e crie um caso de Suporte de conta e cobrança em Entre em contato com a AWS ou envie uma mensagem de e-mail para <awslux-receivables-support@email.amazon.com>.

Para obter mais informações sobre como alterar a preferência monetária para uma moeda compatível, consulte Alteração da moeda que você usa para pagar sua fatura no Guia do usuário do AWS Billing.

A Amazon Web Services EMEA SARL aceita pagamentos por transferência eletrônica de fundos, por cartões de crédito MasterCard, VISA e American Express. Os cartões de crédito Diner's Club ou Discover não são aceitos.

Para obter mais informações, consulte a Ajuda fiscal do comprador do AWS Marketplace.

Marcação de alocação de custo

O AWS Marketplace oferece suporte à marcação de alocação de custos para produtos de software comprados. Você pode usar tags de alocação de custos ativadas para identificar e rastrear o uso de recursos do AWS Marketplace por meio do AWS Cost Explorer, do Relatório de custos e uso da AWS, de Orçamentos da AWS ou de outras ferramentas de análise de custos da nuvem. Para facilitar a classificação e o rastreamento de custos do AWS Marketplace, você pode usar tags de alocação de custos para organizar seus custos de recursos no relatório de alocação de custos.

As tags de alocação de custos no AWS Marketplace vêm das duas fontes a seguir:

- Os custos do produto de software da imagem de máquina da Amazon (AMI) associados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) com tags herdam essas mesmas tags. Você pode ativar essas tags como tags de custo alocado no console do AWS Billing and Cost Management de uma conta. Para obter mais informações sobre como usar tags de alocação de custos com produtos de AMI, consulte Marcação de alocação de custos em produtos de AMI.
- Produtos de AMI, contêiner e software como serviço (SaaS) podem ter tags fornecidas pelo fornecedor. Por exemplo, um produto de SaaS que fatura pelo número de usuários pode usar uma tag para identificar o uso por departamento. Para obter mais informações sobre como usar essas tags, consulte Tags medidas pelo fornecedor.

A marcação de alocação de custos só rastreará os custos a partir do momento em que as tags foram ativadas no console do Billing and Cost Management. Somente os proprietários de Conta da AWS, os proprietários de contas de gerenciamento do AWS Organizations e usuários com as permissões apropriadas podem acessar o console do Billing and Cost Management de uma conta. Independentemente de você usar a marcação de alocação de custos, não há alteração no valor cobrado. Usar ou não tags de alocação de custos não afeta a funcionalidade de seus produtos de software do AWS Marketplace.

Para assinaturas de vendedores qualificados para EMEA, o Relatório de Custo e Uso inclui uma coluna para a Parte Contratante da AWS (Amazon Web Services EMEA SARL).

Tags medidas pelo fornecedor

Os produtos do AWS Marketplace com medição de fornecedores (incluindo produtos de AMI, contêiner e SaaS) podem ter tags fornecidas pelo fornecedor do software como um serviço adicional

para os clientes. Essas tags são tags de alocação de custos que ajudam você a entender seu uso de recursos do AWS Marketplace em todas as métricas fornecidas pelo fornecedor. Você pode usar essas tags para identificar e rastrear o uso de recursos do AWS Marketplace por meio de AWS Cost Explorer Service, AWS Cost and Usage Report, AWS Budgets ou outras ferramentas de análise de custos na nuvem.

As tags aparecem no console do AWS Billing depois que você começa a usar o produto do AWS Marketplace e o fornecedor envia os registros de medição para o AWS Marketplace. Se você estiver usando um produto com base em um compromisso inicial em um contrato, não receberá o uso da medição do produto. Como resultado, você não terá as tags medidas pelo fornecedor no console do AWS Billing. Se você estiver gerenciando uma conta vinculada, deverá ter as permissões `ModifyBilling` e `ViewBilling` para visualizar e ativar as tags no AWS Billing. Para obter mais informações, consulte Políticas de ações de faturamento da AWS no Guia do usuário do faturamento da AWS.

> **Note**
>
> A ativação de tags medidas pelo fornecedor pode aumentar o tamanho do seu relatório de custo e uso. Seu relatório de custo e uso é armazenado no Amazon S3. Portanto, seus custos do Amazon S3 também podem aumentar.

Para ativar tags medidas pelo fornecedor para todos os produtos qualificados do AWS Marketplace

1. Faça login no AWS Management Console e abra o AWS Billing console. Depois, escolha Tags de alocação de custos no painel de navegação à esquerda.
2. Escolha a guia Tags de alocação de custos geradas pela AWS.
3. Pesquise `aws:marketplace:isv:` para encontrar tags para todos os produtos que oferecem suporte à marcação medida pelo fornecedor.
4. Marque as caixas de seleção para todas as tags e escolha Ativar. As tags medidas pelo fornecedor entrarão em vigor em 24 horas.

Tópicos relacionados

Para obter mais informações, consulte os tópicos a seguir:

- Usar tags de alocação de custos no Guia do usuário do AWS Billing.

- Ativar as tags de alocação de custos geradas pela AWS no Guia do usuário do AWS Billing

Lojas privadas

Um mercado privado controla quais produtos os usuários na Conta da AWS, como usuários corporativos e equipes de engenharia, podem adquirir o AWS Marketplace. Ela se baseia no AWS Marketplace e permite que os administradores criem e personalizem catálogos digitais gerenciados de provedores de software independentes (ISVs) aprovados e produtos em conformidade com as políticas internas. Os usuários da Conta da AWS podem encontrar, comprar e implantar produtos aprovados do mercado privado e garantir que todos os produtos disponíveis estejam em conformidade com as políticas e os padrões da organização.

Um mercado privado fornece um amplo catálogo de produtos disponíveis emAWS Marketplace, juntamente com um controle refinado desses produtos. Com AWS Organizations, você pode centralizar o gerenciamento de todas as suas contas, agrupar suas contas em unidades organizacionais (OUs) e anexar políticas de acesso diferentes a cada OU. Você pode criar várias experiências de mercado privadas associadas a toda a sua organização, a uma ou mais OUs ou a uma ou mais contas em sua organização, cada uma com seu próprio conjunto de produtos aprovados. Seus AWS administradores também podem aplicar a marca da empresa a cada experiência de mercado privado com o logotipo, as mensagens e o esquema de cores da sua empresa ou equipe.

Esta seção descreve o uso do mercado privado como comprador. Para obter informações sobre como gerenciar mercados privados como administrador, consulte Criar e gerenciar uma loja privada.

Observações

- Você pode adicionar produtos privados que foram compartilhados com você (por meio de uma oferta privada) a um mercado privado. Para ter mais informações, consulte Assinatura de um produto privado em um mercado privado .
- Em um mercado privado, os clientes têm automaticamente direito a quaisquer produtos cujos EULAs sejam regidos pelo Contrato do Cliente da AWS ou outro contrato com a AWS que rege o uso dos Serviços da AWS. Os clientes já têm direito a esses produtos por padrão; portanto, eles não estão incluídos na lista de produtos que você aprovou em seu mercado privado. Os clientes podem usar o catálogo de serviços para gerenciar a implantação desses produtos.

Visualizar páginas de detalhes do produto

Os usuários só podem assinar produtos que você permitiu no mercado privado que controla a conta. Eles podem procurar e ver a página de detalhes de qualquer produto, mas a assinatura só é habilitada para produtos adicionados ao mercado privado. Se um produto não estiver no mercado privado no momento, o usuário verá um banner vermelho na parte superior da página, informando que o produto não está aprovado para compra no AWS Marketplace.

Se as solicitações de software estiverem habilitadas, os usuários poderão escolher Criar solicitação na página de detalhes do produto. Quando os usuários escolhem Criar solicitação, eles enviam uma solicitação ao administrador para disponibilizar o produto no mercado privado. Para obter mais informações sobre esse recurso, consulte Gerenciar solicitações de usuário.

Assinar um produto em uma loja privada

Para inscrever um produto em seu mercado privado, navegue até a página de detalhes do produto e escolha Continuar. Isso o redireciona para a página de assinatura do produto. Na página de assinatura, você pode fazer suas seleções de configuração e selecionar Subscribe (Assinar).

Se o produto não for aprovado em sua loja privada, Subscribe (Assinar) não estará disponível. Um banner vermelho na parte superior da página indica que esse produto não está aprovado para aquisição no momento. Se as solicitações de software estiverem habilitadas, você poderá escolher Create request (Criar solicitação) para enviar uma solicitação ao administrador pedindo que o produto seja adicionado à sua loja privada.

Assinatura de um produto privado em um mercado privado

Alguns produtos não estão disponíveis publicamente para busca no AWS Marketplace. Esses produtos só podem ser vistos quando você recebe uma oferta privada do vendedor. No entanto, você só poderá assinar se o administrador do mercado privado primeiro adicionar o produto ao mercado privado. Por esse motivo, a oferta privada deve ser estendida tanto para sua Conta da AWS quanto para a conta que inclui o administrador do mercado privado da sua organização. Depois que a oferta privada for estendida ao usuário e ao administrador, o administrador do mercado privado poderá adicionar o produto ao mercado privado. Depois que o produto for aprovado, você poderá assinar o produto como qualquer outra oferta privada.

Solicitação da adição de um produto ao mercado privado

Como usuário, você pode solicitar que o administrador adicione um produto que não esteja em seu mercado privado. Para fazer uma solicitação, navegue até a página de detalhes do produto, escolha Create request (Criar solicitação), insira uma solicitação ao administrador para que o produto seja adicionado à sua loja privada e envie sua solicitação. Para rastrear o status da solicitação, no menu suspenso esquerdo, escolha Your Private Marketplace Requests (Suas solicitações da loja privada).

Criar e gerenciar uma loja privada

Para criar e gerenciar um mercado privado, você deve estar conectado à conta de gerenciamento ou à conta de administrador delegado do mercado privado. Você também deve ter as permissões AWS Identity and Access Management (IAM) na política do AWSPrivateMarketplaceAdminFullAccess IAM. Para obter mais informações sobre como aplicar essa política a usuários, grupos e funções, consulte the section called “Criação de um administrador do mercado privado”.

> **Note**
>
> Se você é um cliente atual de um mercado privado sem a AWS Organizations integração com o mercado privado, você pode criar e gerenciar um mercado privado a partir de qualquer conta em sua organização que tenha a política AWSPrivateMarketplaceAdminFullAccess do IAM.

Esta seção inclui tarefas que você pode concluir como administrador de um mercado privado por meio do site do AWS Marketplace. Você também pode gerenciar mercados privados usando o AWS Marketplace Catalog API. Para obter mais informações, consulte Como trabalhar com um mercado privado na Referência do AWS Marketplace Catalog API.

Começando com o mercado privado

Para começar a usar o mercado privado, verifique se você está conectado à sua conta AWS de gerenciamento, navegue até o Private Marketplace e habilite os seguintes pré-requisitos:

- Acesso confiável — Você deve habilitar o acesso confiável paraAWS Organizations, o que permite que a conta de gerenciamento de uma organização forneça ou revogue o acesso aos AWS Organizations dados de um AWS serviço. Habilitar o acesso confiável é fundamental para que o

mercado privado se AWS Organizations integre e designe o mercado privado como um serviço confiável em sua organização.

- Função vinculada ao serviço — Você deve habilitar a função vinculada ao serviço do mercado privado, que reside na conta de gerenciamento e inclui todas as permissões que o mercado privado exige para descrever AWS Organizations e atualizar os recursos do mercado privado em seu nome. Para obter mais informações sobre a função vinculada ao serviço, consulte Usando funções para configurar o Private Marketplace em. AWS Marketplace

> **Note**
>
> Os clientes atuais do mercado privado podem ativar as configurações do seu mercado privado navegando até a página do administrador do Private Marketplace e escolhendo Configurações. Ao habilitar o acesso confiável AWS Organizations e criar uma função vinculada ao serviço, você pode utilizar recursos, como associar OUs a experiências de mercado privado e registrar um administrador delegado. Quando ativadas, somente a conta de gerenciamento e a conta de administrador delegado podem criar e gerenciar experiências de mercado, com os recursos existentes transferidos para a conta de gerenciamento e compartilhados somente com o administrador delegado. Desativar o acesso confiável removerá a governança do mercado privado de sua organização. Não há grupos de contas exibidos em seu mercado privado. Para visualizar a governança da sua organização em diferentes níveis, use a página Estrutura da organização. Para perguntas ou suporte, entre em contato conosco.

Gerenciando o mercado privado

Você pode gerenciar seu mercado privado na página do administrador do Private Marketplace em Configurações no painel esquerdo. O administrador da conta de gerenciamento e os administradores delegados podem usar essa página para ver detalhes do mercado privado, incluindo o mercado privado padrão e o número de experiências ao vivo.

Os administradores da conta de gerenciamento também podem usar essa página para gerenciar as seguintes configurações.

Administradores delegados

O administrador da conta de gerenciamento pode delegar permissões administrativas privadas do marketplace a uma conta de membro designada, conhecida como administrador delegado. Para registrar uma conta como administrador delegado no mercado privado, o administrador da conta de gerenciamento deve garantir que o acesso confiável e a função vinculada ao serviço estejam habilitados, escolher Registrar um novo administrador, fornecer o número da AWS conta de 12 dígitos e escolher Enviar.

As contas de gerenciamento e as contas de administrador delegado podem realizar tarefas administrativas privadas do marketplace, como criar experiências, atualizar configurações de identidade visual, associar ou desassociar públicos, adicionar ou remover produtos e aprovar ou recusar solicitações pendentes.

Acesso confiável e função vinculada ao serviço

O administrador da conta de gerenciamento pode ativar os seguintes recursos para seu mercado privado.

> **Note**
>
> Os clientes atuais do mercado privado podem ativar as configurações do seu mercado privado navegando até a página do administrador do Private Marketplace e escolhendo Configurações. Ao habilitar o acesso confiável AWS Organizations e criar uma função vinculada ao serviço, você pode utilizar recursos, como associar OUs a experiências de mercado privado e registrar um administrador delegado. Quando ativadas, somente a conta de gerenciamento e a conta de administrador delegado podem criar e gerenciar experiências de mercado, com os recursos existentes transferidos para a conta de gerenciamento e compartilhados somente com o administrador delegado. Desativar o acesso confiável removerá a governança do mercado privado de sua organização. Não há grupos de contas exibidos em seu mercado privado. Para visualizar a governança da sua organização em diferentes níveis, use a página Estrutura da organização. Para perguntas ou suporte, entre em contato conosco.

- Acesso confiável — Você deve habilitar o acesso confiável paraAWS Organizations, o que permite que a conta de gerenciamento de uma organização forneça ou revogue o acesso aos AWS Organizations dados de um AWS serviço. Habilitar o acesso confiável é fundamental para que o

mercado privado se AWS Organizations integre e designe o mercado privado como um serviço confiável em sua organização.

- Função vinculada ao serviço — Você deve habilitar a função vinculada ao serviço do mercado privado, que reside na conta de gerenciamento e inclui todas as permissões que o mercado privado exige para descrever AWS Organizations e atualizar os recursos do mercado privado em seu nome. Para obter mais informações sobre a função vinculada ao serviço, consulte Usando funções para configurar o Private Marketplace em. AWS Marketplace

Criação de uma experiência de mercado privado

Seu mercado privado é composto por uma ou mais experiências de mercado privado. Uma experiência pode ser associada a toda a sua organização, a uma ou mais OUs ou a uma ou mais contas em sua organização. Se você não Conta da AWS é membro de uma organização, então você tem uma experiência de mercado privada associada a uma conta. Para criar seu mercado privado, navegue até Mercado privado, selecione a página Experiências à esquerda e escolha Criar experiência.

> **Note**
>
> Para usar o mercado privado comAWS Organizations, você precisa habilitar todos os recursos da organização. Para obter mais informações, consulte Habilitar todos os atributos na sua organização no Manual do usuário do AWS Organizations.
> Se você não Conta da AWS for membro de uma organização, não precisará de nenhuma etapa prévia para usar o mercado privado.

Sua experiência de mercado privado é criada sem produtos aprovados, sem elementos de marca e não está associada a nenhuma conta em sua organização. Por padrão, não está ativo. Os tópicos a seguir descrevem como trabalhar com sua experiência de mercado privado.

Adição de produtos à experiência de mercado privado

Para adicionar produtos a uma experiência de mercado privado

1. Na página do administrador do Mercado privado, selecione Experiências no painel de navegação esquerdo. Em seguida, na guia Produtos, escolha Todos os produtos do AWS Marketplace. Você pode pesquisar por nome do produto ou nome do vendedor.

2. Marque a caixa de seleção ao lado de cada produto a ser adicionado à loja privada e escolha Add to Private Marketplace (Adicionar à loja privada).

> **Note**
>
> Você também pode adicionar um produto diretamente da página de detalhes do produto escolhendo o botão Adicionar ao mercado privado no banner vermelho. Se o banner vermelho não estiver na página de detalhes do produto, o produto já está em seu mercado privado.

Você também pode adicionar vários produtos a várias experiências ao mesmo tempo escolhendo Adicionar ou remover produtos em massa no painel de navegação esquerdo.

Verificação de produtos na experiência de mercado privado

Para verificar se um produto está aprovado na experiência do mercado privado

1. Na página do administrador do Mercado privado, selecione Experiências no painel de navegação esquerdo.
2. Escolha Produtos aprovados. Todos os produtos aprovados são exibidos na lista de aprovados.

> **Note**
>
> Se você estiver usando uma conta associada à experiência que você está editando e a experiência estiver habilitada, você também poderá visualizar os produtos diretamente no console do AWS Marketplace (https://console.aws.amazon.com/marketplace). Todos os produtos em qualquer resultado de pesquisa exibem um selo de aprovação para aquisição se fizerem parte do seu mercado privado.

Personalização da experiência de mercado privado

As experiências são subconjuntos de produtos e marcas associadas que podem ter um ou mais públicos associados. Uma única experiência de mercado privado pode governar toda a organização se a experiência estiver associada à organização ou governar uma ou mais contas ou unidades organizacionais em sua organização.

Você pode gerenciar suas configurações de experiência na página do administrador do Private Marketplace em Experiências no painel esquerdo. Use esta página para visualizar e gerenciar todas as suas experiências ativas e arquivadas e criar novas experiências para seu mercado privado. Para cada experiência, você pode adicionar um logotipo, adicionar um título e personalizar a interface do usuário para usar o esquema de cores da sua organização.

Gerenciando audiências

Um público é uma organização ou um grupo de unidades organizacionais (OUs) ou contas que você pode associar a uma experiência de mercado privado. Você pode criar um público na página do administrador do Private Marketplace em Experiências no painel esquerdo.

Você pode associar um ou mais públicos a uma experiência. Quando você associa ou desassocia um público, isso pode mudar a experiência de governança de OUs e contas infantis. Use a página Estrutura da organização para ver as contas e OUs afetadas pela associação. Se você desativar o acesso confiável, seus públicos serão desassociados e toda a governança será removida.

> **Note**
>
> Você pode visualizar sua AWS Organizations hierarquia e gerenciar a governança de sua organização a partir de um mercado privado. Para controlar seu mercado privado em nível de unidade organizacional e registrar administradores delegados, habilite o acesso confiável e a função vinculada ao serviço na página Configurações. Para perguntas ou suporte, entre em contato conosco.

Configurar a loja privada

Quando estiver satisfeito com a lista de produtos da experiência, as configurações de marca do mercado e os grupos de contas associados, você poderá ativar seu mercado privado. Na página do administrador do AWSPrivate Marketplace, selecione Experiência no painel de navegação esquerdo e selecione a experiência que você deseja ativar. Na guia Configurações, você pode alterar o status do mercado privado entre Ativo (habilitado) e Não ativo (desabilitado).

Você também pode permitir que os usuários enviem solicitações de software com a opção Solicitações de software. Se as solicitações de software estiverem Ativadas (habilitadas), os usuários finais poderão escolher Criar solicitação na página de detalhes do produto para enviar uma solicitação ao administrador para disponibilizar o produto em seu mercado privado. As solicitações

de software são habilitadas por padrão, e a configuração só pode ser modificada enquanto o mercado privado estiver habilitado.

Quando seu mercado privado está ativo, os usuários finais podem comprar somente os produtos que você aprovou. Quando a loja privada estiver desabilitada, você manterá a lista de produtos. No entanto, desabilitar um mercado privado remove a restrição dos usuários na organização do AWS Organizations. Como resultado, eles podem assinar qualquer produto no AWS Marketplace público.

A criação de um mercado privado não interrompe a execução de imagens de máquina da Amazon (AMIs) ativas em execução nas instâncias do Amazon Elastic Compute Cloud (Amazon EC2). Como prática recomendada, garanta que todos os produtos do AWS Marketplace atualmente em uso em sua organização sejam incluídos em seu mercado privado. Também é uma prática recomendada ter um plano para interromper o uso de produtos não aprovados antes de ativar o mercado privado. Depois que o mercado privado estiver ativo, todas as novas assinaturas ou renovações serão regidas pelos produtos aprovados no catálogo do mercado privado.

Como trabalhar com produtos privados

Alguns produtos não estão disponíveis publicamente para busca no AWS Marketplace. Esses produtos só podem ser vistos quando você recebe uma oferta privada do vendedor. A oferta privada do vendedor inclui um link para o produto. Você pode adicionar o produto ao mercado privado a partir do banner na parte superior da página.

> **Note**
>
> Se você quiser assinar um produto privado de uma conta diferente em sua organização, o vendedor deve incluir sua Conta da AWS (para adicionar o produto ao mercado privado) e a conta do usuário (para assinar o produto) na oferta privada.

Para remover um produto privado do seu mercado privado, você deve entrar em contato com o suporte do AWS Marketplace.

Gerenciar solicitações de usuário

Você pode permitir que os usuários enviem solicitações de produtos a serem adicionados ao catálogo do mercado privado com o recurso de solicitação de software. Para fazer isso, navegue até a página do administrador do mercado privado, selecione Experiências no painel de navegação esquerdo e escolha a experiência que você deseja gerenciar. Na guia Produtos, escolha Solicitações

pendentes. Nessa página, é possível revisar solicitações que seus usuários fizeram para produtos a serem adicionados ao catálogo do mercado privado.

É possível adicionar qualquer número de produtos solicitados nessa página primeiro marcando a caixa de seleção ao lado do nome de cada produto solicitado e escolhendo Add to Private Marketplace (Adicionar à loja privada). Da mesma forma, também é possível recusar uma ou mais solicitações selecionadas escolhendo Decline (Recusar). Para visualizar mais informações sobre um produto (ou a solicitação de software), escolha Visualizar detalhes na coluna Detalhes dessa solicitação.

Ao recusar uma solicitação de produto, é possível adicionar um motivo e evitar solicitações futuras (bloquear) para esse produto. O bloqueio de um produto não impedirá que você adicione o produto à sua loja privada, mas impedirá que seus usuários solicitem o produto.

Arquivamento e reativação de uma experiência de mercado privado

Você pode remover uma experiência de mercado privado arquivando-a. As experiências arquivadas não podem ser atualizadas nem usadas para controlar contas na sua organização. Se você tiver públicos associados a uma experiência arquivada, poderá associá-los a uma experiência diferente. Se você decidir usar a experiência mais tarde, poderá reativá-la quando quiser. Administradores de contas de gerenciamento ou administradores delegados têm permissões para arquivar e reativar experiências.

> **Note**
>
> Antes de arquivar uma experiência, você deve desabilitá-la. Para obter informações sobre como desabilitar uma experiência, consulte Configuração do mercado privado.
> Se você é um cliente atual de um mercado privado sem a AWS Organizations integração com o mercado privado, os administradores da conta que criou a experiência têm permissões para arquivar e reativar experiências.

Para arquivar uma ou mais experiências de mercado privado

1. Na página do administrador do Mercado privado, selecione Experiências no painel de navegação esquerdo.
2. Na guia Experiências ativas, selecione uma ou mais experiências.
3. Escolha Arquivar experiência.

> **Note**
>
> Se uma ou mais experiências tiverem um status Ativo, você deverá colocá-las off-line escolhendo Colocar as experiências) off-line.

4. Para verificar se você deseja arquivar a experiência, digite **`confirm`** (tudo em minúsculas) na caixa de texto.
5. Selecione Archive (Arquivar).

> **Note**
>
> Você também pode arquivar uma experiência selecionando a experiência, escolhendo Arquivar experiência no modo Administrador na guia Configurações e escolhendo Salvar.

Para reativar uma ou mais experiências de mercado privado

1. Na página do administrador do mercado privado, selecione Experiências no painel de navegação esquerdo.
2. Na guia Experiências arquivadas, selecione uma ou mais experiências.
3. Escolha Reativar.
4. Para verificar se você deseja reativar a experiência, digite **`confirm`** na caixa de texto.
5. Escolha Reativar.

> **Note**
>
> Você também pode reativar uma experiência selecionando a experiência, escolhendo Reativar experiência no modo Administrador na guia Configurações e escolhendo Salvar.

Ofertas privadas

O recurso de oferta privada do vendedor do AWS Marketplace permite que você receba os preços do produto e termos do EULA de um vendedor que não está disponível publicamente. Você negocia preços e termos com o vendedor, e o vendedor cria uma oferta privada para a conta do AWS designada. Você aceita a oferta privada e começa a receber o preço e os termos de uso negociados.

Cada oferta privada tem preços e termos de licenciamento especificamente oferecidos à sua conta. O vendedor do produto amplia uma oferta privada para você, e a oferta tem uma data de validade definida. Se não aceitar a oferta privada até a data de validade, dependendo do tipo de produto da oferta privada, você será automaticamente movido para a oferta pública do produto ou não será mais inscrito no produto.

Se você estiver usando o recurso de faturamento consolidado no AWS Organizations, poderá aceitar a oferta privada da conta de gerenciamento da organização ou da conta de um membro. Se você aceitar na conta de gerenciamento, a oferta privada poderá ser compartilhada com todas as contas de membro da organização. As contas de membro que foram previamente assinadas no produto também devem aceitar a nova oferta privada para se beneficiar dos preços. Como alternativa, para produtos de AMI e contêiner, você pode compartilhar a licença da conta de gerenciamento com contas de membro usando o Gerenciador de licença da AWS. As contas de membro que não foram assinadas anteriormente no produto devem aceitar a oferta privada para poderem implantar o produto.

Para obter mais informações sobre o faturamento consolidado, consulte Faturamento consolidado para o AWS Organizations no Guia do usuário do AWS Billing. Veja a seguir os principais pontos a serem lembrados ao começar a usar suas ofertas privadas.

- Os compradores do AWS Marketplace podem acessar serviços de financiamento de terceiros para ofertas privadas. Para obter mais informações, consulte O financiamento do cliente agora está disponível no AWS Marketplace.
- Não há diferença no produto de software que você compra usando uma oferta privada. O software comprado usando uma oferta privada se comportaria da mesma maneira que se você tivesse comprado o software sem uma oferta privada.
- As assinaturas de produtos adquiridas com uma oferta privada são exibidas como qualquer outro produto do AWS Marketplace em sua fatura mensal. É possível usar o faturamento detalhado para visualizar seu uso de cada produto comprado no AWS Marketplace. Cada uma das suas ofertas privadas tem um item de linha correspondente a cada tipo de uso.

- Assinar uma oferta privada não exige a execução de uma nova instância do software. Aceitar a oferta privada modifica o preço de acordo com o preço da oferta privada. Se um produto oferecer execução com 1 clique, será possível implantar uma nova instância do software. Se um produto assumir a execução com 1 clique como padrão, será possível aceitar uma oferta privada sem iniciar uma nova instância. Para iniciar sem implantar uma nova instância, escolha Manual Launch (Execução manual) na página de cumprimento. É possível usar o console do Amazon Elastic Compute Cloud para implantar instâncias adicionais, da mesma forma que faria para outros produtos do AWS Marketplace.
- Quando o vendedor estende a você uma oferta privada, você recebe uma confirmação na conta que ele incluiu em uma oferta privada. As ofertas privadas são vinculadas à conta específica do comprador de software listado. O vendedor do software cria a oferta privada para a conta especificada por você. Cada oferta privada pode ser constituída de até 25 contas.
- Quando você aceita uma oferta privada, ela se torna um acordo (também conhecido como contrato ou assinatura) entre você e o vendedor.
- Os vendedores podem oferecer a atualização ou a renovação da sua compra de um contrato de SaaS ou um contrato de SaaS com produto de consumo. Por exemplo, um vendedor pode criar uma nova oferta privada para conceder novos direitos, oferecer descontos na definição de preço, ajustar programações de pagamento ou alterar o contrato de licença de usuário final (EULA) para usar termos de licença padronizados.

  Essas renovações ou atualizações são feitas na oferta privada original aceita, e você usa o mesmo processo para aceitá-las. Se você aceitar a nova oferta privada de atualização ou renovação, os novos termos do contrato entrarão em vigor imediatamente, sem qualquer interrupção no serviço de software. Quaisquer termos anteriores ou pagamentos programados restantes serão cancelados e substituídos pelos termos deste novo acordo.
- É possível analisar todas as suas assinaturas anuais no AWS Marketplace em Your Software (Seu software). Se uma assinatura anual for adquirida por uma conta usando o AWS Organizations para o faturamento consolidado, ela será compartilhada com toda a família de contas vinculadas. Se a conta compradora não tiver instâncias em execução, a assinatura anual será contada em relação ao uso em outra conta vinculada que executa esse software. Para obter mais informações sobre assinaturas anuais, consulte the section called “Assinaturas de AMI”.
- Quando uma oferta privada expira, você não pode assiná-la. No entanto, você pode entrar em contato com o vendedor. Peça ao vendedor que altere a data de validade da oferta atual para uma data futura ou crie uma nova oferta privada para você.

Tipos de produto qualificados para ofertas privadas

Você pode obter ofertas privadas para os seguintes tipos de produto.

Tipo de oferta	Descrição
Produtos de dados	Para obter mais informações, consulte Aceitação de uma oferta privada no Guia do usuário do AWS Data Exchange.
Contrato de SaaS	Com um contrato de software como serviço (SaaS), você pode confirmar o pagamento antecipado da utilização esperada de um produto SaaS ou negociar uma programaç ão de pagamento flexível com o vendedor. As durações do contrato são de um mês, um ano, dois anos ou três anos, ou selecione uma duração personalizada em meses, até 60 meses. Se você confirmar um pagamento antecipado, será cobrado antecipadamente pelo uso do software do produto. Se o vendedor oferecer uma programação de pagamento flexível, você será cobrado nas datas da programação de pagamento de acordo com os valores listados na oferta privada. O vendedor também pode incluir preços negociados com pagamento conforme o uso acima do uso contratado.
Assinatura de SaaS	Com uma assinatura de SaaS, você concorda com um preço pelo uso de um produto. O vendedor controla e informa seu uso para o AWS Marketplace, e você será cobrado pelo que usa.

Tipo de oferta	Descrição
AMI por hora	Com a imagem de máquina da Amazon (AMI) por hora, você negocia uma taxa horária para usar uma AMI, arredondada para a hora mais próxima.
AMI por hora com anual	Com a AMI por hora com anual, você negocia os preços por hora e a longo prazo por tipo de instância. O preço de longo prazo é para a duração da oferta privada, que pode ser entre 1 dia e 3 anos. Se o vendedor criar uma oferta privada sem um cronograma de pagamento flexível, você poderá executar instâncias do Amazon EC2 pelo preço por hora determinado na oferta privada e, se desejar, comprar compromissos antecipados durante o contrato pelo preço de longo prazo definido na oferta privada. Se o vendedor criar uma oferta privada com uma programação de pagamento flexível, você será cobrado nas datas da programação de pagamento de acordo com os valores listados na oferta privada, independe ntemente do uso. Nesse tipo de oferta privada, o vendedor pode incluir várias instâncias do Amazon EC2 por tipo de instância que você pode executar sem a cobrança do preço por hora. Qualquer uso acima do que está incluído é cobrado pelo preço por hora definido na oferta privada.

Tipo de oferta	Descrição
Contrato da AMI	Com os contratos da AMI, você negocia o preço do contrato e a duração do contrato, que pode ser entre 1 e 60 meses. Se o vendedor criar uma oferta privada sem um cronogram a de pagamento flexível, no momento da aceitação, você poderá configurar o contrato de acordo com o preço e as opções definidas na oferta privada. Se o vendedor criar uma oferta privada com uma programação de pagamento flexível, você será cobrado nas datas da programação de pagamento de acordo com os valores listados na oferta privada. Nesse tipo de oferta privada, o vendedor configura o contrato na oferta privada e não pode configurá -lo no momento da aceitação.
Produtos de contêiner	Com produtos de contêiner, você negocia preços por hora ou anualmente para os produtos de contêiner que usa, por pod, tarefa ou unidade personalizada, de acordo com o produto que está comprando. As ofertas privadas de produtos de contêiner correspon dem às ofertas privadas de produtos da AMI.
Produtos de machine learning	As ofertas privadas podem ser um contrato com uma taxa inicial fixa por um determinado número de dias. No final do contrato, todas as instâncias que continuarem em execução serão cobradas de acordo com a taxa horária definida pelo vendedor na oferta privada.

Tipo de oferta	Descrição
Serviços profissionais	Todas as ofertas de serviços profissionais são ofertas privadas. Você deve trabalhar com o comprador para criar a oferta privada. Consulte Produtos de serviços profissionais para obter mais informações.

Preparar-se para aceitar uma oferta privada

Quando uma oferta privada típica é negociada, você paga o valor total da oferta ao aceitá-la, a menos que esteja usando financiamento de terceiros. Com o financiamento de terceiros, o financiador paga o contrato em seu nome e cobra você com base no cronograma de pagamento acordado. Antes de aceitar uma oferta privada, verifique a estrutura de faturamento da sua empresa, seu método de pagamento de faturamento do AWS e suas configurações de imposto.

Verificar as preferências do AWS Billing and Cost Management

O Billing and Cost Management é o serviço que você usa para pagar a fatura da AWS, monitorar o uso e controlar os custos. Você pode usar o recurso de faturamento consolidado no AWS Organizations para consolidar o faturamento e o pagamento de várias contas da Amazon Internet Services Pvt. Ltd. (AISPL). Toda organização no AWS Organizations tem uma conta de gerenciamento que paga as despesas de todas as contas de membro. A conta de gerenciamento é chamada de conta pagante, e a conta de membro é chamada de conta vinculada. Antes de negociar uma oferta privada, verifique como sua empresa paga a fatura da AWS e para qual conta da AWS é a oferta privada.

Verificar seu método de pagamento

Antes de aceitar uma oferta privada, verifique se o método de pagamento permite pagar todo o custo da oferta privada. Para verificar o método de pagamento, abra o console do Gerenciamento de Faturamento e Custos em https://console.aws.amazon.com/billing/.

Verificar as configurações fiscais

Se sua empresa se qualificar para uma isenção fiscal, verifique suas configurações de imposto. Para visualizar ou modificar suas configurações fiscais, faça login no AWS Management Console e, nas

configurações da conta, visualize as configurações de imposto. Para obter mais informações sobre o registro de impostos, consulte Como faço para adicionar ou atualizar meu número de registro fiscal ou o endereço legal da empresa para minha conta da AWS?.

Visualizar e assinar uma oferta privada

Você pode ver uma oferta privada de uma das seguintes maneiras:

Tópicos

- Visualizando e assinando uma oferta privada em uma lista de ofertas privadas
- Visualizar e assinar uma oferta privada em um link fornecido pelo vendedor
- Visualizar e assinar uma oferta privada na página do produto

Visualizando e assinando uma oferta privada em uma lista de ofertas privadas

Para visualizar e assinar uma oferta privada em uma lista de ofertas privadas estendidas para a Conta da AWS

1. Faça login no console do AWS Marketplace.
2. Navegue até a página Ofertas privadas.
3. Na página Ofertas privadas, na guia Ofertas disponíveis, selecione o ID da oferta para a oferta de interesse.
4. Veja e assine a oferta privada.

Visualizar e assinar uma oferta privada em um link fornecido pelo vendedor

Para ver e assinar uma oferta privada em um link que o vendedor enviou para você

1. Faça login no console do AWS Marketplace.
2. Siga o link enviado pelo vendedor para acessar diretamente a oferta privada.

> **Note**
>
> Seguir esse link antes de fazer login na conta correta resultará em um erro de Página não encontrada (404).

Para obter mais informações, consulte Recebo um erro Página não encontrada (404) quando clico no ID da oferta para ver a oferta privada.

3. Veja e assine a oferta privada.

Visualizar e assinar uma oferta privada na página do produto

Para ver e assinar uma oferta privada na página do produto

1. Faça login no console do AWS Marketplace.
2. Navegue até a página do produto.
3. Veja o banner na parte superior da página mostrando a oferta privada, o ID e a validade da oferta.

> **Note**
>
> As ofertas privadas com datas futuras são listadas como renovações antecipadas. Para obter mais informações, consulte the section called “Trabalhar com contratos com data futura”.

4. Selecione o ID da oferta.
5. Veja e assine a oferta privada.

> **Note**
>
> Se você tiver mais de uma oferta privada para esse produto, cada oferta aparece em Offer name (Nome da oferta). Se você tiver um contrato atual para esse produto, um ícone Em uso aparecerá ao lado dessa oferta.

Solução de problemas de ofertas privadas

Se você encontrar problemas de código de status HTTP 404 (Não encontrado) ou dificuldades semelhantes ao trabalhar com Ofertas privadas no AWS Marketplace, consulte os tópicos nesta seção.

Problemas

- Recebo um erro Página não encontrada (404) quando clico no ID da oferta para ver a oferta privada
- Nenhuma dessas sugestões funciona

Recebo um erro Página não encontrada (404) quando clico no ID da oferta para ver a oferta privada

- Verifique se você acessou a Conta da AWS correta. O vendedor estende ofertas privadas para IDs específicos da Conta da AWS.
- Verifique se a oferta existe em Ofertas privadas no console do AWS Marketplace. Se você não encontrar a oferta em Ofertas privadas, pode ser porque o vendedor estendeu a oferta para um ID de Conta da AWS diferente. Verifique com o vendedor para confirmar o ID da Conta da AWS para o qual a oferta foi estendida.
- Verifique se a oferta privada não expirou visualizando a guia Ofertas aceitas e expiradas em Ofertas privadas no console do AWS Marketplace. Se a oferta tiver expirado, trabalhe com o vendedor para modificar a data de validade da oferta ou estender uma nova oferta à sua conta.
- Verifique se o ID da conta está na lista de permissões para ver a oferta privada. Alguns ISVs usam listas limitadas. Pergunte ao ISV se ele colocou sua conta na lista de permissões para visualizar o produto. A inclusão na lista de permissões é necessária para listas limitadas de produtos de AMI. Se você estiver em uma organização da AWS e o vendedor estender a oferta para a conta de gerenciamento, as contas vinculadas deverão estar na lista de permissões para assinatura. Caso contrário, as contas vinculadas do comprador que não estão na lista de permissões receberão o erro Página não encontrada (404) ao tentar visualizar a oferta.
- Consulte o administrador da AWS para confirmar se você tem permissões `aws-marketplace:ViewSubscriptions` do IAM se precisar ver a oferta. Para obter mais informações sobre a segurança do AWS Marketplace, consulte Segurança no AWS Marketplace.
- Verifique se você está usando um mercado privado.
  - Certifique-se de que o produto esteja na lista de permissões do seu mercado privado (se aplicável), para que você possa comprar o produto. Se você não tiver certeza, entre em contato com o administrador do sistema para verificar.

Nenhuma dessas sugestões funciona

Se nenhuma das sugestões anteriores resolver o erro do código de status HTTP 404 (Não encontrado), tente as seguintes ações no seu navegador:

- Limpe o cache.
- Exclua os cookies.
- Saia e, em seguida, entre novamente.
- Use um modo de navegação anônima ou privada.
- Tente um navegador diferente. Nós não recomendamos usar o Internet Explorer.

Se você concluiu todas as sugestões de solução de problemas e ainda está recebendo um erro de Página não encontrada, envie uma mensagem de e-mail para <mpcustdesk@amazon.com> para obter ajuda.

Página de ofertas privadas no AWS Marketplace

No AWS Marketplace, a página Ofertas privadas lista todas as ofertas privadas que foram estendidas para a sua Conta da AWS para produtos públicos e privados. Todas as ofertas disponíveis para você são exibidas para cada produto. Você pode aceitar uma oferta para cada produto.

Noções básicas da página Ofertas privadas

Você pode ver a página Ofertas privadas fazendo login no console do AWS Marketplace e navegando até Ofertas privadas. As ofertas privadas estendidas para a sua Conta da AWS estão listadas em Ofertas privadas, incluindo o ID da oferta, o produto, o vendedor registrado (ISV ou parceiro de canal), o publicador, os contratos ativos (se aplicável) e a data de validade da oferta. Você pode selecionar o ID da oferta de interesse para ver os detalhes da oferta e assinar uma oferta privada.

A página Ofertas privadas inclui as seguintes informações:

- A guia Ofertas disponíveis lista as ofertas privadas estendidas à sua conta que estão disponíveis para aceitação. O link do ID da oferta nessa guia é o mesmo link que o vendedor pode ter fornecido a você para acessar os detalhes da oferta privada.
- A guia Ofertas aceitas e expiradas lista as ofertas que você aceitou e resultaram na criação de um contrato. Ela também lista as ofertas que atingiram a data de validade definida pelo

vendedor. Essa guia pode ser útil para recuperar um ID de oferta e um ID de contrato anteriores (se disponíveis) ao renovar com um vendedor. Se a oferta resultou em um contrato e o contrato está ativo, você pode escolher o contrato para ver a página de detalhes da assinatura.

> **Note**
>
> As ofertas privadas com datas futuras são listadas como renovações antecipadas. Para obter mais informações, consulte the section called “Trabalhar com contratos com data futura”.

Para obter mais informações sobre como modificar, atualizar ou renovar uma oferta privada, consulte Modificar ou cancelar a assinatura de uma oferta privada.

Permissões necessárias para visualizar a página Ofertas privadas

Para visualizar a página Ofertas privadas no console do AWS Marketplace, você deve ter as seguintes permissões:

- Se você usa políticas gerenciadas pela AWS: `AWSMarketplaceRead-only`, `AWSMarketplaceManageSubscriptions` ou `AWSMarketplaceFullAccess`
- Se você não estiver usando políticas gerenciadas pela AWS: ação do IAM `aws-marketplace:ListPrivateListings` e `aws-marketplace:ViewSubscriptions`

Se você não conseguir visualizar a página Ofertas privadas, entre em contato com o administrador para configurar as permissões corretas do AWS Identity and Access Management (IAM). Para obter mais informações sobre as permissões necessárias do IAM para o AWS Marketplace, consulte Políticas gerenciadas pela AWS para compradores do AWS Marketplace.

Assinatura de uma oferta privada de SaaS

Para uma oferta privada de software como serviço (SaaS), as opções de configuração disponíveis dependem do contrato que você pode negociar com o vendedor.

Conforme mostrado no diagrama a seguir, a página Oferta privada inclui as seguintes seções:

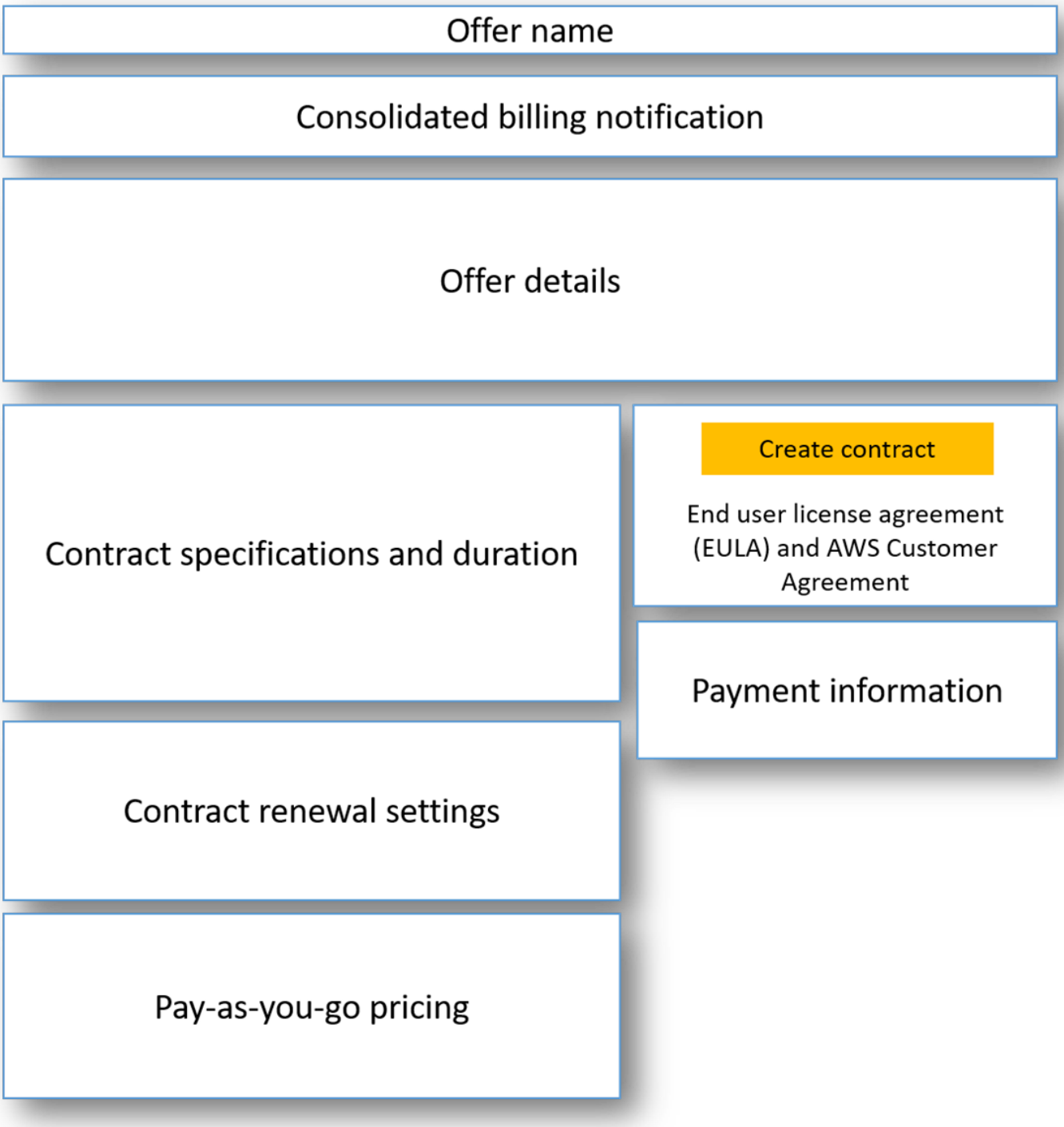
- Nome da oferta: este é o nome que o vendedor deu para a oferta privada quando a criou.

- Informações de faturamento consolidado: essa notificação vai aparecer se você estiver usando faturamento consolidado com Contas da AWS.
- Especificações e duração do contrato: esse painel mostra a duração da oferta e as dimensões que definem a oferta. As dimensões descrevem como o uso é medido e por quanto tempo o preço negociado está em vigor: por exemplo, 5 GB/dia por 12 meses ou US$ 0,01 por usuário por hora. Se a oferta privada for um contrato, você pagará uma quantia acordada de uso ao longo da vigência do contrato. Se a oferta privada por uma assinatura, você pagará pelo uso medido na taxa acordada.

> **Note**
>
> As ofertas privadas com datas futuras são listadas como renovações antecipadas. Para obter mais informações, consulte the section called “Trabalhar com contratos com data futura”.

- Configurações de renovação do contrato: você não pode configurar a renovação automática das ofertas privadas. Para ofertas privadas de produtos SaaS, esse painel sempre indica que não há renovação para essa oferta.
- Preço conforme o uso: se você negociar a definição de preço para o uso de produtos além do que é definido na oferta privada, as especificações de custo de quantidade de uso adicional aparecerão aqui. Por exemplo, se você aceitou um contrato de SaaS para armazenamento físico de dados de 5 GB/dia por 12 meses e usar 10 GB/dia, os primeiros 5 GB serão abrangidos pelo contrato. Os 5 GB/dia adicionais são cobrados conforme o uso. Com assinaturas de SaaS, você tem uma taxa acordada para quantidade de uso durante a vigência do contrato.
- Contrato de licença de usuário final (EULA) e botão de criação de contrato: é aqui que você pode ver o contrato de licença que o vendedor enviou para esta oferta privada. Aqui você também aceita o contrato após ter visualizado todas as especificações de ofertas privadas e está pronto para iniciar o contrato.
- Informações de pagamento: este painel descreve quando o pagamento é devido e, se você negociou uma programação de pagamento, a data e hora em que o pagamento deve ser feito.

> **Important**
>
> Se uma seção não aparecer na página Oferta privada, ela não é uma parte negociada da oferta privada.



Para assinar uma oferta privada de SaaS

1. Siga as etapas em Visualizar e assinar uma oferta privada.

2. No painel de detalhes da oferta, verifique se você escolheu a oferta privada correta. Você pode ter várias ofertas para o produto.
3. No painel de especificação e duração do contrato, verifique se a duração e os detalhes do contrato são o que você negociou. Se não forem, verifique se você selecionou a oferta privada correta ou entre em contato com o vendedor que criou a oferta.

   > **Note**
   >
   > As ofertas privadas com datas futuras são listadas como renovações antecipadas. Para obter mais informações, consulte the section called “Trabalhar com contratos com data futura”.

4. Se você negociou o preço como pagamento conforme o uso, deve haver um painel com informações que descreve os termos negociados. Verifique as informações ou, se estiverem ausentes (e você esperava encontrá-las), entre em contato com o vendedor.
5. No painel de informações de pagamento, verifique as informações de pagamento. Se você negociou um cronograma de pagamento flexível, as datas e os valores de pagamento serão listados. Se não tiver feito isso, o valor total do contrato será cobrada quando você aceitar a oferta.
6. No painel de criação do contrato e EULA, verifique se o EULA é aquele que você negociou com o vendedor. Depois de revisar todos os termos e condições do contrato, escolha Criar contrato para aceitar a oferta.

Depois de aceitar a oferta, uma página de confirmação será aberta, indicando que você se inscreveu com êxito no produto. Escolha Configurar sua conta para ser redirecionado para a página do vendedor e concluir a configuração de sua conta no site do vendedor.

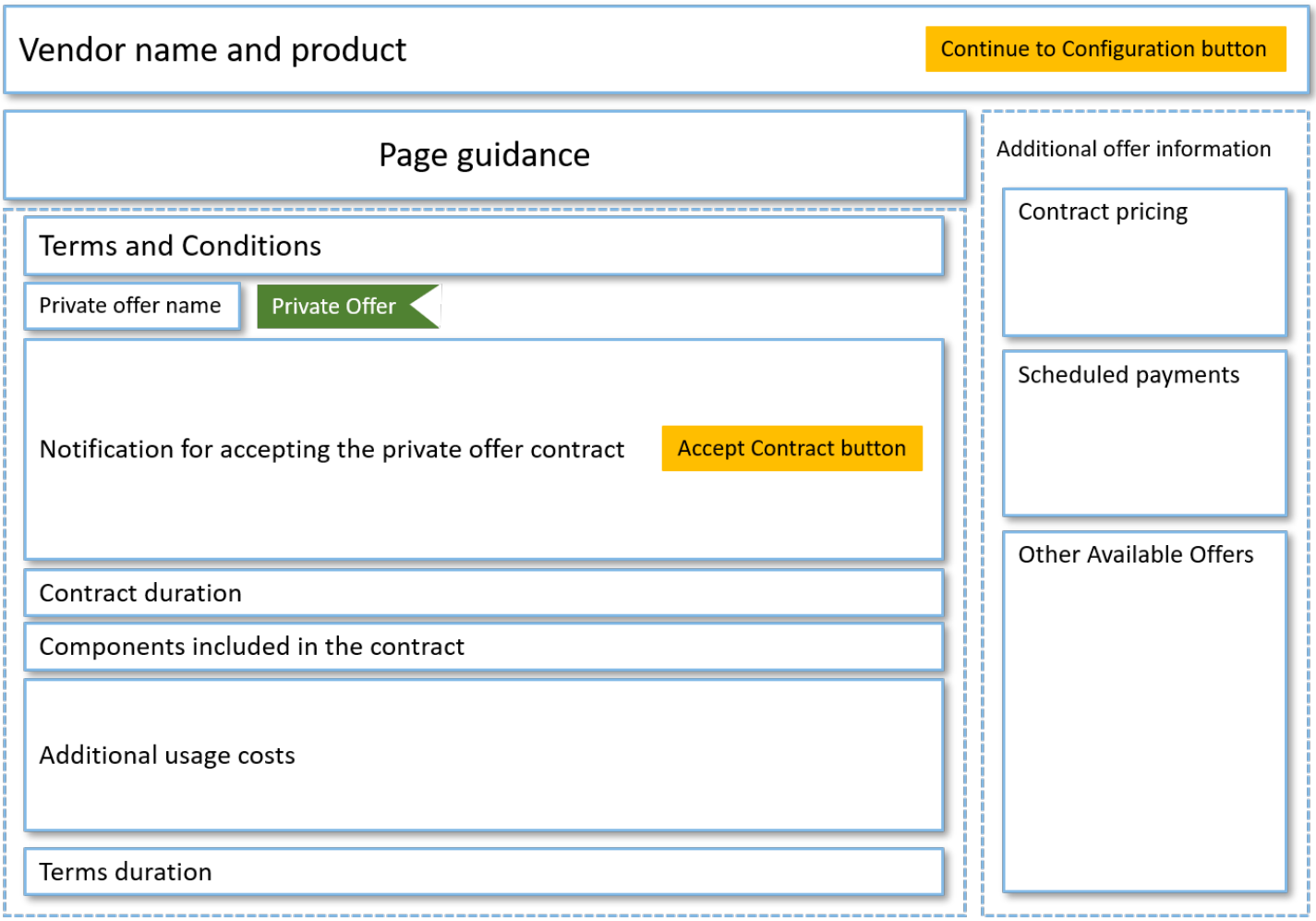
Assinar uma oferta privada de AMI

As seções e as opções de configuração disponíveis para sua oferta privada de imagem de máquina da Amazon (AMI) dependem do contrato que você negociar com o fornecedor do produto. A imagem a seguir mostra o layout de uma página de oferta privada da AMI no site do AWS Marketplace.

Conforme mostrado no diagrama a seguir, a página Oferta privada inclui as seguintes seções:

- Nome do fornecedor e produto: este é o nome do fornecedor e o produto relacionado à oferta privada. O botão de configuração do produto está à direita.

- Orientação da página: essa área tem orientações para concluir as tarefas na página e aceitar a oferta privada.
- Termos e condições: essa seção inclui as seguintes informações:
  - Na parte superior esquerda, encontramos o nome da oferta privada e um rótulo que indica que esta é uma oferta privada.
  - Abaixo da seção do nome da oferta privada, há uma notificação para aceitar o contrato. Você pode usar o botão Aceitar contrato para aceitar a oferta privada.
  - Abaixo da seção de notificação, há seções sobre a duração do contrato, os componentes incluídos no contrato e o preço da instância que você negociou, além de outra oportunidade de visualizar ou baixar o EULA.
- Duração dos termos: esta seção mostra o número de dias do contrato e a data de término do contrato.
- Informações adicionais sobre a oferta: à direita estão imagens em miniatura do preço total do contrato, seu próximo pagamento agendado, os termos atuais e outras ofertas públicas e privadas disponíveis.



Assinatura de uma oferta privada anual da AMI com um cronograma de pagamento flexível

Para assinar uma oferta privada da AMI, você deve aceitar a oferta privada no site do AWS Marketplace. Você não pode aceitar a oferta privada no console do AWS Marketplace ou do console do Amazon Elastic Compute Cloud (Amazon EC2). Se o vendedor criar uma oferta privada com uma programação de pagamento flexível, você será cobrado nas datas da programação de pagamento de acordo com os valores listados na oferta privada. Para aceitar uma oferta privada da AMI com um cronograma de pagamento flexível, use o procedimento a seguir.

Para aceitar uma oferta privada da AMI com um cronograma de pagamento flexível

1. Siga as etapas em Visualizar e assinar uma oferta privada.

2. Verifique se você está visualizando a oferta privada correta. O fornecedor pode criar várias ofertas privadas do produto dele para você. Todas as ofertas privadas adicionais aparecem na seção Outras ofertas disponíveis.
3. Verifique se a data de validade da oferta e as informações de preço são o que você negociou para a oferta privada. Se não forem, verifique se você está visualizando a oferta privada correta.
4. Baixe o EULA e verifique se ele é o que você negociou para a oferta privada.
5. Na seção Duração dos termos, verifique se os termos da oferta privada são o que você negociou.
6. Depois de verificar os detalhes da oferta privada, na seção Termos e condições, escolha Aceitar contrato.
7. Revise os termos e escolha Confirmar se você aceitar.

> **Important**
>
> Não atualize o navegador enquanto o sistema processa a solicitação do seu contrato.

Quando você estiver pronto para configurar a AMI, escolha Continue to Configuration (Continuar configuração). Você deve concluir o processo de assinatura para cada uso do produto.

Assinatura de uma oferta privada anual da AMI sem um cronograma de pagamento flexível

Para assinar uma oferta privada da AMI, você deve aceitar a oferta privada no site do AWS Marketplace. Você não pode aceitá-las no console do AWS Marketplace ou no console do Amazon EC2. Se o vendedor criar uma oferta privada sem um cronograma de pagamento flexível, no momento da aceitação, você poderá configurar o contrato de acordo com o preço e as opções definidas na oferta privada. Para aceitar uma oferta privada da AMI sem um cronograma de pagamento flexível, use o procedimento a seguir.

Para aceitar uma oferta privada da AMI sem um cronograma de pagamento flexível

1. Verifique se você está visualizando a oferta privada correta. O fornecedor pode criar várias ofertas privadas do produto dele para você. As ofertas privadas adicionais aparecem no painel correspondente. Verifique se a oferta que você deseja aceitar aparece como Visualizando essa oferta.

> **Note**
>
> Em muitos casos, a conta pagante não é a conta que usa o produto. Recomendamos que você inicie o produto manualmente em vez de selecionar a opção de um clique se aceitar a oferta usando a conta pagante.

2. Verifique se a data de validade da oferta e as informações de preço são o que você negociou para a oferta privada. Se não forem, verifique se você está visualizando a oferta privada correta.
3. Baixe o EULA e verifique se ele é o que você negociou para a oferta privada.
4. No painel dos termos do contrato, verifique se os termos da oferta privada são o que você negociou.
5. Verifique se os detalhes da oferta são os que você negociou para a oferta privada e selecione Accept Terms (Aceitar termos). Se não forem, verifique se você está visualizando a oferta privada correta.
6. Em Inscrever-se neste software, em Tipo de instância, escolha uma opção na lista de tipos de instância disponíveis. Em Quantidade, escolha o número de licenças.
7. Revise suas seleções. Quando estiver satisfeito, selecione Criar contrato e Confirmar.

Quando você estiver pronto para configurar a AMI, escolha Continue to Configuration (Continuar configuração). Você deve concluir o processo de assinatura para cada uso do produto.

Modificar ou cancelar a assinatura de uma oferta privada

Você pode atualizar as assinaturas padrão de ofertas privadas e também pode modificar algumas ofertas privadas existentes no AWS Marketplace. O processo varia de acordo com o contrato em vigor.

Para muitas assinaturas, quando altera o preço público de uma oferta privada, você negocia a oferta com o ISV ou o parceiro do canal. Depois de aceitar a oferta privada, as assinaturas existentes relacionadas são transferidas automaticamente para o modelo de preços de ofertas privadas. Isso não exige ações adicionais da sua parte. Use as seguintes diretrizes para identificar o cenário e as etapas para começar a receber o preço da sua oferta privada.

Alteração da definição de preço da oferta pública para privada

Depois de aceitar a oferta privada, nenhuma ação adicional é necessária para o usuário que aceitou a oferta. Elas são alteradas para a definição de preço, os termos e as condições definidos na oferta privada. Para alternar para a definição de preço, os termos e as condições da oferta privada, cada usuário vinculado que usa o produto deve aceitar a oferta privada. Qualquer usuário que começar a usar o produto também deverá aceitar a oferta privada para obter a definição de preço, os termos e condições definidos na oferta privada.

Alteração de um contrato de SaaS: atualizações e renovações

Esta seção se aplica ao contrato de software como serviço (SaaS) e ao contrato de SaaS com produtos de consumo. Se você tiver um contrato ativo de uma oferta privada anterior e quiser aceitar uma nova oferta privada para o mesmo produto, o vendedor poderá atualizar ou renovar o contrato existente para modificar os termos, preços ou duração, ou renovar o contrato existente antes que ele termine. Isso resultará em uma nova oferta privada para você aceitar, sem precisar primeiro cancelar o contrato existente.

> **Note**
>
> As ofertas privadas com datas futuras são listadas como renovações antecipadas. Para obter mais informações, consulte the section called “Trabalhar com contratos com data futura”.

Para aceitar um upgrade ou renovação, você deve estar de acordo com os termos de faturamento. Se você não estiver cumprindo os termos de faturamento no momento, envie um ticket para o Atendimento ao Cliente da AWS para alterar o método de pagamento para faturamento.

Se não quiser mudar para o faturamento, você poderá realizar uma das seguintes ações:

- Trabalhar com o fornecedor do produto e a equipe de suporte ao cliente do AWS Marketplace para cancelar o contrato atual antes de aceitar uma nova oferta privada para esse produto
- Aceitar a oferta em outra Conta da AWS.

Alteração de uma assinatura de SaaS para um contrato de SaaS

Para mudar de uma assinatura de SaaS para um contrato de SaaS, você deve primeiro cancelar a assinatura de SaaS. Em seguida, você aceita a oferta privada para o contrato de SaaS. Para

visualizar suas assinaturas de SaaS existentes, escolha Software do Marketplace no canto superior direito do console do AWS Marketplace.

Alteração de um contrato de AMI para um novo contrato

Se você tiver um contrato de imagem de máquina da Amazon (AMI) em vigor em uma oferta privada anterior e quiser aceitar uma nova oferta privada para o mesmo produto, deverá fazer o seguinte:

- Aguarde o contrato de AMI atual expirar antes de aceitar o novo contrato de AMI.
- Trabalhe com o fornecedor do produto e a equipe de suporte ao cliente do AWS Marketplace para encerrar seu contrato atual.
- Aceite a oferta privada usando uma Conta da AWS diferente da que tem o contrato

Alteração de AMI por hora para AMI anual

Quando você muda de uma assinatura de AMI por hora para uma assinatura de AMI anual, ela funciona semelhante a um sistema de voucher. Cada hora de uso da AMI é compensada por uma unidade na assinatura de AMI anual. Quando você compra a assinatura anual por meio de uma oferta privada, todas as contas associadas que estão inscritas no produto mudam automaticamente para a definição de preço negociada na oferta privada. As contas vinculadas que iniciarem uma assinatura depois que a oferta privada entrar em vigor deverão ser inscritas na oferta privada durante a assinatura.

> **Note**
>
> As licenças anuais da sua antiga oferta são desativadas imediatamente após a aceitação dos termos da nova oferta. Trabalhe com o ISV para discutir a compensação das licenças antigas e como prosseguir com a nova oferta.

Alteração de AMI anual para AMI por hora

Quando sua assinatura anual expira, todas as contas vinculadas inscritas no produto são automaticamente alteradas para o preço de AMI por hora. Se uma assinatura anual estiver em vigor, a conta vinculada não poderá mudar para uma assinatura por hora para esse produto sem cancelar a assinatura.

Trabalhar com contratos com data futura e ofertas privadas

Com contratos com data futura (FDA) no AWS Marketplace, você pode assinar produtos cujo uso começa em uma data futura. Você pode gerenciar a compra de um produto independentemente de quando você paga e quando usa o produto.

O FDA ajuda os compradores a realizar as seguintes ações de forma independente para transações no AWS Marketplace:

- Adquira o produto e reserve o negócio aceitando a oferta.
- Comece o uso do produto (ativação de licença/direitos).
- Pague por uma compra (geração de fatura).

O FDA é compatível com ofertas privadas, criando produtos de software como serviço (SaaS), para contrato e contratos com preços de consumo (CCP), e com ou sem pagamentos flexíveis.

Ao usar contratos com data futura, lembre-se das seguintes datas:

Data de assinatura do contrato

A data em que você aceitou a oferta e quando o contrato foi criado. Essa data é quando o ID do contrato é criado.

Data de início do contrato

A data em que o uso do produto começa. Essa é a data futura ou data de início futura. Essa é a data em que sua licença/direito é ativado.

Data de término do contrato

A data em que o contrato termina. O contrato e a licença/direito expiram nessa data.

Para obter mais informações sobre como usar FDAs, consulte os seguintes tópicos:

Tópicos

Criação de contratos com data futura

Para contratos SaaS e contratos com preços de consumo, com e sem cronograma de pagamento flexível, o vendedor define a data de início do contrato como parte da geração de uma oferta privada. Como comprador, você deve trabalhar com os vendedores para garantir que a data de início atenda às suas necessidades.

Para criar um contrato com data futura, use o procedimento a seguir. Você pode ver seus contratos com data futura no console do AWS Marketplace na página Gerenciar assinaturas.

Para criar um contrato com data futura

1. Siga as etapas em Visualizar e assinar uma oferta privada.
2. No painel de detalhes da oferta, verifique se você escolheu a oferta privada correta e se a data de início do contrato está correta. As ofertas com datas futuras são marcadas como Renovações antecipadas no menu suspenso Oferta.

> **Note**
>
> Para produtos SaaS, na data de início do contrato, você deve concluir a configuração de sua conta com o ISV. Não é possível concluir esta etapa antes da data de início do contrato. Para obter mais informações, consulte the section called “Assinatura de uma oferta privada de SaaS”.

Usar um agendador de pagamentos flexível com contratos com data futura

Você pode usar o agendador de pagamentos flexível com contratos com data futura. Você pode configurar pagamentos para compras no momento de sua escolha, entre a data de assinatura do contrato e a data de término do contrato. Essa abordagem inclui pagamentos antes e depois da data de início do contrato.

O vendedor do registro que cria a oferta privada escolhe as datas e os valores de pagamento. Para obter mais detalhes, consulte Programador de pagamento flexível.

Alterar seus contratos com data futura

Você pode aumentar suas unidades adquiridas de uma dimensão específica em seu FDA antes e depois da data de início do contrato. Essa opção é possível quando o contrato não possui

cronograma de pagamento flexível. Para obter mais detalhes, consulte Programador de pagamento flexível.

Será cobrado de você o valor proporcional na data de início do contrato, quando sua alteração for concluída. Se a data de início já tiver passado, você será cobrado imediatamente.

Receber notificações para contratos com data futura

Você recebe notificações por e-mail que são enviadas para sua conta raiz designada sobre as seguintes ações tomadas em seus contratos com data futura:

- Aceitação da oferta e criação do acordo (data de assinatura do contrato)
- Após a ativação da licença ou do direito (data de início do contrato)
- Lembretes para contratos que expiram com 30, 60 ou 90 dias de antecedência
- Expiração do contrato (data de término do contrato)
- Mediante uma alteração ou substituição do contrato

Compartilhamento de assinaturas em uma organização

Quando você assina produtos no AWS Marketplace, é criado um contrato que concede a você uma licença para usar esses produtos. Se a sua Conta da AWS for membro de uma organização, você poderá compartilhar essa licença para produtos de imagem de máquina da Amazon (AMI), contêiner, machine learning e de dados com as outras contas dessa organização. Você deve configurar o suporte de licença no AWS Marketplace e, em seguida, compartilhá-lo no AWS License Manager.

> **Note**
>
> Para obter mais informações sobre o AWS Organizations, consulte o Guia do usuário do AWS Organizations.
> Para obter mais informações sobre o compartilhamento de licenças com sua organização no AWS License Manager, consulte Licenças concedidas no Guia do usuário do AWS License Manager.

O vídeo a seguir apresenta um passo a passo da experiência de compartilhar licenças.

Distribuir direitos de licença do AWS Marketplace (3:56)

Os tópicos a seguir descrevem o processo de visualização, compartilhamento e rastreamento de licenças entre contas.

Tópicos

- Pré-requisitos para compartilhar licenças
- Visualização das licenças
- Compartilhamento de licenças
- Rastreamento do uso da licença

Pré-requisitos para compartilhar licenças

Antes de compartilhar licenças no AWS Marketplace, você deve configurar o compartilhamento de licenças para sua organização. Conclua as tarefas a seguir para configurar o compartilhamento de licenças em sua organização:

- Dê permissão do AWS Marketplace para gerenciar licenças em seu nome para que ele possa criar as concessões de licença associadas ao comprar ou compartilhar suas licenças. Para obter mais informações, consulte Uso de funções para compartilhar direitos para o AWS Marketplace.
- Configure o AWS License Manager para o primeiro uso. Para obter mais informações, consulte Conceitos básicos do AWS License Manager no Guia do usuário do AWS License Manager.

Visualização das licenças

O AWS Marketplace cria automaticamente licenças para produtos de AMI, contêiner, machine learning, software como serviço (SaaS) e dados que você compra. Você pode compartilhar essas licenças com outras contas em sua organização.

> **Note**
>
> Embora as licenças sejam criadas para produtos de SaaS, o compartilhamento de licenças de SaaS não é aceito atualmente.

Você gerencia e compartilha licenças usando o AWS License Manager. No entanto, você pode usar o AWS Marketplace para visualizar as licenças dos produtos que comprou no AWS Marketplace.

Para ver as licenças dos produtos assinados no AWS Marketplace

1. No AWS Marketplace, faça login e escolha Gerenciar assinaturas.
2. Você pode ver todas as licenças ou ver a licença de uma assinatura específica.
    - Para visualizar todas as licenças
        - No menu Ações, selecione Exibir licenças para ver todas as licenças gerenciadas do AWS Marketplace no console do Gerenciador de licença.
    - Para visualizar as licenças de uma única assinatura
        a. Selecione o cartão do produto que você deseja visualizar para acessar a página de detalhes do produto.
        b. No menu Ações, selecione Exibir licença para visualizar a licença desse produto no console do Gerenciador de licença.

> **Note**
>
> Você também pode ver as licenças concedidas que foram agregadas a partir de todas as contas da organização. Para obter mais informações, consulte Licenças concedidas, no Guia do usuário do AWS License Manager.

Compartilhamento de licenças

Somente produtos de AMI, contêiner, machine learning e dados têm licenças que podem ser compartilhadas.

As assinaturas no AWS Marketplace têm um Nível de acesso mostrado nos detalhes do produto:

- Os produtos com um nível de Contrato têm uma licença que você pode usar e compartilhar com outras contas em sua organização.
- Produtos com um nível de Direito são licenças que foram compartilhadas com sua conta. Você pode usar esses produtos, mas não pode compartilhá-los.

O AWS Marketplace oferece suporte para concessões, que compartilham o uso de uma licença diretamente com o AWS Organizations, uma Conta da AWS ou com uma unidade organizacional usando o AWS License Manager. O processo de ativação da concessão agora inclui opções adicionais para substituir as concessões que são ativadas para o mesmo produto proveniente do AWS Marketplace. Para obter mais informações, consulte Licenças concedidas, no Guia do usuário do AWS License Manager.

> **Note**
>
> Para produtos restritos a Regiões da AWS específicas, uma conta com a qual você compartilha sua licença só poderá ativar a licença se a conta estiver dentro de uma região permitida.

Rastreamento do uso da licença

Você pode monitorar as métricas de licença com base no uso dos produtos de AMI do AWS License Manager selecionando a guia Painel de uso em cada licença respectiva.

Para obter mais informações sobre como usar o Gerenciador de licença para monitorar o uso da licença, consulte Licenças concedidas no Guia do usuário do AWS License Manager.

Notificações de compradores para eventos do AWS Marketplace

O AWS Marketplace fornece notificações em tempo hábil por e-mail, eventos do Amazon EventBridge e tópicos do Amazon Simple Notification Service (Amazon SNS).

Tópicos

Notificações por e-mail para eventos do AWS Marketplace

Como comprador no AWS Marketplace, você recebe uma notificação por e-mail quando ocorre uma das seguintes situações:

- Você aceita uma oferta.
- Um vendedor publica uma nova oferta privada relacionada à oferta privada que você aceitou anteriormente ou publica uma atualização da oferta aceita anteriormente.

> **Note**
>
> As notificações são enviadas para o endereço de e-mail que está associado ao ID da Conta da AWS do comprador.

Notificações do Amazon EventBridge para eventos do AWS Marketplace

O AWS Marketplace é integrado ao Amazon EventBridge, antigamente chamado de Amazon CloudWatch Events. O EventBridge é um serviço de barramento de eventos que você pode usar para facilitar a conexão de aplicações a dados de diversas origens. Para obter mais informações, consulte o Guia do usuário do Amazon EventBridge.

Como comprador, você recebe um evento do AWS Marketplace sempre que um vendedor cria uma oferta e a disponibiliza para compra. O evento contém detalhes como ID, data de validade, detalhes do produto e nome do vendedor.

Tópicos

Eventos da API Discovery no Amazon EventBridge para AWS Marketplace

Este tópico fornece informações detalhadas sobre cada evento listado na tabela a seguir.

Ação do vendedor	Evento recebido pelo comprador	Tópico relacionado
Cria uma oferta e a disponibiliza para compra	`Listing Available`	the section called “Eventos para novas listas”

Eventos para novas listas

Quando um vendedor cria uma oferta e a disponibiliza para compra, o comprador recebe um evento com o seguinte tipo de detalhe: `Listing Available`.

> **Note**
>
> Para obter mais informações sobre como criar regras do EventBridge, consulte Regras do Amazon EventBridge no Guia do usuário do Amazon EventBridge.

O seguinte é um exemplo do corpo de um evento `Listing Available`.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "Listing Available",
    "source": "aws.discovery-marketplace",
    "account": "123456789012",
    "time": "2023-08-26T00:00:00Z",
    "region": "us-east-1",
```

```
    "resources": [],
    "detail": {
        "requestId": "3d4c9f9b-b809-4f5e-9fac-a9ae98b05cbb",
        "catalog": "AWSMarketplace",
        "offer": {
            "id": "offer-1234567890123",
            "expirationDate": "2025-08-26T00:00:00Z"
        },
        "product": {
            "id": "bbbbaaaa-abcd-1111-abcd-666666666666",
            "title": "Product Title"
        },
        "sellerOfRecord": {
            "name": "Seller Name"
        }
    }
}
```

Integrar o AWS Marketplace a sistemas de compras

É possível configurar a integração do AWS Marketplace ao software de aquisição do Coupa ou do SAP Ariba. Após concluir a configuração, os usuários da sua organização podem usar o software de aquisição para buscar e solicitar uma assinatura de produtos do AWS Marketplace. Depois que a solicitação de assinatura for aprovada, a transação será concluída e o usuário será notificado de que a assinatura do software está disponível. Quando o usuário faz login no AWS Marketplace, o produto do software é listado como uma assinatura comprada e fica disponível para uso. A integração com seu sistema de compras também pode integrar as faturas do AWS Marketplace ao seu sistema de ordens de compra.

Como funciona a integração de compras

É possível configurar o software de compras para se integrar ao AWS Marketplace seguindo o protocolo cXML (commerce extensible markup language). Essa integração cria um ponto de acesso em um catálogo de terceiros, conhecido como conexão externa.

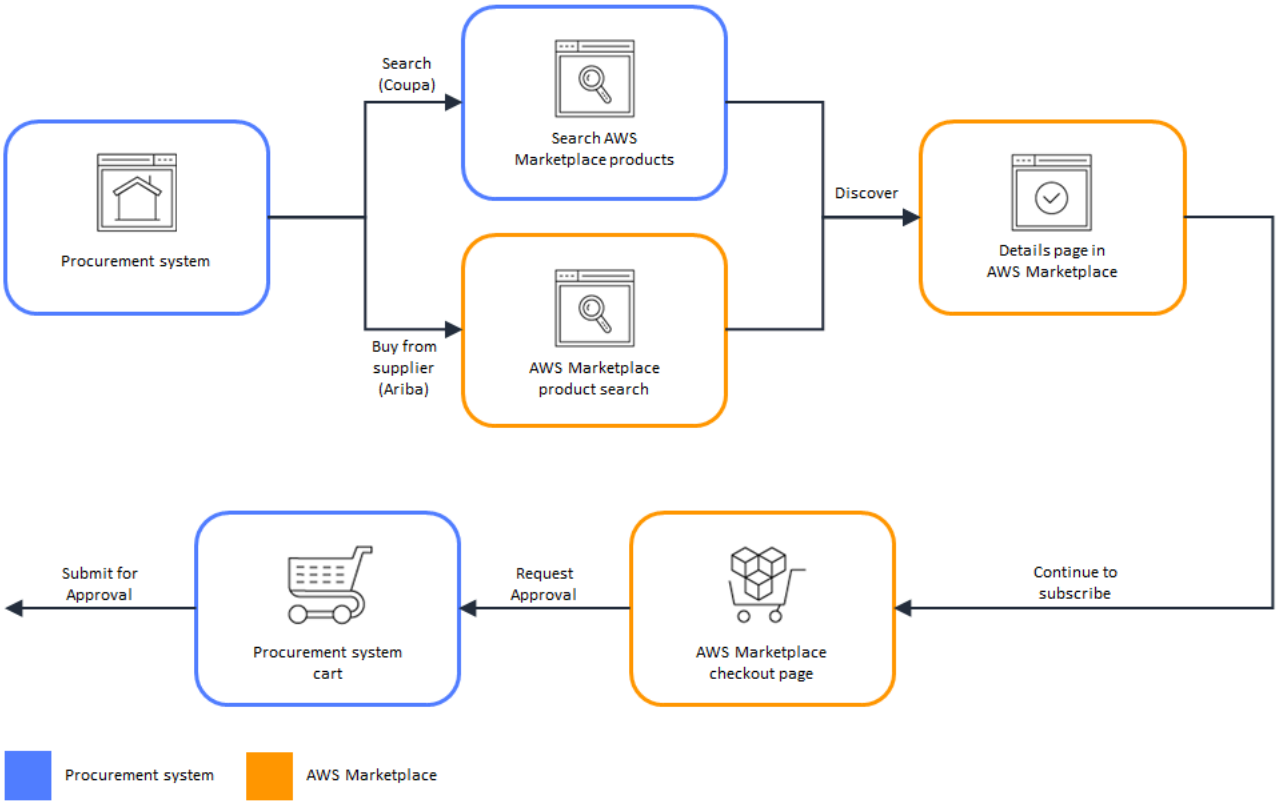
A integração é um pouco diferente, com base no sistema de compras:

- Coupa: usando o recurso Coupa Open Buy, você pode pesquisar o AWS Marketplace dentro do Coupa. O Coupa exibe os resultados da pesquisa e, quando o usuário escolhe um produto, ele é redirecionado ao AWS Marketplace para ver os detalhes. Como alternativa, os usuários do software de compras da Coupa podem acessar o catálogo do AWS Marketplace na seção Shop Online da página inicial. O usuário também pode optar por começar a procurar produtos diretamente no AWS Marketplace.
- SAP Ariba: o Ariba redireciona os usuários para o AWS Marketplace para pesquisar software e obter detalhes sobre um produto. Depois que um administrador configura a integração da conexão externa, os usuários do software de compras da Ariba podem encontrar o software AWS Marketplace escolhendo a guia Catálogo e, em seguida, selecionando o catálogo do AWS Marketplace. Isso os redireciona para o AWS Marketplace para encontrar os produtos nos quais estão interessados.

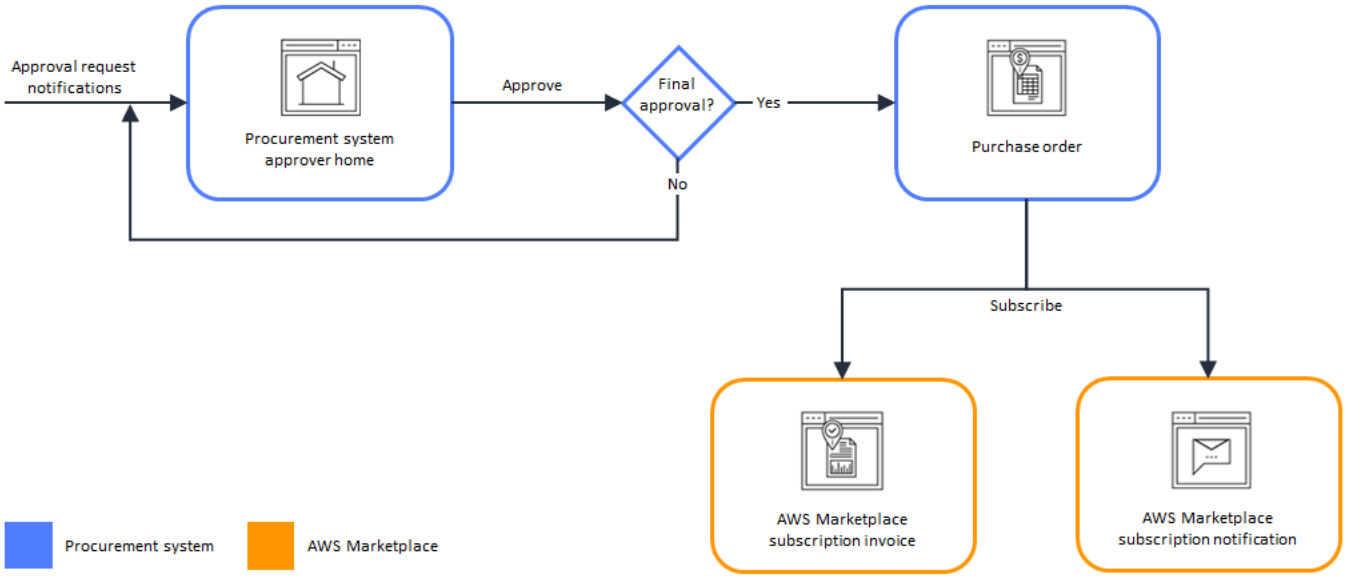
  Os usuários da Ariba devem iniciar as compras de dentro da Ariba, não no AWS Marketplace.

Quando o usuário quer comprar uma assinatura na qual está navegando no AWS Marketplace, ele cria uma solicitação de assinatura no AWS Marketplace. Na página de assinatura do produto, em vez

de concluir a compra, o usuário solicita a aprovação. A solicitação é enviada de volta a um carrinho de compras no sistema de compras para concluir o processo de aprovação. O diagrama a seguir mostra o processo de solicitação de assinatura do sistema de compras.



Quando o sistema de compras recebe a solicitação do AWS Marketplace, o sistema de aquisição inicia um fluxo de trabalho para concluir o processo de aprovação. Depois que a solicitação é aprovada, o sistema de ordens de compra do sistema de aquisição conclui automaticamente a transação no AWS Marketplace e notifica o usuário de que a assinatura está pronta para implantação. O solicitante não precisa retornar ao AWS Marketplace para concluir a compra. No entanto, talvez eles queiram retornar ao AWS Marketplace para obter instruções sobre como usar o produto que compraram. O AWS Marketplace envia uma mensagem de e-mail para a conta da AWS usada para acessar o AWS Marketplace. A mensagem de e-mail informa ao destinatário que a assinatura foi bem-sucedida e que o software está disponível por meio do AWS Marketplace. O diagrama a seguir mostra o processo de aprovação de solicitação de assinatura do sistema de compras.



As notas adicionais sobre a integração com sistemas de compras incluem o seguinte:

- As avaliações gratuitas não geram uma fatura no sistema de compras, porque não têm uma cobrança associada a elas.
- Os contratos que têm uma cobrança única, além do pagamento conforme o uso, podem exigir dois conjuntos de aprovações. Uma aprovação é para o preço do contrato (ou anual) e a outra para o preço por hora ou por unidade (pagamento conforme o uso).
- Clientes com PSI (integrações de sistemas de compras) podem ativar as pré-aprovações para produtos gratuitos e produtos BYOL. Há duas configurações, uma para produtos gratuitos e BYOL. Quando a configuração está habilitada, os pedidos são pré-aprovados no AWS Marketplace e os clientes não precisam enviar pedidos ao sistema de compras para aprovação. Quando a configuração estiver desabilitada, os clientes enviarão aprovações por meio do botão Solicitar aprovação para o sistema de compras. Quando a configuração de pré-aprovação para produtos gratuitos e BYOL está desabilitada, pedidos de USD 0,00 são produzidos no sistema de compras do cliente. Para obter mais informações sobre as integrações do sistema de compras, consulte https://aws.amazon.com/marketplace/features/procurementsystem

Configuração da integração do sistema de compras

Para configurar a integração entre o AWS Marketplace e seu sistema de compras, você inicia o processo no AWS Marketplace e o conclui no sistema de compras. É possível usar as informações

geradas no AWS Marketplace para configurar a conexão externa com o sistema de compras. Para concluir a configuração, as contas usadas devem atender aos seguintes requisitos:

- A Conta da AWS usada para concluir a configuração do AWS Marketplace deve ser a conta de gerenciamento e ter as permissões do AWS Identity and Access Management (IAM) definidas na política gerenciada pela `AWSMarketplaceProcurementSystemAdminFullAccess`.
- A conta do sistema de compras usada para concluir a configuração deve ter acesso administrativo para configurar um contrato, um fornecedor e uma conexão externa no sistema de compras.

Configurar permissões do IAM

As seguintes permissões do IAM estão na política gerenciada pela AWSpolítica gerenciada: AWSMarketplaceProcurementSystemAdminFullAccess e são necessárias para configurar a integração entre o AWS Marketplace e um sistema de compras.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Recomendamos o uso de permissões gerenciadas do IAM em vez de configurar permissões manualmente. O uso dessa abordagem é menos propenso ao erro humano e, se a permissão for alterada, a política gerenciada será atualizada. Para ter mais informações sobre como configurar e usar o IAM no AWS Marketplace, consulte Segurança no AWS Marketplace.

Configuração do AWS Marketplace para integração com o Coupa

Depois de configurar as permissões do IAM, você estará pronto para configurar a integração do AWS Marketplace com o Coupa. Navegue até Gerenciar compras. No painel Gerenciar sistemas de compras, insira um nome e uma descrição para a conexão externa. Também é possível mudar a integração para o modo de teste para que os usuários possam testar a integração sem criar assinaturas do produto até que você esteja pronto. Para configurar a parte do AWS Marketplace da integração, conclua o procedimento a seguir.

Para configurar o AWS Marketplace para integrar-se ao Coupa

1. Em Gerenciar sistemas de aquisição do AWS Marketplace, em Procurement systems (Sistemas de aquisição), selecione Set up Coupa integration (Configurar integração ao Coupa).
2. Na página Manage Coupa integration (Gerenciar integração ao Coupa), em Account information (Informações da conta), insira o nome e a descrição da sua integração.

   > **Note**
   >
   > Talvez você queira que suas faturas no console do AWS Billing façam referência à ordem de compra da Commerce Extensible Markup Language (cXML) usada para assinar o produto contratual de software como serviço (SaaS). Nesse caso, você pode habilitar a integração do faturamento usando uma função vinculada ao serviço nas configurações do AWS Marketplace.

3. Você pode ativar ou desativar as configurações para Habilitar redirecionamento e Modo de teste e, em seguida, selecionar Salvar para concluir a integração no sistema AWS Marketplace.

Depois de concluir a integração no AWS Marketplace, você deve continuar configurando a integração no Coupa. Use as informações geradas nessa página para configurar a conexão externa no sistema do Coupa.

A configuração do AWS Marketplace usa como padrão o modo de teste habilitado. No modo de teste, as solicitações de assinatura vão para o back-end do Coupa para que você possa ver o fluxo completo, mas a fatura final não é criada. Isso ajuda você a concluir a configuração e habilitar a conexão externa de maneira planejada.

> **Note**
>
> Você pode ativar ou desativar o modo de teste, conforme necessário.
> Não se esqueça de desativar o modo de teste quando terminar a integração. Caso contrário, os usuários do sistema parecerão estar criando solicitações, mas nenhum software será comprado.

Configurar o Coupa

Para configurar a integração ao AWS Marketplace no sistema do Coupa, copie as informações do painel Purchase information (Informações da compra) da página Manage Coupa integration (Gerenciar integração ao Coupa) no AWS Marketplace. Use essas informações para concluir as etapas nos links a seguir e para orientar você durante a configuração do sistema de compras Coupa.

- Configuração da conexão externa do Coupa
- Configuring a Supplier for cXML Purchase Orders

> **Note**
>
> Para obter informações sobre os códigos UNSPSC usados pelo AWS Marketplace, consulte Códigos UNSPSC usados pelo AWS Marketplace.

Configuração do AWS Marketplace para integração com o SAP Ariba

Para configurar a integração do AWS Marketplace com o Ariba, você deve trabalhar com a equipe de operações do AWS Marketplace para criar uma conexão externa de nível 1. Para obter mais informações sobre a conexão externa do SAP Ariba, consulte Introdução à conexão externa do SAP Ariba no site da SAP Community.

Colete as seguintes informações para se preparar para a configuração:

- O ID da sua Conta da AWS. Se a sua Conta da AWS faz parte de uma organização da AWS, o ID da conta de gerenciamento também é necessário.
- O ID de rede Ariba (ANID) do sistema SAP Ariba.

> **Note**
>
> Para obter informações sobre ANIDs no Ariba e respostas a outras perguntas sobre o Ariba, consulte a página Ariba Network for Suppliers: Frequently Asked Questions no site do SAP Ariba.

Para configurar o AWS Marketplace para integrar-se ao Ariba

1. Em Gerenciar sistemas de aquisição do AWS Marketplace, em Sistemas de compras, selecione Configurar integração ao Ariba.
2. Na página Gerenciar integração com o SAP Ariba, em Informações da conta, insira o nome e a descrição da integração, bem como o ID da rede SAP Ariba (ANID) do seu sistema Ariba.

   > **Note**
   >
   > Talvez você queira que suas faturas no console do AWS Billing façam referência à ordem de compra cXML usada para assinar o produto de contrato de SaaS. Nesse caso, você pode habilitar a integração do faturamento usando uma função vinculada ao serviço nas configurações do AWS Marketplace.

3. Verifique se o Modo de teste está habilitado e selecione Salvar para salvar as configurações de integração do AWS Marketplace.
4. Entre em contato conosco para iniciar o processo de criação da integração com o SAP Ariba. Inclua as informações acima. O AWS Marketplace envia instruções para configurar e testar a integração com o Ariba.

> **Note**
>
> Você precisa ter acesso de administrador ao sistema SAP Ariba para criar o relacionamento do fornecedor com o AWS Marketplace.

Seguindo as instruções e as configurações da equipe do AWS Marketplace, você cria a integração no ambiente de teste SAP Ariba, com o AWS Marketplace em execução no modo de teste. No ambiente de teste, as solicitações de assinatura vão para o back-end do Ariba para que você possa

ver o fluxo completo, incluindo as aprovações, sem criar uma assinatura no AWS Marketplace, e nenhuma fatura é gerada. Essa abordagem permite testar a configuração antes de habilitar a conexão externa na produção. Depois que o teste estiver concluído e você estiver pronto para começar a produção, entre em contato conosco para configurar a conta no ambiente de produção.

> **Note**
>
> Não se esqueça de passar para a produção quando terminar de testar a integração. Caso contrário, os usuários do sistema pensarão que estão criando solicitações, mas nenhum software será comprado.

Quando o teste estiver concluído e você tiver trabalhado com a equipe do AWS Marketplace para desativar o modo de teste, a integração estará concluída.

Para obter mais informações sobre como configurar o SAP Ariba, consulte os seguintes tópicos no SAP Ariba:

- Conexão externa do SAP Ariba no site do SAP Ariba
- Introdução à conexão externa do SAP Ariba no site da SAP Community

> **Note**
>
> Para obter informações sobre os códigos UNSPSC usados pelo AWS Marketplace, consulte Códigos UNSPSC usados pelo AWS Marketplace.

Códigos UNSPSC usados pelo AWS Marketplace

O AWS Marketplace usa o seguinte código United Nations Standard Products and Services (UNSPSC) para as listagens de software enviadas de volta ao carrinho de compra: 43232701

Desabilitação da integração a sistemas de compras

Para desabilitar a integração com o Coupa ou o SAP Ariba, você deve remover a integração da conexão externa do sistema de compras. Para fazer isso, desabilite a funcionalidade de redirecionamento automático do AWS Marketplace do Coupa ou do Ariba. Isso desabilita a integração, mas mantém as configurações e permite que ela seja reativada facilmente.

Se você precisar remover completamente a configuração de integração no AWS Marketplace, entre em contato conosco.

Avaliações gratuitas

Alguns dos produtos listados no AWS Marketplace oferecem avaliações gratuitas. A avaliação gratuita permite testar o software antes de comprá-lo. As avaliações gratuitas estão limitadas a um determinado tempo de uso gratuito ou por um período específico. Você não pode pausar um período de avaliação gratuita depois que ele começa.

Preços de software e infraestrutura

As avaliações gratuitas oferecidas pelos vendedores se aplicam somente aos preços de software de produtos listados no AWS Marketplace. Os compradores são responsáveis por todos os custos de infraestrutura ao usar o produto do vendedor no AWS Marketplace, independentemente de o preço do software incluir uma avaliação gratuita. Esses custos de infraestrutura são definidos pela AWS e estão disponíveis nas respectivas páginas de preços. Por exemplo, se você assinar um produto de imagem de máquina da Amazon (AMI) que tenha uma avaliação gratuita, não será cobrado pelo uso da AMI durante o período de avaliação. No entanto, você pode ser cobrado pela instância do Amazon Elastic Compute Cloud (Amazon EC2) na qual executa o produto de AMI.

> **Note**
>
> Alguns produtos podem exigir infraestrutura adicional da AWS para funcionar. Por exemplo, os vendedores podem fornecer instruções ou modelos de implantação que implantam balanceadores de carga, armazenamento, bancos de dados ou outros Serviços da AWS na sua Conta da AWS. Para entender quais Serviços da AWS o vendedor exigiu no produto, consulte as páginas de detalhes dos produtos listados no AWS Marketplace. Em seguida, revise as páginas de preços dos Serviços da AWS.

Avaliações gratuitas para produtos baseados em AMI

Alguns produtos de AMI com preços por hora ou por hora com preços anuais no AWS Marketplace têm avaliações gratuitas. Ao assinar uma avaliação gratuita, você pode executar uma instância do Amazon EC2 do produto de AMI por um período definido pelo vendedor sem incorrer nas cobranças de software por hora. Você é responsável pela taxa de infraestrutura. A execução de instâncias adicionais do Amazon EC2 incorrerá na cobrança de software por hora por instância. As avaliações gratuitas são convertidas automaticamente em uma assinatura paga após o vencimento.

Se não encerrar a instância do Amazon EC2 antes do término da avaliação gratuita, você incorrerá em cobranças de software por hora quando a avaliação terminar. O cancelamento da assinatura da avaliação gratuita não encerra automaticamente as instâncias do Amazon EC2, e você incorre em cobranças de software por qualquer uso contínuo. Para obter mais informações sobre taxas de infraestrutura, consulte Definição de preço do Amazon EC2.

Avaliações gratuitas para produtos baseados em contêiner

Alguns produtos de contêiner com preços por hora ou por hora com preços de longo prazo no AWS Marketplace têm avaliações gratuitas. Quando você assina uma avaliação gratuita, é possível executar várias tarefas do Amazon Elastic Container Service (Amazon ECS) ou pods do Amazon Elastic Kubernetes Service (Amazon EKS) por um período sem incorrer em cobranças de software por hora. O número de tarefas ou pods incluídos e a duração da avaliação gratuita são definidos pelo vendedor. Você é responsável pela taxa de infraestrutura. A execução de tarefas ou pods adicionais além do número incluído na avaliação gratuita incorrerá na cobrança horária do software por tarefa ou pod. As avaliações gratuitas são convertidas automaticamente em uma assinatura paga após o vencimento.

Se não encerrar a tarefa ou pod antes do término da avaliação gratuita, você incorrerá em cobranças de software por hora quando a avaliação terminar. O cancelamento da assinatura da avaliação gratuita não encerra automaticamente as tarefas ou pods, e você incorre em cobranças de software por qualquer uso contínuo. Para obter mais informações sobre taxas de infraestrutura, consulte Definição de preço do Amazon ECS e Definição de preço do Amazon EKS.

Avaliações gratuitas de produtos de machine learning

Alguns produtos de machine learning com preços por hora no AWS Marketplace têm avaliações gratuitas. Ao assinar uma avaliação gratuita, você pode executar endpoints do Amazon SageMaker, trabalhos de transformação em lote ou trabalhos de treinamento por um período definido pelo vendedor sem incorrer em cobranças de software por hora. Você é responsável pela taxa de infraestrutura. As avaliações gratuitas são convertidas automaticamente em uma assinatura paga após o vencimento.

Se você não encerrar nenhum endpoint, trabalho de transformação em lote ou trabalho de treinamento do Amazon SageMaker antes do término da avaliação gratuita, você incorrerá em cobranças de software por hora quando a avaliação terminar. O cancelamento da assinatura da avaliação gratuita não encerra automaticamente os endpoints, trabalhos de transformação em lote

ou trabalhos de treinamento do Amazon SageMaker, e você incorre em cobranças de software por qualquer uso contínuo. Para obter mais informações sobre taxas de infraestrutura, consulte Definição de preço do Amazon SageMaker.

Avaliações gratuitas para produtos SaaS

Os produtos de software como serviço (SaaS) no AWS Marketplace têm avaliações gratuitas. As avaliações gratuitas de SaaS não se convertem automaticamente em contratos pagos. Se você não desejar mais a avaliação gratuita, poderá deixá-la expirar. Para obter mais informações, consulte Avaliações gratuitas de SaaS.

Utilizar nível de uso gratuito da AWS com o AWS Marketplace

Para ajudar novos clientes da Amazon Web Services (AWS) a começar a usar a nuvem, a AWS criou um nível de uso gratuito. O nível gratuito pode ser usado em tudo o que você queira executar na nuvem: iniciar novos aplicativos, testar aplicativos existentes na nuvem ou simplesmente obter experiência prática com a AWS. Quando o período de uso gratuito expira (ou se o uso do aplicativo excede os limites do nível de uso gratuito), basta pagar as taxas padrão, conforme o uso. Para obter mais informações, consulte AWS Free Tier (Nível gratuito da AWS).

Os clientes do nível gratuito da AWS podem usar o software AWS Marketplace gratuitamente por até 750 horas de uso do Amazon Elastic Compute Cloud (Amazon EC2) por mês durante um ano. Para começar a usar, consulte AWS Marketplace.

Adicionar assinaturas do AWS Marketplace ao AWS Service Catalog

O Service Catalog permite que as organizações criem e gerenciem catálogos de serviços de TI aprovados para uso na Amazon Web Services (AWS). Esses serviços de TI podem incluir tudo, de imagens de máquinas virtuais, servidores, software e bancos de dados a arquiteturas completas de aplicativos multicamada. O Service Catalog permite que você gerencie centralmente os serviços de TI comumente implantados. Ele ajuda você a atingir uma governança consistente e requisitos de conformidade, ao mesmo tempo que permite que os usuários implantem rapidamente somente os serviços de TI aprovados de que precisam.

Para obter mais informações, consulte Adicionar produtos do AWS Marketplace ao portfólio no Guia do administrador do Service Catalog.

Análises de produtos

O AWS Marketplace quer que os compradores obtenham as informações necessárias para fazer escolhas de compra inteligentes. Como cliente da AWS, você pode enviar avaliações por escrito para itens listados no AWS Marketplace. Incentivamos compartilhar as opiniões sobre as opiniões, sejam elas favoráveis ou desfavoráveis.

> **Note**
>
> Os produtos de dados não oferecem suporte a avaliações de produtos.

Diretrizes

Qualquer pessoa com uma assinatura do AWS Marketplace de um produto pode criar uma análise dele. Use as seguintes diretrizes para escrever avaliações de produtos:

- Inclua motivos: as melhores avaliações incluem não apenas se você gostou ou não de um produto, mas também o motivo. É possível discutir produtos relacionados e como o item em questão se compara a eles.
- Seja específico: concentre-se em recursos específicos do produto e na experiência com ele. Para avaliações de vídeos, escreva uma breve introdução.
- Seja conciso: as avaliações por escrito devem ter pelo menos 20 palavras e são limitadas a 5.000 palavras. O tamanho ideal é de 75 a 500 palavras.
- Seja sincero: apreciamos opiniões honestas sobre o produto, positivas ou negativas. Informações úteis podem ajudar nas decisões de compra de nossos clientes.
- Seja transparente: se você recebeu um produto gratuito em troca de sua avaliação, divulgue isso de forma clara e visível.

Restrições

A AWS reserva-se o direito de remover avaliações que incluam qualquer um dos conteúdos a seguir.

- Material questionável, incluindo:
  - Conteúdo obsceno ou de mau gosto

  - Linguagem ofensiva ou comentários depreciativos
  - Promoção de conduta ilegal ou imoral
- Conteúdo promocional, incluindo:
  - Anúncios, material promocional ou publicações repetidas que reafirmem o mesmo ponto
  - Opiniões em relação a alguém ou em nome de uma pessoa ou empresa com interesse financeiro no produto ou em um produto diretamente concorrente (incluindo análises de autores, editores, fabricantes ou comerciantes terceiros que vendem o produto)
  - Comentários escritos para qualquer forma de remuneração que não seja uma cópia gratuita do produto, incluindo avaliações que façam parte de um pacote de publicidade pago
  - Avaliações escritas por um cliente sem uma assinatura verificável do produto
- Conteúdo inadequado, incluindo:
  - Conteúdo copiado de outras pessoas, incluindo cotações excessivas
  - Informações de contato ou URLs externos à Amazon.com
  - Detalhes sobre disponibilidade ou solicitação/envio alternado
  - Vídeos com marca d'água
  - Comentários sobre outras avaliações visíveis na página porque a visibilidade está sujeita a alterações sem aviso prévio
  - Conteúdo em idioma estrangeiro, a menos que haja uma clara conexão com o produto
  - Texto com problemas de formatação
- Informações fora do tópico, incluindo:
  - Comentários sobre o vendedor ou a experiência de envio
  - Comentários sobre erros de digitação e imprecisões em nosso catálogo ou descrição do produto, para isso, use o formulário de comentários na parte inferior da página do produto

Em caso de dúvidas sobre avaliações de clientes, entre em contato conosco.

Prazo e expectativas

Nós nos esforçamos para processar as avaliações de produtos o mais rápido possível. No entanto, a equipe do AWS Marketplace deve se comunicar com o revisor e com o vendedor para confirmar e analisar a validade do feedback em relação a the section called “Diretrizes” e the section called “Restrições”. Seguimos a mesma orientação de tempo e expectativas descrita no Guia do vendedor do AWS Marketplace sobre quanto tempo será necessário para concluir o processo.

Obter suporte

Para questões gerais do AWS Marketplace, entre em contato conosco. Para dúvidas sobre o software comprado por meio do AWS Marketplace, entre em contato com o vendedor do software.

AWS Marketplace Vendor Insights

O AWS Marketplace Vendor Insights simplifica as avaliações de risco de software, ajudando você a adquirir software confiável e que atenda aos padrões do setor. Com o AWS Marketplace Vendor Insights, você pode monitorar o perfil de segurança de um produto quase em tempo real em uma única interface de usuário. Ele reduz seu esforço de avaliação ao fornecer um painel com as informações de segurança de um produto de software. Você pode usar o painel para visualizar e avaliar informações, como privacidade de dados, segurança de aplicações e controle de acesso.

O AWS Marketplace Vendor Insights coleta dados de segurança dos vendedores e oferece suporte aos compradores por meio da aquisição de software confiável que atenda continuamente aos padrões do setor. Ao se integrar ao AWS Audit Manager, o AWS Marketplace Vendor Insights pode obter automaticamente informações de segurança atualizadas para seus produtos de software como serviço (SaaS) no AWS Marketplace. AWS Marketplace O Vendor Insights se integra a relatórios de terceiros do AWS Artifact para que você possa acessar relatórios de conformidade sob demanda para o software do fornecedor, juntamente com relatórios para Serviços da AWS.

O AWS Marketplace Vendor Insights fornece informações baseadas em evidências de 10 categorias de controle e vários controles. Ele coleta as informações baseadas em evidências de três fontes:

- Contas de produção do fornecedor: dos vários controles, 25 permitem a coleta de evidências ao vivo das contas de produção de um fornecedor. A evidência ao vivo de cada controle é gerada por uma ou mais regras de AWS Config que avaliam as configurações dos recursos da AWS de um vendedor. A evidência ao vivo é o método de atualizar consistentemente dados de várias fontes para apresentar as informações mais atuais. O AWS Audit Manager captura as evidências e as entrega ao painel do AWS Marketplace Vendor Insights.
- Relatórios ISO 27001 e SOC 2 Tipo II do fornecedor: as categorias de controle são mapeadas para controles nos relatórios da Organização Internacional de Padronização (ISO) e Service Organization Controls (SOC) 2. Quando os vendedores compartilham esses relatórios com o AWS Marketplace Vendor Insights, o serviço extrai os dados relevantes e os apresenta no painel.
- Autoavaliação do fornecedor: os vendedores concluem uma autoavaliação. Eles também podem criar e enviar outros tipos de autoavaliação, incluindo a autoavaliação de segurança do AWS Marketplace Vendor Insights e o Consensus Assessment Initiative Questionnaire (CAIQ).

O vídeo a seguir demonstra como você pode simplificar a avaliação de risco do SaaS e usar o AWS Marketplace Vendor Insights.

Começar a usar o AWS Marketplace Vendor Insights como comprador

O AWS Marketplace Vendor Insights apresenta informações de segurança para produtos de software disponíveis no AWS Marketplace. Você pode usar o AWS Marketplace Vendor Insights para visualizar perfis de segurança de produtos no AWS Marketplace.

O painel do AWS Marketplace Vendor Insights apresenta os artefatos de conformidade e as informações de controle de segurança de um produto de software usando o AWS Marketplace Vendor Insights para avaliar o produto. AWS Marketplace O Vendor Insights coleta as informações baseadas em evidências para vários controles de segurança apresentados no painel.

Não há cobrança pelo uso do AWS Marketplace Vendor Insights para acessar informações de segurança e conformidade dos produtos.

Encontrar produtos com o AWS Marketplace Vendor Insights

Você pode ver o perfil e as informações resumidas de um produto no painel do AWS Marketplace Vendor Insights ou selecionar os controles de categoria e saber mais sobre os dados coletados no produto. Para encontrar produtos no AWS Marketplace com o AWS Marketplace Vendor Insights, use o procedimento a seguir.

Para encontrar produtos com o AWS Marketplace Vendor Insights

1. Faça login no AWS Management Console e abra o AWS Marketplace console.
2. Escolha Exibir todos os produtos.
3. Veja os produtos que têm a tag Vendor Insights.
4. Em Refinar resultados para Vendor Insights, escolha Perfis de segurança.
5. Na página Detalhes do produto, em Visão geral do produto, escolha a seção Vendor Insights.
6. Escolha Exibir todos os perfis desse produto.
7. Você pode ver detalhes sobre o produto na Visão geral, bem como uma lista dos Certificados de segurança recebidos.
8. Escolha Solicitar acesso.
9. Na página Solicitar acesso aos dados do Vendor Insight, forneça suas informações e escolha Solicitar acesso.

Uma mensagem de sucesso é exibida, indicando que você solicitou o acesso aos dados do AWS Marketplace Vendor Insights para este produto.

Solicitar acesso aos dados de avaliação assinando

Com o AWS Marketplace Vendor Insights, você pode monitorar continuamente o perfil de segurança do software do fornecedor. Primeiro, assine ou solicite acesso aos dados de avaliação do fornecedor do produto que você deseja monitorar. Se não quiser mais monitorar os dados de avaliação de um produto, você pode cancelar a assinatura dos dados de avaliação. Não há cobrança pelo uso do AWS Marketplace Vendor Insights para acessar informações de segurança e conformidade dos produtos. Para obter mais informações sobre a definição de preço, consulte Definição de preço do AWS Marketplace Vendor Insights.

Para ter acesso a todos os dados de avaliação de um produto de um fornecedor específico, você precisa assinar os dados de avaliação do produto.

Para assinar os dados de avaliação do AWS Marketplace Vendor Insights de um produto

1. Faça login no AWS Management Console e abra o AWS Marketplace console.
2. Escolha Vendor Insights.
3. No Vendor Insights, escolha um produto.
4. Escolha a guia Overview (Visão geral).
5. Escolha Solicitar acesso.
6. Insira suas informações nos campos fornecidos.
7. Quando terminar, escolha Solicitar acesso.

   Uma mensagem de sucesso aparece indicando que você solicitou acesso a todos os dados de avaliação do fornecedor para este produto.

Cancelar a assinatura dos dados da avaliação

Se não quiser mais acessar os dados de avaliação de um produto do fornecedor, você pode cancelar a assinatura dos dados de avaliação do produto.

Para cancelar a assinatura dos dados de avaliação do AWS Marketplace Vendor Insights de um produto

1. Faça login no AWS Management Console e abra o AWS Marketplace console.
2. Escolha Vendor Insights.
3. Na página Detalhes do produto, escolha um produto e escolha Cancelar assinatura.
4. Leia os termos apresentados com o cancelamento da assinatura dos dados do AWS Marketplace Vendor Insights.
5. Digite **`Unsubscribe`** no campo de entrada de texto e escolha Cancelar assinatura.

   Uma mensagem de sucesso é exibida, indicando que você cancelou a assinatura dos dados do AWS Marketplace Vendor Insights e não será mais cobrado pelo acesso.

Visualização do perfil de segurança de um produto com o AWS Marketplace Vendor Insights

O AWS Marketplace Vendor Insights coleta dados de segurança dos vendedores. O perfil de segurança de um produto exibe informações atualizadas sobre segurança, resiliência, conformidade e outros fatores necessários para sua avaliação. Essas informações ajudam compradores como você a adquirir um software confiável que atenda continuamente aos padrões do setor. Para cada produto de software como serviço (SaaS) que avalia, o AWS Marketplace Vendor Insights coleta as informações baseadas em evidências para vários controles de segurança.

Tópicos

- Painel no AWS Marketplace Vendor Insights
- Veja o perfil de segurança de um produto de SaaS
- Noções básicas sobre as categorias de controle

Painel no AWS Marketplace Vendor Insights

O painel apresenta os artefatos de conformidade e as informações de controle de segurança de um produto de software que são coletados pelo AWS Marketplace Vendor Insights. São fornecidas informações baseadas em evidências para todas as categorias de controle de segurança, como uma alteração na residência de dados ou na expiração da certificação. O painel consolidado fornece alterações nas informações de conformidade. AWS Marketplace O Vendor Insights elimina

a necessidade de criar questionários adicionais e usar software de avaliação de risco. Com um painel atualizado e validado de forma consistente, você pode monitorar continuamente o controle de segurança do software após a aquisição.

Veja o perfil de segurança de um produto de SaaS

O AWS Marketplace Vendor Insights ajuda você a tomar decisões sobre o software de um vendedor. AWS Marketplace O Vendor Insights extrai dados das informações baseadas em evidências de um vendedor em 10 categorias de controle e vários controles. Você pode visualizar o perfil e as informações resumidas de um produto de SaaS no painel ou selecionar categorias de controle para saber mais sobre os dados coletados. Você deve ser assinante do produto e ter acesso para visualizar as informações de conformidade por meio do perfil.

1. Faça login no AWS Management Console e abra o AWS Marketplace console.
2. Escolha Vendor Insights.
3. No Vendor Insights, escolha um produto.
4. Na página Detalhes do perfil, escolha a guia Segurança e conformidade.

> **Note**
>
> Um número em um círculo vermelho indica o número de controles não compatíveis.

5. Em Categorias de controle, escolha o texto em qualquer uma das categorias listadas para ver mais informações.

   - Escolha o primeiro nome de controle (Você tem uma política/procedimento para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais aplicáveis?).
   - Leia as informações apresentadas. Você também pode visualizar relatórios de relatórios de terceiros de AWS Artifact ou visualizar exceções do auditor.
   - Selecione o nome do produto na navegação acima para retornar à página Detalhes do produto.

Noções básicas sobre as categorias de controle

O AWS Marketplace Vendor Insights fornece informações baseadas em evidências de vários controles em 10 categorias. AWS Marketplace O Vendor Insights coleta as informações de três fontes: contas de produção do fornecedor, autoavaliação do fornecedor e relatórios ISO 27001

e SOC 2 Tipo II do fornecedor. Para obter mais informações sobre essas fontes, consulte AWS Marketplace Vendor Insights.

A lista a seguir fornece uma descrição de cada categoria de controle:

Gerenciamento de acesso

Identifica, rastreia, gerencia e controla o acesso a um sistema ou uma aplicação.

Segurança da aplicação

Verifica se a segurança foi incorporada à aplicação ao projetá-la, desenvolvê-la e testá-la.

Política de auditoria, conformidade e segurança

Avalia a adesão de uma organização aos requisitos regulatórios.

Resiliência e continuidade dos negócios

Avalia a capacidade da organização de se adaptar rapidamente às interrupções, mantendo a continuidade dos negócios.

Segurança de dados

Protege dados e ativos.

Segurança do dispositivo de usuário final

Protege os dispositivos portáteis do usuário final e as redes às quais eles estão conectados contra ameaças e vulnerabilidades.

Recursos humanos

Avalia a divisão relacionada a funcionários quanto ao tratamento de dados confidenciais durante processos como contratação, pagamento e demissão de funcionários.

Segurança da infraestrutura

Protege ativos essenciais contra ameaças e vulnerabilidades.

Gerenciamento de riscos e resposta a incidentes

Avalia o nível de risco considerado aceitável e as medidas tomadas para responder aos riscos e ataques.

Política de segurança e configuração

Avalia as políticas e as configurações de segurança que protegem os ativos de uma organização.

Conjuntos de categorias de controle

As tabelas a seguir fornecem informações detalhadas para cada categoria com informações sobre os valores de cada categoria coletada. A lista a seguir descreve o tipo de informação em cada coluna da tabela:

- Conjunto de controles: os controles são atribuídos a um conjunto de controles e cada controle reflete a função de segurança da categoria. Cada categoria tem vários conjuntos de controles.
- Nome do controle: nome da política ou do procedimento. “Requer atestado manual” significa que é necessária uma confirmação por escrito ou documentação da política ou do procedimento.
- Descrição do controle: perguntas, informações ou documentação necessárias sobre esta política ou procedimento.
- Detalhe da extração de evidências: informações e contexto necessários sobre o controle para obter ainda mais os dados necessários para essa categoria.
- Valor de exemplo: exemplo fornecido para orientação sobre a aparência de um valor de conformidade para essa categoria para que esteja de acordo com os padrões regulatórios.

Tópicos

Controles de gerenciamento de acesso

Os controles de gerenciamento de acesso identificam, rastreiam, gerenciam e controlam o acesso a um sistema ou uma aplicação. Esta tabela lista os valores e as descrições dos controles de gerenciamento de acesso.

Conjunto de controles	Título do controle	Descrição do controle
Autenticação segura	Gerenciamento de acesso 3.1.1 - Autenticação segura - Dados pessoais no ID do usuário (requer atestado manual)	Você precisa de dados pessoais (a endereço de e-mail) no ID do usuá
	Gerenciamento de acesso 3.1.2 - Autenticação segura - A aplicação suporta autenticação de dois fatores (requer atestado manual)	A aplicação oferece suporte à aute fatores?
	Gerenciamento de acesso 3.1.3 - Autenticação segura - Bloqueio de conta (requer atestado manual)	A conta do cliente será bloqueada logins com falha?
Gerenciamento de credenciais	Gerenciamento de acesso 3.2.1 - Gerenciamento de credenciais - Política de senha	A aplicação tem uma política de se
	Gerenciamento de acesso 3.2.2 - Gerenciamento de credenciais - Criptografia de senha	A política de senha exige que as c (senha e ID de usuário) sejam crip trânsito e criptografadas com salt c as?
	Gerenciamento de acesso 3.2.3 - Gerenciamento de credenciais - Gerenciamento de segredos	Você usa algum serviço de gerenc segredos?
	Gerenciamento de acesso 3.2.4 - Gerenciamento de credenciais - Credenciais no código (requer atestado manual)	As credenciais estão incluídas no c

Conjunto de controles	Título do controle	Descrição do controle
Acesso ao ambiente de produção	Gerenciamento de acesso 3.3.1 - Acesso ao ambiente de produção - Logon único (requer atestado manual)	O SSO está habilitado para acessa produção?
	Gerenciamento de acesso 3.3.2 - Acesso ao ambiente de produção - Autenticação de dois fatores	A autenticação de dois fatores é n acessar o ambiente de produção c
	Gerenciamento de acesso 3.3.3 - Acesso ao ambiente de produção - Usuário raiz (requer atestado manual)	O usuário raiz é usado somente co acessar o ambiente de produção?
	Gerenciamento de acesso 3.3.4 - Acesso ao ambiente de produção - MFA de usuário raiz	O usuário raiz exige autenticação
	Gerenciamento de acesso 3.3.5 - Acesso ao ambiente de produção - Acesso remoto	O acesso remoto ao ambiente de p protegido por meio de mecanismos criptografados ou autenticação bas
Política de controle de acesso	Gerenciamento de acesso 3.4.1 - Política de controle de acesso - Acesso com privilégio mínimo	Você segue a política de acesso c mínimo para que os usuários aces produção?
	Gerenciamento de acesso 3.4.2 - Política de controle de acesso - Revisão da política de acesso	Todas as políticas de acesso no a produção são revisadas regularme

Conjunto de controles	Título do controle	Descrição do controle
	Gerenciamento de acesso 3.4.3 - Política de controle de acesso - Configuração de políticas de segurança e usuários (requer atestado manual)	A aplicação permite que os cliente usuários e privilégios?
	Gerenciamento de acesso 3.4.4 - Política de controle de acesso - Segmentação lógica (requer atestado manual)	Há segmentação lógica dos usuári
	Gerenciamento de acesso 3.4.5 - Política de controle de acesso - Revisão de acesso após a demissão	Todas as políticas de acesso relev as após a demissão ou a mudança funcionário?
Logs de acesso	Gerenciamento de acesso 3.5.1 - Logs de acesso	Você registra atividades realizadas individuais no ambiente de produç

Controles de segurança da aplicação

Os controles de segurança da aplicação verificam se a segurança foi incorporada à aplicação ao projetá-la, desenvolvê-la e testá-la. Esta tabela lista os valores e as descrições dos controles da política de segurança da aplicação.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Ciclo de vida de desenvolv imento seguro de software	Segurança de aplicações 4.1.1 - Ciclo de vida de desenvolv	O ambiente de desenvolv imento, teste e preparação	Especifique se o ambiente de desenvolv imento, teste	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	imento seguro de software - Ambiente separado	é separado do ambiente de produção?	e preparação é separado do ambiente de produção.	
	Segurança de aplicações 4.1.2 - Ciclo de vida de desenvolv imento seguro de software - Prática de codificação segura	Os engenheiros de segurança trabalham com desenvolvedores em práticas de segurança?	Especifique se desenvolvedores e engenheiros de segurança trabalham juntos em práticas de codificação segura.	Sim
	Segurança de aplicações 4.1.3 - Ciclo de vida de desenvolv imento seguro de software - Uso de dados do cliente no ambiente de teste (requer atestado manual)	Os dados do cliente já foram usados nos ambientes de teste, desenvolv imento ou controle de qualidade?	Os dados do cliente já foram usados nos ambientes de teste, desenvolv imento ou controle de qualidade? Em caso afirmativo, quais dados são usados e para que são usados?	Não

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de aplicações 4.1.4 - Ciclo de vida de desenvolv imento seguro de software - Conexão segura	O SSL/TLS está habilitado para todas as páginas da Web e comunicações que usam dados do cliente?	Especifiq ue se uma conexão segura (como SSL/ TLS) é usada para todas as comunicações com os dados do cliente.	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de aplicações 4.1.5 - Ciclo de vida de desenvolvimento seguro de software - Backup de imagem	O backup dos instantâneos de imagens da aplicação é feito?	Especifique se é feito backup de instantâneos de imagem (como sistemas que suportam a aplicação e sistemas que hospedam dados do cliente). Em caso afirmativo, existe um processo para garantir que os instantâneos de imagens contendo dados com escopo sejam autorizados antes de serem capturados? O controle de acesso está implementado para os instantâneos de imagem?	Sim. O backup das imagens é feito com a aprovação do cliente e da gerência.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Análise de segurança da aplicação	Segurança de aplicações 4.2.1 - Análise de segurança da aplicação - Análise segura do código	A análise segura do código é feita antes de cada lançamento?	Especifique se uma análise do código de segurança é feita antes de cada lançamento.	Sim
	Segurança de aplicações 4.2.2 - Análise de segurança da aplicação - Teste de penetração	Os testes de penetração são realizados? Podemos obter relatórios de testes de penetração?	Especifique se os testes de penetração são realizados na aplicação. Em caso afirmativo, você pode compartilhar os últimos três relatórios como evidência manual?	Sim
	Segurança de aplicações 4.2.3 - Análise de segurança da aplicação - Patches de segurança	Todos os patches de segurança de alto risco disponíveis são aplicados e verificados regularmente?	Especifique se os patches de segurança de alto risco são aplicados regularmente. Em caso afirmativo, com que frequência eles são aplicados?	Sim. Os patches de segurança são aplicados mensalmente.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de aplicações 4.2.4 - Análise de segurança da aplicação - Verificações de vulnerabilidade em aplicações	As verificações de vulnerabilidade são realizadas em todas as aplicações voltadas para a Internet regularmente e após mudanças significativas?	Especifique se as verificações de vulnerabilidade são realizadas em todas as aplicações voltadas para a Internet. Em caso afirmativo, com que frequência as verificações de vulnerabilidade são feitas? Podemos obter uma cópia do relatório?	Sim. As varreduras de vulnerabilidade são realizadas mensalmente.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de aplicações 4.2.5 - Análise de segurança da aplicação - Gerenciamento de ameaças e vulnerabilidades	Existem processos para gerenciar as ferramentas de avaliação de ameaças e vulnerabilidades e os dados que elas coletam?	Especifique se há processos para gerenciar ferramentas de avaliação de ameaças e vulnerabilidades e suas descobertas. Você poderia fornecer mais detalhes sobre como as ameaças e vulnerabilidades são gerenciadas?	Sim. Todas as ameaças e vulnerabilidades de diferentes fontes são agregadas em um portal. Elas são gerenciadas por gravidade.
	Segurança de aplicações 4.2.6 - Análise de segurança da aplicação - Verificações antimalware	A verificação antimalware é feita na rede e nos sistemas que hospedam a aplicação regularmente?	Especifique se a verificação antimalware é feita na rede e nos sistemas que hospedam a aplicação. Em caso afirmativo, com que frequência isso é feito? Você pode fornecer o relatório?	Sim. As verificações antimalware são realizadas mensalmente.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Logs de aplicações	Segurança de aplicações 4.3.1 - Logs de aplicação - Logs de aplicação	Os logs de aplicação são coletados e revisados?	Especifique se os logs de aplicação são coletados e revisados. Em caso afirmativo, por quanto tempo os logs são retidos?	Sim. Os logs são retidos por um ano.
	Segurança de aplicações 4.3.2 - Logs de aplicação - Acesso aos logs	Os logs do sistema operacional e da aplicação estão protegidos contra modificação, exclusão e/ou acesso inadequado?	Especifique se os logs do sistema operacional e da aplicação estão protegidos contra modificação, exclusão e/ou acesso inadequado. No caso de uma violação ou incidente, você tem processos implementados para detectar a perda de logs de aplicação?	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de aplicações 4.3.3 - Logs de aplicação - Dados armazenados em logs (requer atestado manual)	Você armazena as informações de identificação pessoal (PII) em logs?	Especifique se você armazena as informações de identificação pessoal (PII) em logs.	Não. Nenhum dado de PII será armazenado nos logs.
Política de controle de alterações	Segurança de aplicações 4.4.1 - Política de controle de alterações - Teste funcional e de resiliência	Os testes funcionais e de resiliência são feitos antes de lançar uma alteração?	Especifique se o teste funcional e de resiliência é feito na aplicação antes de uma nova versão.	Sim
	Segurança de aplicações 4.4.2 - Política de controle de alterações - Procedimentos de controle de alterações	Os procedimentos de controle de alterações são necessários para todas as mudanças no ambiente de produção?	Especifique se os procedimentos de controle de alterações estão em vigor para todas as alterações feitas no ambiente de produção.	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de aplicações 4.4.3 - Política de controle de alterações - Evite erros/riscos humanos na produção	Você tem algum processo implementado para verificar se os erros humanos e os riscos não entram na produção?	Especifique que há algum processo para verificar se o erro humano e os riscos não entram na produção.	Sim
	Segurança de aplicações 4.4.4 - Política de controle de alterações - Alterações de documentos e logs	Você documenta e registra alterações que podem afetar os serviços?	Especifique se as alterações que afetam o serviço são documentadas e registradas. Em caso afirmativo, por quanto tempo os logs são retidos?	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de aplicações 4.4.5 - Política de controle de alterações - Notificação de alteração para compradores (requer atestado manual)	Existe algum processo formal para garantir que os clientes sejam notificados antes da realização de alterações que possam afetar os serviços?	Especifique se os clientes serão notificad os antes de fazer alterações que possam afetar os serviços. Em caso afirmativ o, qual é o SLA para notificar os clientes sobre alterações impactantes?	Sim. Notificam os os clientes 90 dias antes das alterações impactantes.

Controles de auditoria e conformidade

Os controles de auditoria e conformidade avaliam a adesão de uma organização aos requisitos regulatórios. Esta tabela lista os valores e as descrições dos controles de auditoria e conformidade.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Certificações concluídas	Auditoria e conformidade 1.1.1 - Certifica ções concluídas (requer atestado manual)	Liste as certifica ções que você tem.	Especifique quais certifica ções você tem.	SOC2, ISO/IEC 27001
Certificação em andamento	Auditoria e conformid ade 1.2.1 -	Liste certifica dos adicionais que estão em	Liste todos os certifica dos adicionai	Sim. A certifica ção PCI está em

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Certificação em andamento (requer atestado manual)	andamento no momento.	s que estão sendo auditados ou revisados no momento com uma data de conclusão estimada.	andamento (ETA Q2 2022).
Procedimentos que garantem a conformidade	Auditoria e conformidade 1.3.1 - Procedimentos que garantem a conformidade - Procedimentos que garantem a conformidade	Você tem alguma política ou procedimento para garantir a conformidade com os requisitos legislativos, regulatórios e contratuais aplicáveis?	Especifique se você tem alguma política ou procedimento para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais aplicáveis. Em caso afirmativo, liste os detalhes sobre o procedimento e faça o upload das evidências manuais.	Sim. Enviamos documentos como SOC2, ISO/IEC 27001.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Auditoria e conformidade 1.3.2 - Procedimentos que garantem a conformidade - Auditorias para monitorar requisitos pendentes	As auditorias são concluídas para monitorar os requisitos regulatórios e de conformidade pendentes?	Especifique se as auditorias são feitas para monitorar os requisitos pendentes. Em caso afirmativo, forneça detalhes.	Sim, as auditorias são feitas mensalmente para monitorar os requisitos pendentes.
	Auditoria e conformidade 1.3.3 - Procedimentos que garantem a conformidade - Desvios e exceções (requer atestado manual)	Você tem algum processo para lidar com desvios e exceções dos requisitos de conformidade?	Especifique se há algum processo para lidar com exceções ou desvios dos requisitos de conformidade. Em caso afirmativo, forneça detalhes.	Sim. Temos um log de desvios e ferramentas de relatórios. Investigamos todas as exceções ou desvios para evitar futuras ocorrências.

Controles de resiliência de negócios

Os controles de resiliência de negócios avaliam a capacidade da organização de se adaptar rapidamente às interrupções e, ao mesmo tempo, manter a continuidade dos negócios. Esta tabela lista os valores e as descrições dos controles da política de resiliência de negócios.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Resiliência de negócios	Resiliência e continuidade de negócios 6.1.1 - Resiliência de negócios - Testes de failover (requer atestado manual)	Os testes de failover do site são realizados pelo menos uma vez por ano?	Especifique se os testes de failover são realizados anualmente. Em caso negativo, com que frequência eles são realizados?	Sim
	Resiliência e continuidade de negócios 6.1.2 - Resiliência de negócios - Análise de impacto nos negócios (requer atestado manual)	Foi realizada alguma análise de impacto nos negócios?	Especifique se uma análise de impacto nos negócios foi feita. Em caso afirmativo, quando foi concluída pela última vez? Forneça detalhes sobre a análise realizada.	Sim. Uma análise de impacto nos negócios foi concluída há seis meses.
	Resiliência e continuidade de negócios 6.1.3 - Resiliência de negócios - Dependências de fornecedores de terceiros	Há alguma dependência de provedores de serviços de terceiros essenciais (além de um provedor	Especifique se há alguma dependência de fornecedores de terceiros (além de um provedor de serviços em nuvem).	Não

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	(requer atestado manual)	de serviços em nuvem)?	Em caso afirmativo, você pode fornecer detalhes sobre os fornecedores?	
	Resiliência e continuidade de negócios 6.1.4 - Resiliência de negócios - Testes de continuidade e recuperação de terceiros (requer atestado manual)	Você exige que fornecedores de terceiros tenham seus próprios processos e exercícios de recuperação de desastres?	Especifique se fornecedores de terceiros devem ter seus próprios processos e exercícios de recuperação de desastres.	Não aplicável nesta amostra.
	Resiliência e continuidade de negócios 6.1.5 - Resiliência de negócios - Violação de contrato de fornecedores de terceiros (requer atestado manual)	Os contratos com provedores de serviços essenciais incluem alguma penalidade ou cláusula de remediação por violação de disponibilidade e continuidade de venda e envio pela Amazon (SSA)?	As cláusulas de penalidade ou remediação por violação de disponibilidade e continuidade estão incluídas nos contratos com fornecedores de terceiros?	Não aplicável nesta amostra.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Resiliência e continuidade de negócios 6.1.6 - Resiliência de negócios - Integridade do sistema	Você tem monitores ou alertas para entender a integridade do sistema?	Especifique se há monitores ou alertas para entender a integridade do sistema.	Sim
Continuidade dos negócios	Resiliência e continuidade de negócios 6.2.1 - Continuidade de negócios - Políticas/ procedimentos de continuidade de negócios	Os procedimentos formais de continuidade de negócios são desenvolvidos e documentados?	Especifique se procedimentos formais são desenvolvidos e mantidos para a continuidade de negócios. Em caso afirmativo, forneça mais detalhes sobre os procedimentos.	Sim
	Resiliência e continuidade de negócios 6.2.2 - Continuidade de negócios - Estratégias de resposta e recuperação	As estratégias específicas de resposta e recuperação estão definidas para as atividades priorizadas?	Especifique se as estratégias de recuperação e resposta foram desenvolvidas para as atividades e os serviços do cliente.	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Resiliência e continuidade de negócios 6.2.3 - Continuidade de negócios - Testes de continuidade de negócios	Você realiza testes de recuperação para garantir a continuidade dos negócios?	Especifique se você realiza testes de recuperação para garantir a continuidade dos negócios em caso de falha.	Sim. Em caso de falha, os sistemas para continuidade dos negócios serão ativados em duas horas.
	Resiliência e continuidade de negócios 6.2.4 - Continuidade de negócios - Impacto da disponibilidade em ambientes de multilocação (requer atestado manual)	Você limita a capacidade do comprador de impor uma carga que pode afetar a disponibilidade de outros usuários do seu sistema?	Especifique se a carga de um comprador pode afetar a disponibilidade de outro comprador. Em caso afirmativo, qual é o limite até o qual não haverá impacto? Em caso negativo, você pode fornecer mais detalhes sobre como garantir que os serviços não sejam afetados durante o pico de uso e acima?	Sim. Limite não disponível para esta amostra.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Disponibilidade da aplicação	Resiliência e continuidade de negócios 6.3.1 - Disponibilidade da aplicação - Registro de disponibilidade (requer atestado manual)	Houve algum problema significativo relacionado à confiabilidade ou disponibilidade no último ano?	Especifique se houve algum problema significativo relacionado à confiabilidade ou disponibilidade no último ano.	Não
	Resiliência e continuidade de negócios 6.3.2 - Disponibilidade da aplicação - Janela de manutenção programada (requer atestado manual)	O tempo de inatividade é esperado durante a manutenção programada?	Especifique se há uma janela de manutenção programada durante a qual os serviços podem ficar inativos. Em caso afirmativo, quanto tempo dura o tempo de inatividade?	Não

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Resiliência e continuidade de negócios 6.3.3 - Disponibilidade da aplicação - Portal de incidentes on-line (requer atestado manual)	Existe um portal on-line de status de resposta a incidentes que descreva interrupções planejadas e não planejadas?	Especifique se há um portal de status de incidentes que descreva interrupções planejadas e não planejadas. Em caso afirmativo, forneça detalhes sobre como um cliente pode acessá-lo. Quanto tempo após a interrupção o portal será atualizado?	Sim. O cliente pode acessar os detalhes em example.com.
	Resiliência e continuidade dos negócios 6.3.4 - Disponibilidade da aplicação - Objetivo de tempo de recuperação (requer atestado manual)	Existe um objetivo de tempo de recuperação (RTO) específico?	Especifique se há um objetivo de tempo de recuperação (RTO). Em caso afirmativo, você pode fornecer o RTO?	Sim, um RTO de duas horas.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Resiliência e continuidade dos negócios 6.3.5 - Disponibilidade da aplicação - Objetivo de ponto de recuperação (requer atestado manual)	Existe um objetivo de ponto de recuperação (RPO) específico?	Especifique se há um objetivo de ponto de recuperação (RPO). Em caso afirmativo, você pode fornecer o RPO?	Sim, um RPO de uma semana.

Controles de segurança de dados

Os controles de segurança de dados protegem dados e ativos. Esta tabela lista os valores e as descrições dos controles de segurança de dados.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Dados do cliente ingeridos	Segurança de dados 2.1.1 - Dados do cliente ingeridos (requer atestado manual)	Crie uma lista dos dados necessários dos clientes para a funcionalidade do produto.	Descreva todos os dados consumidos pelos clientes. Especifique se dados sensíveis ou confidenciais são consumidos.	Nenhum dado sensível e confidencial é consumido . Este produto consome apenas informações não confidenciais, como logs de aplicações, infraestrutura e Serviços da

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
				AWS. (AWS CloudTrail, AWS Config, logs de fluxo de VPC)
Local de armazenamento de dados	Segurança de dados 2.2.1 - Local de armazenamento de dados (requer atestado manual)	Onde os dados do cliente são armazenados? Liste os países e regiões onde os dados são armazenados.	Especifique a lista de países e regiões onde os dados são armazenados.	Ohio (EUA), Oregon (EUA), Irlanda (UE)
Controle de acesso	Segurança de dados 2.3.1 - Controle de acesso - Acesso de funcionários (requer atestado manual)	Os funcionários têm acesso aos dados não criptografados dos clientes?	Especifique se os funcionários têm acesso aos dados não criptografados do cliente. Em caso afirmativo, explique resumidamente por que eles precisam de acesso. Em caso negativo, explique resumidamente como você controla o acesso.	Não, todos os dados são criptografados quando armazenados. Os funcionários não terão acesso aos dados do cliente, mas apenas aos dados sobre seu uso.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de dados 2.3.2 - Controle de acesso - Aplicação móvel (requer atestado manual)	Os clientes podem acessar seus dados por meio de uma aplicação móvel?	Especifique se os clientes podem acessar seus dados usando uma aplicação móvel. Em caso afirmativo, forneça mais detalhes. Como os clientes fazem login? As credenciais são armazenadas em cache pela aplicação? Com que frequência os tokens são atualizados?	Não, o serviço não pode ser acessado usando uma aplicação móvel.
	Segurança de dados 2.3.3 - Controle de acesso - Países para os quais os dados são transmitidos (requer atestado manual)	Os dados do cliente são transmitidos para países fora da origem?	Os dados do cliente são transmitidos para países fora da origem? Em caso afirmativo, especifique a lista de países para os quais os dados do cliente são transmitidos ou recebidos.	Não

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de dados 2.3.4 - Controle de acesso - Os dados são compartilhados com fornecedores de terceiros (requer atestado manual)	Os dados do cliente são compartilhados com fornecedores de terceiros (exceto provedores de serviços em nuvem)?	Os dados do cliente são compartilhados com fornecedores de terceiros? Em caso afirmativo, especifique a lista de fornecedores de terceiros e os países ou regiões para os quais você fornece dados de clientes.	Não

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de dados 2.3.5 - Controle de acesso - Política de segurança relacionada a fornecedores de terceiros	Você tem políticas ou procedimentos em vigor para garantir que fornecedores de terceiros mantenham a confidencialidade, a disponibilidade e a integridade dos dados do cliente?	Especifique se você tem políticas ou procedimentos em vigor para garantir que fornecedores de terceiros mantenham a confidencialidade, a disponibilidade e a integridade dos dados do cliente. Em caso afirmativo, faça o upload de um manual ou documento das políticas ou procedimentos.	Não aplicável nesta amostra.
Criptografia de dados	Segurança de dados 2.4.1 - Criptografia de dados - Criptografia de dados em repouso	Todos os dados são criptografados em repouso?	Especifique se todos os dados são criptografados em repouso.	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de dados 2.4.2 - Criptografia de dados - Criptografia de dados em trânsito	Todos os dados são criptografados em trânsito?	Especifique se todos os dados são criptografados em trânsito.	Sim
	Segurança de dados 2.4.3 - Criptografia de dados - Algoritmos fortes (requer atestado manual)	Você usa algoritmos de criptografia fortes?	Você usa algoritmos de criptografia fortes? Em caso afirmativo, especifique quais algoritmos de criptografia (como RSA, AES 256) são usados.	Sim. O AES 256 é usado para criptografar os dados.
	Segurança de dados 2.4.4 - Criptografia de dados - Chave de criptografia exclusiva (requer atestado manual)	Os clientes têm a capacidade de gerar uma chave de criptografia exclusiva?	Os clientes podem fornecer ou gerar suas próprias chaves de criptografia exclusivas? Em caso afirmativo, forneça mais detalhes e envie evidências.	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de dados 2.4.5 - Criptografia de dados - Acesso às chaves de criptografia (requer atestado manual)	Os funcionários são impedidos de acessar as chaves de criptografia de um cliente?	Especifiq ue se seus funcionários estão impedidos de acessar as chaves de criptografia de um cliente. Em caso negativo, explique por que eles têm acesso às chaves do cliente. Em caso afirmativo, explique como o acesso é controlado.	Sim. As chaves criptográ ficas são armazenadas com segurança e alternadas periodicamente. Os funcionários não têm acesso a essas chaves.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Armazenamento e classificação de dados	Segurança de dados 2.5.1 - Armazenamento e classificação de dados - Backup de dados	Você faz backup dos dados do cliente?	Especifique se você faz backup dos dados do cliente. Em caso afirmativo, descreva sua política de backup (incluindo detalhes sobre a frequência com que o backup ocorre, onde o backup é armazenado, criptografia de backup e redundância).	Sim, o backup é feito a cada três meses. O backup é criptografado e armazenado na mesma região dos dados do cliente. O engenheiro de suporte ao cliente tem acesso para restaurar o backup, mas não os dados no backup.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de dados 2.5.2 - Armazenamento e classificação de dados - Política de controle de acesso a dados	Você implementa controles de acesso apropriados para os dados armazenados do cliente? Forneça suas políticas de controle de acesso.	Especifique se os controles de acesso apropriados (como o RBAC) são implementados para os dados armazenados do cliente. Forneça mais detalhes e evidências manuais sobre como você controla o acesso aos dados.	Sim. Os controles de acesso com privilégios mínimos são implementados para restringir o acesso aos dados do cliente.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de dados 2.5.3 - Armazenamento e classificação de dados - Dados da transação (requer atestado manual)	Os detalhes da transação do cliente (como informações do cartão de pagamento e informações sobre os grupos que realizam transações) estão armazenados em uma zona perimetral?	Especifique se os detalhes da transação do cliente (como informações do cartão de pagamento e informações sobre os grupos que realizam transações) serão armazenados em uma zona perimetral. Em caso afirmativo, explique por que eles precisam ser armazenados na zona perimetral.	Não

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança de dados 2.5.4 - Armazenamento e classificação de dados - Classificação de informações	Os dados do cliente são classificados de acordo com os requisitos legais ou regulamentares, o valor comercial e a sensibilidade à divulgação ou modificação não autorizadas?	Especifique se os dados do cliente são classificados por confidencialidade. Em caso afirmativo, faça o upload da evidência manual dessa classificação.	Sim
	Segurança de dados 2.5.5 - Armazenamento e classificação de dados - Segmentação de dados (requer atestado manual)	A capacidade de segmentação e separação de dados entre clientes é fornecida?	Especifique se os dados de diferentes clientes são segmentados. Em caso negativo, explique os mecanismos necessários para proteger os dados contra contaminação cruzada.	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Retenção de dados	Segurança de dados 2.6.1 - Retenção de dados (requer atestado manual)	Por quanto tempo você retém os dados?	Especifique a duração da retenção de dados. Se o período de retenção diferir de acordo com a classificação e a confidenc ialidade dos dados, você pode fornecer detalhes sobre cada período de retenção?	6 meses
Retenção de dados após o cancelamento da assinatura dos compradores	Segurança de dados 2.6.2 - Retenção de dados após o cancelamento da assinatur a do cliente (requer atestado manual)	Por quanto tempo você retém os dados depois que os compradores cancelam a assinatura?	Especifique a duração da retenção de dados após o cancelamento da assinatura dos clientes.	3 meses

Controles de segurança do dispositivo de usuário final

Os controles de segurança do dispositivo do usuário final protegem os dispositivos portáteis do usuário final e as redes às quais eles estão conectados contra ameaças e vulnerabilidades. Esta tabela lista os valores e as descrições dos controles da política de segurança do dispositivo do usuário final.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Inventário de ativos/software	Segurança do dispositivo do usuário final 7.1.1 - Inventário de ativos/software - Inventário de ativos	A lista de inventário de ativos é atualizada periodicamente?	Especifique se um inventário de ativos é mantido. Em caso afirmativo, com que frequência ele é atualizado?	Sim. O inventário é atualizado semanalmente.
	Segurança do dispositivo do usuário final 7.1.2 - Inventário de ativos/software - Inventário de software e aplicações	Todas as plataformas e aplicações de software instalados em sistemas com escopo definido são inventariados?	Especifique se o inventário de todos os softwares e aplicações instalados é mantido. Em caso afirmativo, com que frequência ele é atualizado?	Sim. O inventário é atualizado semanalmente.
Segurança de ativos	Segurança do dispositivo do usuário final 7.2.1 - Segurança de ativos - Patches de segurança	Todos os patches de segurança de alto risco disponíveis são aplicados e verificados pelo menos mensalmente em todos os dispositivos do usuário final?	Especifique se todos os patches de segurança de alto risco são aplicados pelo menos uma vez por mês. Em caso negativo, com que frequência são aplicados? Você pode	Sim. Temos uma equipe de segurança que realiza esse processo quinzenalmente.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
			fornecer mais detalhes sobre como gerenciar os patches?	
	Segurança do dispositivo do usuário final 7.2.2 - Segurança de ativos - Segurança de endpoint	Você tem segurança de endpoint?	Especifique se a segurança de endpoint está instalada em todos os dispositivos. Em caso afirmativo, você pode fornecer mais detalhes sobre a ferramenta e como ela é mantida?	Sim. Nossa equipe de segurança lida com isso quinzenalmente usando ferramentas internas.
	Segurança do dispositivo do usuário final 7.2.3 - Segurança de ativos - Manutenção e reparo de ativos (requer atestado manual)	A manutenção e o reparo dos ativos organizacionais são realizados e registrados, com ferramentas aprovadas e controladas?	Especifique se a manutenção e o reparo dos ativos são executados e registrados com ferramentas controladas. Em caso afirmativo, você poderia fornecer mais detalhes sobre como isso é gerenciado?	Sim. Toda a manutenção dos dispositivos é registrada. Essa manutenção não causa tempo de inatividade.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança do dispositivo do usuário final 7.2.4 - Segurança de ativos - Controle de acesso para dispositivos	Os dispositivos têm controle de acesso habilitado?	Especifique se os dispositivos têm controles de acesso (como RBAC) habilitados.	Sim. O acesso com privilégios mínimos é implementado para todos os dispositivos.
Logs do dispositivo	Segurança do dispositivo do usuário final 7.3.1 - Logs do dispositivo - Detalhes suficientes nos logs (requer atestado manual)	Há detalhes suficientes registrados nos logs do sistema operacional e do dispositivo para apoiar a investigação de incidentes?	Especifique se detalhes suficientes (como tentativas de login bem-sucedidas e com falha e alterações em configurações e arquivos confidenciais) estão incluídos nos logs para apoiar a investigação de incidentes. Em caso negativo, forneça mais detalhes sobre como você lida com as investigações de incidentes.	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança do dispositivo do usuário final 7.3.2 - Logs do dispositivo - Acesso aos logs do dispositivo	Os logs do dispositivo estão protegidos contra modificação, exclusão e/ou acesso inadequado?	Especifique se os logs do dispositivo estão protegidos contra modificação, exclusão e/ou acesso inadequado. Em caso afirmativo, você pode fornecer detalhes sobre como aplicá-la?	Sim. As alterações nos logs são impostas pelo controle de acesso. Todas as alterações nos logs geram um alerta.
	Segurança do dispositivo do usuário final 7.3.3 - Logs do dispositivo - Retenção de logs (requer atestado manual)	Os logs são mantidos por tempo suficiente para investigar um ataque?	Por quanto tempo os logs serão retidos?	Sim, um ano.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Gerenciamento de dispositivos móveis	Segurança do dispositivo do usuário final 7.4.1 - Gerenciamento de dispositivos móveis - Programa de gerenciamento de dispositivos móveis	Existe algum programa de gerenciamento de dispositivos móveis?	Especifique se há algum programa de gerenciamento de dispositivos móveis. Em caso afirmativo, especifique qual ferramenta é usada para gerenciamento de dispositivos móveis.	Sim. Usamos ferramentas internas.
	Segurança do dispositivo do usuário final 7.4.2 - Gerenciamento de dispositivos móveis - Acesse o ambiente de produção a partir de dispositivos móveis privados (requer atestado manual)	A equipe está impedida de acessar o ambiente de produção usando dispositivos móveis privados não gerenciados?	Especifique se os funcionários são impedidos de acessar o ambiente de produção usando dispositivos móveis privados não gerenciados. Em caso negativo, como você aplica esse controle?	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança do dispositivo do usuário final 7.4.3 - Gerenciamento de dispositivos móveis - Acesse dados do cliente a partir de dispositivos móveis (requer atestado manual)	Os funcionários são impedidos de usar dispositivos móveis privados não gerenciados para visualizar ou processar dados de clientes?	Especifique se os funcionários são impedidos de acessar os dados do cliente usando dispositivos móveis não gerenciados. Em caso negativo, qual é o caso de uso para permitir o acesso? Como você monitora o acesso?	Sim

Controles de recursos humanos

Os controles de recursos humanos avaliam a divisão relacionada a funcionários para lidar com dados confidenciais durante processos como contratação, pagamento e demissão de funcionários. Esta tabela lista os valores e as descrições dos controles de políticas de recursos humanos.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Política de recursos humanos	Recursos humanos 9.1.1 - Política de recursos humanos - Análise de	A análise de antecedentes é feita antes da contratação?	Especifique se a análise de antecedentes é feita para todos os funcionários antes da contratação.	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	antecedentes dos funcionários			
	Recursos humanos 9.1.2 - Política de recursos humanos - Contrato de funcionários	Um contrato de trabalho é assinado antes da contratação?	Especifique se um contrato de trabalho foi assinado antes da contratação.	Sim
	Recursos humanos 9.1.3 - Política de recursos humanos - Treinamento de segurança para funcionários	Todos os funcionários passam por treinamento de conscientização sobre segurança regularmente?	Especifique se os funcionár ios passam por treinamento de segurança regularme nte. Em caso afirmativo, com que frequência eles passam por treinamento de segurança?	Sim. Eles passam por treinamento de segurança anualmente.
	Recursos humanos 9.1.4 - Política de recursos humanos - Processo disciplinar por não conformid ade de políticas	Existe um processo disciplinar para o não cumprimen to das políticas de recursos humanos?	Especifique se há um processo disciplinar por não conformid ade com as políticas de recursos humanos.	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Recursos humanos 9.1.5 - Política de recursos humanos - Verificação de antecedentes de empreiteiros/ subcontratados (requer atestado manual)	As verificações de antecedentes são realizadas para fornecedores, contratados e subcontratados terceirizados?	Especifique se a verificação de antecedentes é feita para fornecedores, contratados e subcontratados terceirizados. Em caso afirmativo, a verificação de antecedentes é feita regularmente?	Sim. A verificação de antecedentes é feita anualmente.
	Recursos humanos 9.1.6 - Política de recursos humanos - Devolução de ativos após a demissão	Existe um processo para verificar a devolução dos ativos constituintes após a demissão?	Especifique se há um processo para verificar a devolução dos ativos constituintes após a demissão do funcionário.	Sim

Controles de segurança da infraestrutura

Os controles de segurança da infraestrutura protegem ativos críticos contra ameaças e vulnerabilidades. Esta tabela lista os valores e as descrições dos controles da política de segurança da infraestrutura.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Segurança física	Segurança da infraestrutura 8.1.1 - Segurança física - Acesso físico às instalações	As pessoas que precisam de acesso presencial aos ativos (como edifícios, veículos ou hardware) precisam fornecer identificação e todas as credenciais necessárias?	Especifique se as pessoas que precisam de acesso presencial aos ativos (como edifícios, veículos, hardware) devem fornecer identificação e todas as credenciais necessárias.	Sim
	Segurança da infraestrutura 8.1.2 - Segurança física - Segurança física e controles ambientais em vigor	A segurança física e os controles ambientais estão em vigor no datacenter e nos prédios de escritórios?	Especifique se a segurança física e os controles ambientais estão em vigor para todas as instalações.	Sim
	Segurança da infraestrutura 8.1.3 - Segurança física - Acesso de visitantes (requer atestado manual)	Você registra o acesso dos visitantes?	Se os visitantes tiverem permissão para entrar na instalação, os logs de acesso dos visitantes são mantidos? Em	Sim. Os logs serão mantidos por um ano.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
			caso afirmativo, por quanto tempo os logs são retidos?	
Segurança de rede	Segurança da infraestrutura 8.2.1 - Segurança de rede - Desabilitar portas e serviços não utilizados (requer atestado manual)	Todas as portas e serviços não utilizados estão desabilitados no ambiente e nos sistemas de produção?	Especifique se todas as portas e serviços não utilizados estão desabilitados no ambiente e nos sistemas de produção.	Sim
	Segurança da infraestrutura 8.2.2 - Segurança de rede - Uso de firewalls	Os firewalls são usados para isolar sistemas críticos e confidenciais em segmentos de rede separados dos segmentos de rede com sistemas menos confidenciais?	Especifique se os firewalls são usados para isolar segmentos críticos e sensíveis de segmentos com sistemas menos sensíveis.	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança da infraestrutura 8.2.3 - Segurança de rede - Revisão das regras de firewall	Todas as regras de firewalls são revisadas e atualizadas regularmente?	Com que frequência as regras de firewall são revisadas e atualizadas?	Sim. As regras de firewall são atualizadas a cada três meses.
	Segurança da infraestrutura 8.2.4 - Segurança de rede - Sistemas de detecção/prevenção de intrusões	Os sistemas de detecção e prevenção de intrusões estão implantados em todas as zonas confidenciais da rede e onde quer que os firewalls estejam habilitados?	Especifique se os sistemas de detecção e prevenção de intrusões estão habilitados em todas as zonas confidenciais da rede.	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Segurança da infraestrutura 8.2.5 - Segurança de rede - Padrões de segurança e fortalecimento	Você tem padrões de segurança e fortalecimento em vigor para dispositivos de rede?	Especifique se você tem padrões de segurança e fortalecimento em vigor para dispositivos de rede. Em caso afirmativo, você pode fornecer mais detalhes (incluindo detalhes sobre a frequência com que esses padrões são implementados e atualizados)?	Sim. Os padrões de segurança e fortalecimento são implementados mensalmente nos dispositivos de rede.
Serviços em nuvem	Segurança da infraestrutura 8.3.1 - Serviços em nuvem - Plataformas usadas para hospedar aplicações (requer atestado manual)	Liste as plataformas de nuvem que você usa para hospedar sua aplicação.	Especifique quais plataformas de nuvem você usa para hospedar sua aplicação.	AWS

Controles de gerenciamento de riscos e resposta a incidentes

O gerenciamento de riscos e os controles de resposta a incidentes avaliam o nível de risco considerado aceitável e as medidas tomadas para responder aos riscos e ataques. Esta tabela lista os valores e as descrições dos controles de gerenciamento de riscos e políticas de resposta a incidentes.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Avaliação de risco	Gerenciamento de riscos/resposta a incidentes 5.1.1 - Avaliação de riscos - Abordar e identificar riscos	Existe um processo formal focado em identificar e abordar os riscos de incidentes disruptivos para a organização?	Especifique se há um processo para identificar e abordar os riscos que causam incidentes disruptivos para a organização.	Sim
	Gerenciamento de riscos/resposta a incidentes 5.1.2 - Avaliação de riscos - Processo de gerenciamento de riscos	Existe um programa ou processo para gerenciar o tratamento dos riscos identificados durante as avaliações?	Especifique se há um programa ou processo para gerenciar riscos e mitigações. Em caso afirmativo, você pode fornecer mais detalhes sobre o processo de gerenciamento de riscos?	Sim. Analisamos e corrigimos problemas regularmente para abordar não conformidades. As informações a seguir são identificadas para qualquer problema que afete nosso meio ambiente: • Detalhes do problema identificado

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
				• Causa raiz • Controles de compensação • Gravidade • Proprietário • Rumo a curto prazo • Rumo a longo prazo
	Gerenciamento de riscos/resposta a incidentes 5.1.3 - Avaliação de risco - Avaliações de risco	As avaliações de risco são feitas com frequência?	As avaliações de risco são feitas com frequência? Em caso afirmativo, especifique a frequência das avaliações de risco.	Sim. As avaliações de risco são concluídas a cada seis meses.
	Gerenciamento de riscos/resposta a incidentes 5.1.4 - Avaliação de risco - Avaliação de risco de fornecedores de terceiros	As avaliações de risco são realizadas para todos os fornecedores de terceiros?	Especifique se as avaliações de risco são realizadas para todos os fornecedores de terceiros. Em caso afirmativo, com que frequência?	Não aplicável nesta amostra.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Gerenciamento de riscos/resposta a incidentes 5.1.5 - Avaliação de risco - Reavaliação de risco quando o contrato muda	As avaliações de risco são realizadas quando ocorrem mudanças na prestação de serviços ou no contrato?	Especifique se as avaliações de risco serão realizadas sempre que uma prestação de serviço ou contrato for alterada.	Não aplicável nesta amostra.
	Gerenciamento de riscos/resposta a incidentes 5.1.6 - Avaliação de riscos - Aceitar riscos (requer atestado manual)	Existe um processo para a gerência aceitar riscos de forma consciente e objetiva e aprovar planos de ação?	Especifique se há um processo para a gerência entender e aceitar riscos e aprovar planos de ação e um cronograma para corrigir um problema relacionado ao risco. O processo inclui fornecer detalhes das métricas por trás de cada risco para a gerência?	Sim. Detalhes sobre a gravidade do risco e os possíveis problemas, se não forem mitigados, são fornecidos à gerência antes que ela aprove um risco.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Gerenciamento de riscos/resposta a incidentes 5.1.7 - Avaliação de risco - Métricas de risco (requer atestado manual)	Você tem medidas para definir, monitorar e relatar métricas de risco?	Especifique se há um processo para definir, monitorar e relatar métricas de risco.	Sim
Gerenciamento de incidentes	Gerenciamento de riscos/resposta a incidentes 5.2.1 - Gerenciamento de incidentes - Plano de resposta a incidentes	Existe um plano formal de resposta a incidentes?	Especifique se há um plano formal de resposta a incidentes.	Sim
	Gerenciamento de riscos/resposta a incidentes 5.2.2 - Gerenciamento de incidentes - Entre em contato para relatar incidentes de segurança (requer atestado manual)	Existe um processo para os clientes denunciarem um incidente de segurança?	Especifique se há um processo para os clientes relatarem um incidente de segurança. Em caso afirmativo, como um cliente pode relatar um incidente de segurança?	Sim. Os clientes podem denunciar incidentes em example.com.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Gerenciamento de riscos/resposta a incidentes 5.2.3 - Gerenciamento de incidentes - Relatar incidentes/principais atividades	Você relata as principais atividades?	Você relata as principais atividades? Qual é o SLA para relatar as principais atividades?	Sim. Todas as principais atividades serão relatadas em uma semana.
	Gerenciamento de riscos/resposta a incidentes 5.2.4 - Gerenciamento de incidentes - Recuperação de incidentes	Você tem planos de recuperação de desastres?	Especifique se você tem planos de recuperação após a ocorrência de um incidente. Em caso afirmativo, você pode compartilhar detalhes sobre os planos de recuperação?	Sim. Após um incidente, a recuperação será feita em 24 horas.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Gerenciamento de riscos/resposta a incidentes 5.2.5 - Gerenciamento de incidentes - Logs disponíveis para compradores em caso de ataque (requer atestado manual)	No caso de um ataque, os recursos relevantes (como logs, relatórios de incidentes ou dados) estarão disponíveis para os clientes?	Recursos relevantes (como logs, relatórios de incidentes ou dados) relacionados ao uso estarão disponíveis para os clientes caso ocorra um ataque ou incidente?	Sim
	Gerenciamento de riscos/resposta a incidentes 5.2.6 - Gerenciamento de incidentes - Boletim de segurança (requer atestado manual)	Você tem um boletim de segurança que descreve os ataques e vulnerabilidades mais recentes que afetam suas aplicações?	Especifique se você tem um boletim de segurança que descreve os ataques e vulnerabilidades mais recentes que afetam suas aplicações. Em caso afirmativo, você pode fornecer os detalhes?	Sim. Os clientes podem denunciar incidentes em example.com.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Detecção de incidente	Gerenciamento de riscos/resposta a incidentes 5.3.1 - Detecção de incidentes - Registro em log abrangente	Existe um registro em log abrangente para apoiar a identificação e mitigação de incidentes?	Especifique se há um registro em log abrangente e habilitado. Identifique os tipos de eventos que o sistema é capaz de registrar. Por quanto tempo os logs são retidos?	Sim. Os seguintes eventos são registrados: aplicações, dispositivos e Serviços da AWS, como AWS CloudTrail, AWS Config e logs de fluxo de VPC. Os logs são retidos por um ano.
	Gerenciamento de riscos/resposta a incidentes 5.3.2 - Detecção de incidentes - Monitoramento de logs	Você monitora e alerta sobre atividades incomuns ou suspeitas usando mecanismos de detecção, como monitoramento de logs?	Especifique se o monitoramento e o alerta de segurança regulares são executados. Em caso afirmativo, isso inclui monitoramento de logs para comportamentos incomuns ou suspeitos?	Sim. Todos os registros são monitorados quanto a comportamentos incomuns, como vários logins com falha, login de uma geolocalização incomum ou outros alertas suspeitos.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
	Gerenciamento de riscos/resposta a incidentes 5.3.3 - Detecção de incidentes - Violação de dados de terceiros	Existe um processo para identificar, detectar e registrar problemas de segurança, privacidade ou violação de dados de subcontratados?	Especifique se há um processo em vigor para identificar e detectar fornecedores de terceiros ou subcontratados em caso de violação de dados, problemas de segurança ou problemas de privacidade.	Sim
SLA para notificação de incidentes	Gerenciamento de riscos/resposta a incidentes 5.4.1 - SLA para notificação de incidentes (requer atestado manual)	Qual é o SLA para enviar notificações sobre incidentes ou violações?	Qual é o SLA para enviar notificações sobre incidentes ou violações?	7 dias

Controles de políticas de segurança e configuração

Os controles de políticas de segurança e configuração avaliam as políticas e as configurações de segurança que protegem os ativos de uma organização. Esta tabela lista os valores e as descrições dos controles de política de segurança e configuração.

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
Políticas de segurança da informação	Política de segurança e configuração 10.1.1 - Políticas de segurança da informaçã o - Política de segurança da informação	Você tem uma política de segurança da informação que pertence e é mantida por uma equipe de segurança?	Especifique se você tem uma política de segurança da informação. Em caso afirmativ o, compartil he ou envie uma evidência manual.	Sim. Construím os nossa política de segurança com base na estrutura do NIST.
	Política de segurança e configuração 10.1.2 - Políticas de segurança da informaçã o - Revisão de políticas	Todas as políticas de segurança são revisadas anualmente?	Especifique se as políticas de segurança são revisadas anualment e. Em caso negativo, com que frequência as políticas são revisadas?	Sim. Revisadas todos os anos.
Políticas para configurações de segurança	Política de segurança e configura ção 10.2.1 - Políticas para configurações de segurança - Configurações de segurança (requer atestado manual)	Os padrões de configuração de segurança são mantidos e documentados?	Especifique se todos os padrões de configuração de segurança são mantidos e documenta dos. Em caso afirmativo, compartilhe ou envie uma	Sim

Conjunto de controles	Título do controle	Descrição do controle	Detalhe da extração de evidências	Valor de exemplo
			evidência manual.	
	Política de segurança e configuração 10.2.2 - Políticas para configurações de segurança - Análise das configurações de segurança (requer atestado manual)	As configurações de segurança são revisadas pelo menos uma vez por ano?	Especifique se as configurações de segurança são revisadas pelo menos uma vez por ano. Em caso negativo, especifique a frequência da revisão.	Sim. Revisadas a cada três meses.
	Política de segurança e configuração 10.2.3 - Políticas para configurações de segurança - Alterações nas configurações	As alterações nas configurações são registradas?	Especifique se as alterações de configuração são registradas. Em caso afirmativo, por quanto tempo os logs são retidos?	Sim. Todas as alterações nas configurações são monitoradas e registradas. Os alertas são gerados quando as configurações são alteradas. Os logs são retidos por seis meses.

Exportação de instantâneos como comprador usando o AWS Marketplace Vendor Insights

Um instantâneo do perfil de segurança é uma postura point-in-time. A exportação de instantâneos fornece uma maneira de baixar e revisar dados off-line, analisar dados de evidências e comparar produtos.

Exportar um instantâneo

Você pode exportar para os formatos JSON ou CSV. Para exportar um instantâneo, siga estas etapas.

1. Faça login no AWS Management Console e abra o AWS Marketplace console.
2. Escolha Vendor Insights.
3. No Vendor Insights, escolha um produto.
4. Na guia Segurança e conformidade, vá para a seção Resumo e escolha Exportar.
5. Na lista suspensa, escolha Baixar (JSON) ou Baixar (CSV).

Controle do acesso no AWS Marketplace Vendor Insights

O AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda você a controlar o acesso aos recursos da AWS. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional. Se você for administrador, vai controlar quem pode ser autenticado (conectado) e autorizado (ter permissões) a usar os recursos do AWS Marketplace. AWS Marketplace O Vendor Insights usa o IAM para controlar o acesso aos dados, avaliações, autoatestação do vendedor e relatórios de auditoria padrão do setor.

Recomendamos que crie usuários e grupos com o IAM para controlar quem pode fazer o que no Portal de gerenciamento do AWS Marketplace. Depois, adicione usuários aos grupos e gerencie os grupos. Você pode atribuir uma política ou permissões ao grupo para fornecer permissões somente leitura. Se você tiver outros usuários que precisam de acesso somente leitura, poderá adicioná-los ao grupo que criou em vez de adicionar permissões à Conta da AWS deles.

Uma política é um documento que define as permissões que se aplicam a um usuário, grupo ou função. As permissões determinam o que os usuários podem fazer na AWS. Uma política normalmente concede acesso a ações específicas e pode, opcionalmente, permitir que as ações

sejam autorizadas para recursos específicos, como instâncias do Amazon EC2, buckets do Amazon S3 e assim por diante. As políticas também podem negar o acesso explicitamente. Uma permissão é uma instrução em uma política que concede ou nega o acesso a um recurso específico.

> **Important**
>
> Todos os usuários do que você cria são autenticados usando suas credenciais. No entanto, eles usam a mesma Conta da AWS. Qualquer alteração feita pelo usuário pode afetar toda a conta.

O AWS Marketplace tem permissões definidas para controlar as ações que alguém com essas permissões pode tomar no Portal de gerenciamento do AWS Marketplace. Também há políticas que o AWS Marketplace cria e gerencia que combinam várias permissões. A política `AWSMarketplaceSellerProductsFullAccess` concede ao usuário acesso total aos produtos no Portal de gerenciamento do AWS Marketplace.

Para obter mais informações sobre as ações, os recursos e as chaves de condição disponíveis, consulte Ações, recursos e chaves de condição do AWS Marketplace Vendor Insights na Referência de autorização de serviço.

Permissões para compradores do AWS Marketplace Vendor Insights

Você pode usar as seguintes permissões nas políticas do IAM para o AWS Marketplace Vendor Insights. Você pode combinar as permissões em uma única política do IAM para conceder as permissões desejadas.

`GetProfileAccessTerms`

`GetProfileAccessTerms` permite que os usuários recuperem os termos necessários para revisar, aceitar e obter acesso a um perfil do AWS Marketplace Vendor Insights.

Grupos de ação: somente leitura e leitura/gravação.

Recursos necessários: `SecurityProfile`.

`ListEntitledSecurityProfiles`

`ListEntitledSecurityProfiles` permite que os usuários listem todos os perfis de segurança que eles têm o direito ativo de ler.

Grupos de ação: somente leitura, somente lista e leitura/gravação.

Recursos necessários: nenhum

`ListEntitledSecurityProfileSnapshots`

`ListEntitledSecurityProfileSnapshots` permite que os usuários listem os instantâneos de um perfil de segurança que eles tenham o direito ativo de ler.`SecurityProfile`.

Grupos de ação: somente leitura, somente lista e leitura/gravação.

Recursos necessários: `SecurityProfile`

`GetEntitledSecurityProfileSnapshot`

`GetEntitledSecurityProfileSnapshot` permite que os usuários obtenham os detalhes de um instantâneo de um perfil de segurança que eles tenham o direito ativo de ler.

Grupos de ação: somente leitura e leitura/gravação.

Recursos necessários: `SecurityProfile`

Segurança no AWS Marketplace

Listamos softwares de vendedores de alta qualidade e trabalhamos ativamente para manter a qualidade de nossa seleção. Como cada cliente é diferente, nosso objetivo é fornecer informações suficientes sobre os produtos listados no AWS Marketplace para que os clientes possam tomar boas decisões de compra.

> **Note**
>
> Para obter informações sobre segurança para produtos de dados no AWS Data Exchange, consulte Segurança no Guia do usuário do AWS Data Exchange.
> Para obter informações sobre segurança para vendedores no AWS Marketplace, consulte Segurança do AWS Marketplace no Guia do usuário do AWS Marketplace.

Informações de assinantes compartilhadas com vendedores

Podemos compartilhar suas informações de contato com nossos vendedores pelos seguintes motivos:

- Se for necessário que eles forneçam treinamento e suporte técnico ao cliente.
- Para ativação de software, configuração e personalização de conteúdo.
- Compensar suas equipes de vendas internamente.

Além disso, podemos compartilhar informações como nome da empresa, endereço completo e taxas de uso com vendedores para que eles remunerem suas equipes de vendas. Também podemos compartilhar determinadas informações com vendedores para ajudá-los a avaliar a eficácia das campanhas de marketing. Os vendedores podem usar essas informações junto com informações que eles já possuem para determinar prêmios para suas equipes de vendas ou usar para um determinado comprador.

Caso contrário, geralmente não compartilhamos informações de clientes com vendedores, e quaisquer informações compartilhadas não são de identificação pessoal, a menos que você nos dê permissão para compartilhar essas informações ou se acreditarmos que o fornecimento das informações aos vendedores é necessário para estarmos em conformidade com leis ou regulamentações.

Atualizar as políticas do IAM para IPv6

Os clientes do AWS Marketplace usam políticas do IAM para definir um intervalo permitido de endereços IP e impedir que qualquer endereço IP fora do intervalo configurado possa acessar os recursos do AWS Marketplace.

O domínio do site do AWS Marketplace está sendo atualizado para o protocolo IPv6.

As políticas de filtragem de endereços IP que não estiverem atualizadas para lidar com endereços IPv6 podem resultar na perda de acesso de clientes aos recursos do site do AWS Marketplace.

Clientes afetados pela atualização de IPv4 para IPv6

Os clientes que estão usando o endereçamento duplo são afetados por essa atualização. O endereçamento duplo indica que a rede oferece suporte a IPv4 e IPv6.

Se você estiver usando endereçamento duplo, deverá atualizar as políticas do IAM que estão atualmente configuradas com endereços no formato IPv4 para incluir endereços no formato IPv6.

Para obter ajuda com problemas de acesso, entre em contato com AWS Support.

> **Note**
>
> Os seguintes clientes não são afetados por essa atualização:
>
> - Clientes que estão somente em redes IPv4.
> - Clientes que estão somente em redes IPv6.

O que é IPv6?

IPv6 é o padrão IP de última geração destinado a substituir o IPv4. A versão anterior, IPv4, usa um esquema de endereçamento de 32 bits para suportar 4,3 bilhões de dispositivos. Em vez disso, o IPv6 usa endereçamento de 128 bits para suportar aproximadamente 340 trilhões de trilhões de trilhões (ou 2 vezes a 128ª potência) de dispositivos.

```
2001:cdba:0000:0000:0000:0000:3257:9652
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:965
```

Atualização de uma política do IAM para IPv6

Atualmente, as políticas do IAM são usadas para definir um intervalo permitido de endereços IP usando o filtro `aws:SourceIp`.

O endereçamento duplo suporta tráfego IPv4 e IPV6. Se sua rede usa endereçamento duplo, você deve garantir que todas a políticas do IAM usadas para filtragem de endereços IP estejam atualizadas para incluir intervalos de endereços IPv6.

Por exemplo, essa política de bucket do Amazon S3 identifica os intervalos de endereços IPv4 permitidos `192.0.2.0.*` e `203.0.113.0.*` no elemento `Condition`.

```
# https://docs.aws.amazon.com/IAM/latest/UserGuide/
reference_policies_examples_aws_deny-ip.html
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*",
        "Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*",
                    "*203.0.113.0/24*"
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
    }
}
```

Para atualizar essa política, o elemento `Condition` da política é atualizado para incluir intervalos de endereços IPv6 `2001:DB8:1234:5678::/64` e `2001:cdba:3257:8593::/64`.

> **Note**
>
> NÃO REMOVA os endereços IPv4 existentes porque eles são necessários para a compatibilidade com versões anteriores.

```
"Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*", <<DO NOT remove existing IPv4 address>>
                    "*203.0.113.0/24*", <<DO NOT remove existing IPv4 address>>
                    "*2001:DB8:1234:5678::/64*", <<New IPv6 IP address>>
                    "*2001:cdba:3257:8593::/64*" <<New IPv6 IP address>>
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
```

Para obter mais informações sobre permissões de acesso com o IAM, consulte Políticas gerenciadas e políticas em linha no Guia do usuário do AWS Identity and Access Management.

Teste da rede após a atualização de IPv4 para IPv6

Depois de atualizar as políticas do IAM para o formato IPv6, você pode testar se sua rede está acessando o endpoint IPv6 e a funcionalidade do site do AWS Marketplace.

Tópicos

- Teste da rede com Linux/Unix ou Mac OS X
- Teste da rede com o Windows 7 ou o Windows 10
- Teste do site do AWS Marketplace

Teste da rede com Linux/Unix ou Mac OS X

Se estiver usando o Linux/Unix ou o Mac OS X, você poderá testar se sua rede está acessando o endpoint do IPv6 usando o comando curl a seguir:

```
curl -v -s -o /dev/null http://ipv6.ec2-reachability.amazonaws.com/
```

Por exemplo, se estiver conectado por meio do IPv6, o endereço IP conectado exibirá as informações a seguir:

```
* About to connect() to aws.amazon.com port 443 (#0)
*   Trying IPv6 address... connected
* Connected to aws.amazon.com (IPv6 address) port 443 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.18.1 (x86_64-unknown-linux-gnu) libcurl/7.18.1 OpenSSL/1.0.1t
 zlib/1.2.3
> Host: aws.amazon.com
```

Teste da rede com o Windows 7 ou o Windows 10

Se estiver usando o Windows 7 ou 10, você poderá testar se sua rede pode acessar um endpoint de pilha dupla por meio do IPv6 ou do IPv4. Use o comando `ping` conforme mostrado no exemplo a seguir.

```
ping aws.amazon.com
```

Esse comando retornará endereços IPv6 se você estiver acessando um endpoint via IPv6.

Teste do site do AWS Marketplace

Testar a funcionalidade do site do AWS Marketplace após a atualização depende principalmente de como sua política foi escrita e para que ela é usada. Em geral, você deve verificar se a funcionalidade especificada na política funciona conforme o esperado.

Os cenários a seguir podem ajudar você a começar com o teste da funcionalidade do site do AWS Marketplace.

Como comprador no site do AWS Marketplace, teste se é possível realizar as tarefas a seguir:

- Assinar um produto do AWS Marketplace.
- Configurar um produto do AWS Marketplace.
- Lançar ou executar um produto do AWS Marketplace.

Como vendedor no site do AWS Marketplace, teste se é possível realizar as tarefas a seguir:

- Gerenciar os produtos do AWS Marketplace existentes.
- Criar um produto do AWS Marketplace.

Controlar o acesso a assinaturas do AWS Marketplace

O AWS IAM Identity Center ajuda você a criar ou conectar com segurança suas identidades de força de trabalho e gerenciar seu acesso centralmente em todas as Contas da AWS e aplicações. O Centro de Identidade do IAM é a abordagem recomendada para a autenticação e a autorização da força de trabalho na AWS para organizações de qualquer tamanho e tipo. Para obter orientações adicionais de configuração, revise a Arquitetura de referência de segurança da AWS.

O Centro de Identidade do IAM fornece um portal de usuário em que os usuários finais podem encontrar e acessar em um único lugar as Conta da AWS atribuídas, funções, aplicações de nuvem e aplicações personalizadas. O Centro de Identidade do IAM atribui acesso de login único a usuários e grupos em seu diretório conectado e usa conjuntos de permissões para determinar seu nível de acesso. Isso habilita credenciais de segurança temporárias. Você pode definir seu nível de acesso atribuindo funções gerenciadas pela AWS específicas para acesso do AWS Marketplace para delegar o gerenciamento de assinaturas do AWS Marketplace em toda a sua organização da AWS.

Por exemplo, o Cliente A assume uma função por meio da federação com a política `ManagedMarketplace_ViewOnly` anexada à função. Isso significa que o Cliente A só pode ver as assinaturas no AWS Marketplace. Você pode criar um perfil do IAM com permissões para visualizar assinaturas e conceder permissão ao Cliente A para assumir essa função.

Criação de perfis do IAM para acesso do AWS Marketplace

Você pode usar funções do IAM para delegar acesso aos seus recursos da AWS.

Para criar perfis do IAM para atribuir permissões do AWS Marketplace

1. Abra o console do IAM.
2. No painel de navegação à esquerda, escolha Roles (Funções) e Create role (Criar função).
3. Escolha a Conta da AWS.
4. Em Adicionar permissões, selecione uma das seguintes políticas:

   - Para conceder permissões somente para visualizar assinaturas, mas não alterá-las, escolha AWSMarketplaceRead-only.
   - Para conceder permissões para assinar e cancelar assinaturas, escolha AWSMarketplaceManageSubscriptions.
   - Para permitir controle total de suas assinaturas, escolha AWSMarketplaceFullAccess.

5. Escolha Next (Próximo).
6. Em Nome da função, digite um nome para a função. Por exemplo, *MarketplaceReadOnly* ou *MarketplaceFullAccess*. Então, escolha Criar função. Para ter mais informações, consulte Criar perfis do IAM.

> **Note**
>
> O administrador da conta especificada pode conceder permissão para assumir essa função a qualquer usuário do .

Repita as etapas anteriores para criar mais funções com conjuntos de permissões diferentes para que cada pessoa de usuário possa usar o perfil do IAM com permissões personalizadas.

Você não está limitado às permissões das políticas gerenciadas pela AWS descritas aqui. Você pode usar o IAM para criar políticas com permissões personalizadas e, em seguida, adicionar essas políticas a perfis do IAM. Para ter mais informações, consulte Gerenciar políticas do IAM e Adicionar permissões de identidade do IAM.

Políticas gerenciadas pela AWS para o AWS Marketplace

Você pode usar políticas gerenciadas pela AWS para fornecer as permissões básicas do AWS Marketplace. Depois, para cada cenário exclusivo, você pode criar suas próprias políticas e aplicá-las aos perfis com os requisitos específicos para o cenário. As seguintes políticas gerenciadas básicas do AWS Marketplace estão disponíveis para você controlar quem tem quais permissões:

- `AWSMarketplaceRead-only`
- `AWSMarketplaceManageSubscriptions`
- `AWSPrivateMarketplaceRequests`
- `AWSPrivateMarketplaceAdminFullAccess`
- `AWSMarketplaceFullAccess`

O AWS Marketplace também fornece políticas gerenciadas especializadas para cenários específicos. Para obter uma lista completa das políticas gerenciadas pela AWS para compradores do AWS Marketplace, bem como descrições das permissões que eles fornecem, consulte Políticas gerenciadas pela AWS para compradores do AWS Marketplace.

Permissões para trabalhar com o Gerenciador de licença

O AWS Marketplace se integra ao AWS License Manager para gerenciar e compartilhar licenças de produtos que você assina entre contas em sua organização. Para ver os detalhes completos de suas assinaturas no AWS Marketplace, um usuário deve ser capaz de listar as informações da licença no AWS License Manager.

Para garantir que seus usuários tenham as permissões necessárias para ver todos os dados sobre seus produtos e assinaturas do AWS Marketplace, adicione a seguinte permissão:

- `license-manager:ListReceivedLicenses`

Para ver mais informações sobre definição de permissões, consulte Gerenciar políticas do IAM no Guia do usuário do IAM.

Recursos adicionais

Para obter mais informações sobre como gerenciar perfis do IAM, consulte Identidades do IAM (usuários, grupos de usuários e perfis) no Guia do usuário do IAM.

Para obter mais informações sobre o gerenciamento de permissões e políticas do IAM, consulte Controle do acesso a recursos da AWS usando políticas no Guia do usuário do IAM.

Para obter mais informações sobre como gerenciar permissões e políticas do IAM para produtos de dados no AWS Data Exchange, consulte Gerenciamento de identidade e acesso no AWS Data Exchange no Guia do usuário do AWS Data Exchange.

Políticas gerenciadas pela AWS para compradores do AWS Marketplace

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para todos os clientes da AWS usarem. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em um política gerenciada pela AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política está vinculada. É mais provável que a AWS atualize uma política gerenciada pela AWS quando um novo AWS service (Serviço da AWS) é lançado ou novas operações de API são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte AWSPolíticas gerenciadas pela no Guia do usuário do IAM.

Esta seção lista cada uma das políticas usadas para gerenciar o acesso do comprador ao AWS Marketplace. Para obter informações sobre as políticas do vendedor, consulte Políticas gerenciadas pela AWS para vendedores do AWS Marketplace no Guia do vendedor do AWS Marketplace.

Tópicos

Política gerenciada da AWS: AWSMarketplaceDeploymentServiceRolePolicy

Não é possível anexar `AWSMarketplaceDeploymentServiceRolePolicy` às entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o AWS Marketplace realize ações em seu nome. Para ter mais informações, consulte Usar perfis vinculados a serviço do AWS Marketplace.

Essa política concede permissões de contribuidor que permitem ao AWS Marketplace gerenciar parâmetros relacionados à implantação, que são armazenados como segredos no AWS Secrets Manager, em seu nome.

AWSPolítica gerenciada da : AWSMarketplaceFullAccess

É possível anexar a política `AWSMarketplaceFullAccess` a suas identidades do IAM.

Essa política concede permissões administrativas que oferecem acesso total ao AWS Marketplace e a serviços relacionados a eles, tanto como comprador quanto como vendedor. Essas permissões incluem a capacidade de assinar e cancelar a assinatura do software AWS Marketplace, gerenciar instâncias do software AWS Marketplace no AWS Marketplace, criar e gerenciar um mercado privado em sua conta, bem como o acesso ao Amazon EC2, ao AWS CloudFormation e ao Amazon EC2 Systems Manager.

Detalhes da permissão

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:*",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStackResource",
                "cloudformation:DescribeStackResources",
                "cloudformation:DescribeStacks",
                "cloudformation:List*",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
```

```
                "ec2:DescribeVpcs",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:DeregisterImage",
                "ec2:DescribeSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:CreateImage",
                "ec2:DescribeInstanceStatus",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:DescribeDocument",
                "sns:ListTopics",
                "sns:GetTopicAttributes",
                "sns:CreateTopic",
                "iam:GetRole",
                "iam:GetInstanceProfile",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::*image-build*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:Publish",
                "sns:setTopicAttributes"
            ],
            "Resource": "arn:aws:sns:*:*:*image-build*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": [
                        "ec2.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com"
                    ],
                    "iam:AssociatedResourceARN": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
                    ]
                }
            }
        }
    ]
}
```

AWSpolítica gerenciada: AWSMarketplaceImageBuildFullAccess

> **Important**
>
> O AWS Marketplace interromperá o método de entrega do Private Image Build em abril de 2024. O método de entrega só está disponível para assinantes existentes até que seja descontinuado. Para obter mais informações, consulte Private image build.

É possível anexar a política `AWSMarketplaceImageBuildFullAccess` a suas identidades do IAM.

Esta política concede permissões ao colaborador que oferecem acesso total ao recurso de criação de imagens privadas do AWS Marketplace. Além de criar imagens privadas, ela também fornece permissões para adicionar tags às imagens e para iniciar e encerrar instâncias do Amazon EC2.

Detalhes da permissão

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListBuilds",
                "aws-marketplace:StartBuild",
                "aws-marketplace:DescribeBuilds"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:TerminateInstances",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/marketplace-image-build:build-id": "*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:role/*Automation*",
                "arn:aws:iam::*:role/*Instance*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "ec2.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:DescribeDocument",
                "ec2:DeregisterImage",
                "ec2:CopyImage",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:DescribeImages",
                "ec2:DescribeSubnets",
                "ec2:DeleteSnapshot",
                "ec2:CreateImage",
                "ec2:RunInstances",
                "ec2:DescribeInstanceStatus",
                "sns:GetTopicAttributes",
                "iam:GetRole",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::*image-build*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:*::image/*",
                "arn:aws:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:Publish"
            ],
            "Resource": [
                "arn:aws:sns:*:*:*image-build*"
            ]
        }
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com"
                    ],
                    "iam:AssociatedResourceARN": [
                "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
                "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
                "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
                "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
                "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
                "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
                "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
                "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
                    ]
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/marketplace-image-build:build-id": "*"
                },
                "StringNotEquals": {
                    "ec2:CreateAction": "RunInstances"
                }
            }
        }
    ]
}
```

AWSpolítica gerenciada: AWSMarketplaceLicenseManagementServiceRolePolicy

Você não pode se vincular AWSMarketplaceLicenseManagementServiceRolePolicy às suas entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o AWS Marketplace realize ações em seu nome. Para ter mais informações, consulte Usar perfis vinculados a serviço do AWS Marketplace.

Essa política concede permissões ao colaborador que permitem que o AWS Marketplace gerencie licenças em seu nome.

Detalhes da permissão

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLicenseManagerActions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "license-manager:ListReceivedGrants",
                "license-manager:ListDistributedGrants",
                "license-manager:GetGrant",
                "license-manager:CreateGrant",
                "license-manager:CreateGrantVersion",
                "license-manager:DeleteGrant",
```

```
                "license-manager:AcceptGrant"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWSpolítica gerenciada: AWSMarketplaceManageSubscriptions

É possível anexar a política `AWSMarketplaceManageSubscriptions` a suas identidades do IAM.

Essa política concede aos colaboradores permissões que permitem a assinatura e o cancelamento da assinatura de produtos do AWS Marketplace.

Detalhes da permissão

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-marketplace:ViewSubscriptions",
                "aws-marketplace:Subscribe",
                "aws-marketplace:Unsubscribe"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "aws-marketplace:CreatePrivateMarketplaceRequests",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
```

```
                "aws-marketplace:ListPrivateListings"
            ]
        }
    ]
}
```

AWSpolítica gerenciada: AWSMarketplaceProcurementSystemAdminFullAccess

É possível anexar a política `AWSMarketplaceProcurementSystemAdminFullAccess` a suas identidades do IAM.

Essa política concede permissões de administrador que permitem gerenciar todos os aspectos de uma integração do eProcurement do AWS Marketplace, incluindo listar as contas em sua organização. Para obter mais informações sobre integrações do eProcurement, consulte Integrar o AWS Marketplace a sistemas de compras.

Detalhes da permissão

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:PutProcurementSystemConfiguration",
                "aws-marketplace:DescribeProcurementSystemConfiguration",
                "organizations:Describe*",
                "organizations:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWSpolítica gerenciada: AWSMarketplaceRead -somente

É possível anexar a política `AWSMarketplaceRead-only` a suas identidades do IAM.

Essa política concede permissões somente leitura que permitem visualizar produtos, ofertas privadas e assinaturas para sua conta do AWS Marketplace, bem como visualizar os recursos do Amazon EC2, do AWS Identity and Access Management e do Amazon SNS na conta.

Detalhes da permissão

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Action": [
                "aws-marketplace:ViewSubscriptions",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListBuilds",
                "aws-marketplace:DescribeBuilds",
                "iam:ListRoles",
                "iam:ListInstanceProfiles",
                "sns:GetTopicAttributes",
                "sns:ListTopics"
            ]
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ]
```

```
        },
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListPrivateListings"
            ]
        }
    ]
}
```

AWSpolítica gerenciada: AWSPrivateMarketplaceAdminFullAccess

É possível anexar a política `AWSPrivateMarketplaceAdminFullAccess` a suas identidades do IAM.

Essa política concede permissões de administrador que permitem acesso total para gerenciar mercados privados em sua conta (ou organização). Para obter mais informações sobre como usar vários administradores, consulte the section called “Criação de políticas personalizadas para administradores de mercados privados”.

Detalhes da permissão

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrivateMarketplaceRequestPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "PrivateMarketplaceCatalogAPIPermissions",
            "Effect": "Allow",
```

```
            "Action": [
                "aws-marketplace:ListEntities",
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:StartChangeSet",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PrivateMarketplaceCatalogTaggingPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:TagResource",
                "aws-marketplace:UntagResource",
                "aws-marketplace:ListTagsForResource"
            ],
            "Resource": "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
        },
        {
            "Sid": "PrivateMarketplaceOrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListRoots",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*"
        }
    ]
}
```

AWSpolítica gerenciada: AWSPrivateMarketplaceRequests

É possível anexar a política `AWSPrivateMarketplaceRequests` a suas identidades do IAM.

Essa política concede aos colaboradores permissões de acesso para solicitar que produtos sejam adicionados ao seu mercado privado e para visualizar essas solicitações. Essas solicitações devem ser aprovadas ou negadas por um administrador privado do mercado.

Detalhes da permissão

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:CreatePrivateMarketplaceRequests",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": "*"
        }
    ]
}
```

Política gerenciada da AWS: AWSServiceRoleForPrivateMarketplaceAdminPolicy

Não é possível anexar `AWSServiceRoleForPrivateMarketplaceAdminPolicy` às entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o AWS Marketplace realize ações em seu nome. Para ter mais informações, consulte Usar perfis vinculados a serviço do AWS Marketplace.

Essa política concede aos colaboradores permissões que permitem descrever e atualizar AWS Marketplace os recursos do Private Marketplace e descreverAWS Organizations.

AWSPolítica gerenciada da : AWSVendorInsightsAssessorFullAccess

É possível anexar a política `AWSVendorInsightsAssessorFullAccess` a suas identidades do IAM.

Essa política concede acesso total para visualização de recursos intitulados do AWS Marketplace Vendor Insights e gerenciamento de assinaturas do AWS Marketplace Vendor Insights. Essas solicitações devem ser aprovadas ou negadas por um administrador. Permite o acesso somente leitura a relatórios de terceiros do AWS Artifact.

O AWS Marketplace Vendor Insights identifica que o avaliador é igual ao comprador e o fornecedor é igual ao vendedor.

Detalhes da permissão

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource": "*"
    },
    {
      "Action": [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws-marketplace:AgreementType": "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
         "artifact:GetReport",
         "artifact:GetReportMetadata",
         "artifact:GetTermForReport",
         "artifact:ListReports"
      ],
```

```
      "Resource": "arn:aws:artifact:*::report/*"
    }
  ]
}
```

AWSPolítica gerenciada da : AWSVendorInsightsAssessorReadOnly

É possível anexar a política `AWSVendorInsightsAssessorReadOnly` a suas identidades do IAM.

Essa política concede acesso somente leitura para visualização dos recursos do AWS Marketplace Vendor Insights. Essas solicitações devem ser aprovadas ou negadas por um administrador. Permite o acesso somente leitura aos relatórios do AWS Artifact.

As solicitações devem ser aprovadas ou negadas por um administrador. Permite o acesso somente leitura a relatórios de terceiros do AWS Artifact.

O AWS Marketplace Vendor Insights identifica o avaliador como o comprador e o fornecedor é igual ao vendedor para os fins deste guia.

Detalhes da permissão

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "artifact:GetReport",
         "artifact:GetReportMetadata",
         "artifact:GetTermForReport",
         "artifact:ListReports"
      ],
      "Resource": "arn:aws:artifact:*::report/*"
    }
```

```
  ]
}
```

Atualizações do AWS Marketplace para políticas gerenciadas pela AWS

Visualizar detalhes sobre atualizações em políticas gerenciadas pela AWS para o AWS Marketplace desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página Histórico do documento do AWS Marketplace.

Alteração	Descrição	Data
AWSServiceRoleForPrivateMarketplaceAdminPolicy: adicionada política para novo recurso no AWS Marketplace	AWS Marketplaceadicion ou uma nova política para apoiar o gerenciamento e a descrição dos recursos do Private MarketplaceAWS Organizations.	16 de fevereiro de 2024
AWSPrivateMarketplaceAdminFullAccess: atualizar para uma política existente.	AWS Marketplaceatualizou a política para apoiar a leitura AWS Organizations de dados.	16 de fevereiro de 2024
AWSMarketplaceDeploymentServiceRolePolicy: adicionada política para novo recurso no AWS Marketplace	O AWS Marketplace adicionou uma nova política para dar suporte ao gerenciamento de parâmetros relacionados à implantação.	29 de novembro de 2023
AWSMarketplaceRead-somente e AWSMarketplaceManageSubscriptions—atualizações das políticas existentes	O AWS Marketplace atualizou as políticas existentes para permitir o acesso à página Ofertas privadas.	19 de janeiro de 2023
AWSPrivateMarketplaceAdminFullAccess: atualizar para uma política existente.	O AWS Marketplace atualizou a política do novo recurso de	9 de dezembro de 2022

Alteração	Descrição	Data
	autorização com base em tags.	
AWSVendorInsightsAssessorReadOnlyAWS Marketplaceatualizado `AWSVendorInsightsAssessorReadOnly`	O AWS Marketplace atualizou `AWSVendorInsightsAssessorReadOnly` para adicionar acesso somente leitura aos relatórios em relatórios de terceiros do AWS Artifact (prévia).	30 de novembro de 2022
AWSVendorInsightsAssessorFullAccessAWS Marketplaceatualizado `AWSVendorInsightsAssessorFullAccess`	O AWS Marketplace atualizou `AWSVendorInsightsAssessorFullAccess` para adicionar pesquisa de contrato e acesso somente leitura aos relatórios de terceiros do AWS Artifact (prévia).	30 de novembro de 2022
AWSVendorInsightsAssessorFullAccesse AWSVendorInsightsAssessorReadOnly— Políticas adicionadas para novos recursos em AWS Marketplace	Adição de políticas do AWS Marketplace para o novo recurso AWS Marketplace Vendor Insights: `AWSVendorInsightsAssessorFullAccess` e `AWSVendorInsightsAssessorReadOnly`	26 de julho de 2022
AWSMarketplaceFullAccess e AWSMarketplaceImageBuildFullAccess: atualizações em políticas existentes	O AWS Marketplace removeu as permissões que não eram mais necessárias para melhorar a segurança.	4 de março de 2022

Alteração	Descrição	Data
AWSPrivateMarketplaceAdminFullAccess: atualização para uma política existente	O AWS Marketplace removeu as permissões não utilizadas na política `AWSPrivateMarketplaceAdminFullAccess` .	27 de agosto de 2021
AWSMarketplaceFullAccess: atualização para uma política existente	O AWS Marketplace removeu uma permissão duplicada `ec2:DescribeAccountAttributes` da política `AWSMarketplaceFullAccess` .	20 de julho de 2021
O AWS Marketplace iniciou o rastreamento das alterações	O AWS Marketplace começou a monitorar as alterações para as políticas gerenciadas da AWS.	20 de abril de 2021

Encontrar o número da Conta da AWS para suporte ao cliente

Se você ou seus usuários precisam entrar em contato com AWS Support, você precisa do seu número de Conta da AWS.

Para encontrar o número da Conta da AWS

1. Faça login no AWS Management Console usando o nome do usuário.
2. Na parte superior da barra de navegação, escolha Support (Suporte) e, em seguida, Support Center (Atendimento ao cliente).

O ID da Conta da AWS (número da conta) é mostrado abaixo da barra de navegação superior.

Usar perfis vinculados a serviço do AWS Marketplace

O AWS Marketplace usa funções vinculadas a serviços do AWS Identity and Access Management (IAM). O perfil vinculado a serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao

AWS Marketplace. Os perfis vinculados a serviços são predefinidos pelo AWS Marketplace e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Tópicos

Uso de funções para compartilhar direitos para o AWS Marketplace

O AWS Marketplace usa funções vinculadas a serviços do AWS Identity and Access Management (IAM). O perfil vinculado a serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao AWS Marketplace. Os perfis vinculados a serviços são predefinidos pelo AWS Marketplace e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração do AWS Marketplace porque dispensa a inclusão manual das permissões necessárias. O AWS Marketplace define as permissões de funções vinculadas ao serviço e, a menos que definido em contrário, somente o AWS Marketplace pode assumir as funções. As permissões definidas incluem a política de confiança e a política de permissões. Essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Para compartilhar suas assinaturas do AWS Marketplace com outras contas em sua organização da AWS com o AWS License Manager, você deve conceder permissões do AWS Marketplace para cada conta com a qual deseja compartilhar. Faça isso usando a função AWSServiceRoleForMarketplaceLicenseManagement. Consulte Crie uma função vinculada ao serviço para o AWS Marketplace para obter mais detalhes.

Para obter informações sobre outros serviços compatíveis com funções vinculadas aos serviços, consulte Serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Funções vinculadas aos serviços. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculada ao serviço AWS Marketplace

O AWS Marketplace usa a função vinculada ao serviço chamada AWSServiceRoleForMarketplaceLicenseManagement. Essa função fornece ao AWS Marketplace

permissões para criar e gerenciar licenças no AWS License Manager para os produtos que você assina no AWS Marketplace.

A função vinculada ao serviço AWSServiceRoleForMarketplaceLicenseManagement confia no seguinte serviço para realizar ações no Gerenciador de licença em seu nome:

- `license-management.marketplace.amazonaws.com`

A política de permissões de perfil chamada AWSMarketplaceLicenseManagementServiceRolePolicy permite que o AWS Marketplace conclua as seguintes ações nos recursos especificados:

- Ações:
  - `"organizations:DescribeOrganization"`
  - `"license-manager:ListReceivedGrants"`
  - `"license-manager:ListDistributedGrants"`
  - `"license-manager:GetGrant"`
  - `"license-manager:CreateGrant"`
  - `"license-manager:CreateGrantVersion"`
  - `"license-manager:DeleteGrant"`
  - `"license-manager:AcceptGrant"`
- Recursos:
  - Todos os recursos (`"*"`)

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou perfil) crie, edite ou exclua um perfil vinculado ao serviço. Para ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Crie uma função vinculada ao serviço para o AWS Marketplace

O AWS Marketplace cria uma função vinculada ao serviço quando você configura a integração com o AWS License Manager.

Você pode especificar que o AWS Marketplace crie a função vinculada ao serviço para todas as contas em sua organização de uma vez, ou você pode criar a função vinculada ao serviço para uma conta por vez. A opção de criar funções vinculadas a serviços em todas as contas só estará

disponível se sua organização tiver a opção Todos os recursos habilitada. Para obter mais detalhes, consulte Habilitar todos os recursos na sua organização no Guia do usuário do AWS Organizations.

Para criar funções vinculadas a serviços em todas as contas

1. No console do AWS Marketplace, faça login e escolha Configurações.
2. Na seção Integração do AWS Organizations, selecione Criar integração.
3. Na página Criar integração do AWS Organizations, selecione Habilitar acesso confiável em toda a organização e escolha Criar integração.

> **Note**
>
> Essa configuração habilita a confiança no AWS Organizations. Como resultado, além da ação atual, contas futuras adicionadas à organização têm a função vinculada ao serviço adicionada automaticamente.

Para criar funções vinculadas a serviços para a conta atual

1. No console do AWS Marketplace, faça login e escolha Configurações.
2. Na seção Integração do AWS Organizations, selecione Configurar integração.
3. Na página Criar integração do AWS Organizations, selecione a Função vinculada ao serviço de gerenciamento de licenças do AWS Marketplace para essa conta e escolha Criar integração.

> **Important**
>
> Se você optar por criar a função vinculada ao serviço somente para a conta atual, ela não permitirá acesso confiável em toda a sua organização. Você deve repetir essas etapas para cada conta que deseja compartilhar (dar ou receber) licenças no AWS Marketplace. Isso inclui contas que são adicionadas à organização no futuro.

Editar uma função vinculada ao serviço para o AWS Marketplace

O AWS Marketplace não permite que você edite a função vinculada ao serviço. 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 uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Marketplace

Se você não precisar mais usar um atributo ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o serviço AWS Marketplace estiver usando a função quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API da AWS para excluir o perfil vinculado ao serviço AWSServiceRoleForMarketplaceLicenseManagement. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões suportadas por funções vinculadas ao serviço do AWS Marketplace

O AWS Marketplace oferece suporte a funções vinculadas a serviços em todas as Regiões da AWS onde o serviço estiver disponível. Para obter mais informações, consulte Regiões e endpoints da AWS Marketplace.

Uso de funções para trabalhar com ordens de compra no AWS Marketplace

O AWS Marketplace utiliza perfis vinculados a serviço do AWS Identity and Access Management (IAM). O perfil vinculado a serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao AWS Marketplace. Os perfis vinculados a serviços são predefinidos pelo AWS Marketplace e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração do AWS Marketplace porque você não precisa adicionar as permissões necessárias manualmente. AWS Marketplace define as permissões de suas funções vinculadas ao serviço e, a menos que definido de outra forma, somente AWS

Marketplace pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões. Essa política não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus recursos do AWS Marketplace, pois você não pode remover por engano as permissões de acesso aos recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas aos serviços, consulte serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Funções vinculadas aos serviços. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculada ao serviço AWS Marketplace

AWS Marketplaceusa a função vinculada ao serviço chamada AWSServiceRoleForMarketplacePurchaseOrders— essa função fornece AWS Marketplace permissões para anexar números de pedidos de compra às suas AWS Marketplace assinaturas em. AWS Billing and Cost Management

A função vinculada ao serviço AWSServiceRoleForMarketplacePurchaseOrders confia nos seguintes serviços para aceitar a função:

- `purchase-orders.marketplace.amazonaws.com`

A política de permissões de função nomeada AWSMarketplacePurchaseOrdersServiceRolePolicyAWS Marketplacepermite concluir as seguintes ações nos recursos especificados:

- Ação: `"purchase-orders:ViewPurchaseOrders", "purchase-orders:ModifyPurchaseOrders"` em `"*"`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado ao serviço. Para ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Crie uma função vinculada ao serviço para o AWS Marketplace

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você configura a integração com o AWS Billing and Cost Management, o AWS Marketplace cria uma função vinculada ao serviço.

> **Note**
>
> No AWS Organizations, essa configuração só funciona na conta de gerenciamento. Você deve executar esse procedimento na conta de gerenciamento. Isso configura a função vinculada ao serviço e o suporte a ordens de compra para todas as contas na organização.

Como criar um perfil vinculado ao serviço

1. No console do AWS Marketplace, entre na conta de gerenciamento e escolha Configurações.
2. Na seção Integração do AWS Billing, selecione Configurar integração.
3. Na página Criar integração do AWS Billing, selecione a Função vinculada ao serviço de gerenciamento de faturamento do AWS Marketplace para sua organização e escolha Criar integração.

Se você excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, poderá usar esse mesmo processo para recriar o perfil na sua conta. Quando você configura a integração com o AWS Billing and Cost Management, o AWS Marketplace cria uma função vinculada ao serviço novamente.

Editar uma função vinculada ao serviço para o AWS Marketplace

O AWS Marketplace não permite que você edite a função vinculada ao serviço AWSServiceRoleForMarketplacePurchaseOrders. 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 da função usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Marketplace

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja

monitorada ativamente ou mantida. No entanto, você deve limpar suo perfil vinculado ao serviço para excluí-la manualmente.

Exclusão manual da função vinculada ao serviço

Use o console do IAM, a AWS CLI ou a API da AWS para excluir o perfil vinculado ao serviço AWSServiceRoleForMarketplacePurchaseOrders. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas por funções vinculadas ao serviço do AWS Marketplace

O AWS Marketplace oferece suporte a funções vinculadas a serviços em todas as Regiões da AWS onde o serviço estiver disponível. Para obter mais informações, consulte Regiões e endpoints da AWS Marketplace.

Usar funções para configurar e lançar produtos no AWS Marketplace

O AWS Marketplace utiliza perfis vinculados a serviço do AWS Identity and Access Management (IAM). O perfil vinculado a serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao AWS Marketplace. Os perfis vinculados a serviços são predefinidos pelo AWS Marketplace e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração do AWS Marketplace porque você não precisa adicionar as permissões necessárias manualmente. AWS Marketplace define as permissões de suas funções vinculadas ao serviço e, a menos que definido de outra forma, somente AWS Marketplace pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões. Essa política não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros produtos que oferecem suporte às funções vinculadas a serviços, consulte Serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Yes (Sim) na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculada ao serviço AWS Marketplace

O AWS Marketplace usa a função vinculada ao serviço chamada AWSServiceRoleForMarketplaceDeployment para permitir que o AWS Marketplace gerencie parâmetros relacionados à implantação, que são armazenados como segredos em AWS Secrets Manager, em seu nome. Esses segredos podem ser referenciados pelos vendedores em modelos

do AWS CloudFormation, que você pode iniciar ao configurar produtos que tenham o início rápido ativado no AWS Marketplace.

A função vinculada ao serviço AWSServiceRoleForMarketplaceDeployment confia nos seguintes serviços para assumir a função:

- `deployment.marketplace.amazonaws.com`

Use a política de permissões de função chamada AWSMarketplaceDeploymentServiceRolePolicy para permitir que o AWS Marketplace conclua ações em seus recursos.

> **Note**
>
> Para obter mais informações sobre políticas gerenciadas do AWS Marketplace, consulte Políticas gerenciadas pela AWS para compradores do AWS Marketplace.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ManageMarketplaceDeploymentSecrets",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:CreateSecret",
    "secretsmanager:PutSecretValue",
    "secretsmanager:DescribeSecret",
    "secretsmanager:DeleteSecret",
    "secretsmanager:RemoveRegionsFromReplication"
   ],
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "ListSecrets",
```

```
    "Effect": "Allow",
    "Action": [
     "secretsmanager:ListSecrets"
    ],
    "Resource": [
     "*"
    ]
   },
   {
    "Sid": "TagMarketplaceDeploymentSecrets",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:TagResource"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
    "Condition": {
     "Null": {
      "aws:RequestTag/expirationDate": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": [
       "expirationDate"
      ]
     },
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   }
  ]
}
```

Você deve configurar permissões para permitir que seus usuários, grupos ou perfis criem, editem ou excluam um perfil vinculado ao serviço. Para ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Crie uma função vinculada ao serviço para o AWS Marketplace

A configuração da função vinculada ao serviço é uma ação única que fornece permissões para todos os produtos que têm o início rápido ativado, desde que a função exista.

Ao configurar um produto com o início rápido ativado, o AWS Marketplace detectará se você tem a função vinculada ao serviço necessária criada para sua conta. Se a função estiver faltando, será

exibido um prompt para ativar a integração dos parâmetros de implantação do AWS Marketplace, que inclui um botão Habilitar integração. O AWS Marketplace cria a função vinculada ao serviço para você ao selecionar esse botão.

> **Important**
>
> Essa função vinculada ao serviço aparecerá na sua conta se você tiver configurado anteriormente um produto com o início rápido ativado. Para obter mais informações, consulte Um novo perfil apareceu em minha Conta da AWS.

Se você excluir essa função vinculada ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar a função em sua conta. Ao abrir a página Configuração de qualquer produto que tenha o início rápido habilitado, você verá o botão Habilitar integração, que pode ser escolhido novamente para recriar a função vinculada ao serviço.

Você também pode usar o console do IAM para criar uma função vinculada ao serviço com o caso de uso AWS Marketplace: gerenciamento de implantações. Na AWS CLI ou na API do AWS, crie um perfil vinculado a serviço com o nome de serviço `deployment.marketplace.amazonaws.com`. Para obter mais informações, consulte Criar um perfil vinculado a serviço no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Editar uma função vinculada ao serviço para o AWS Marketplace

O AWS Marketplace não permite que você edite a função vinculada ao serviço. 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 uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Marketplace

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o serviço estiver usando um perfil quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir recursos do AWS Marketplace usados pelo serviço `deployment.marketplace.amazonaws.com`, você deve excluir todos os segredos relacionados à implantação do marketplace do SecretsManager. Você pode encontrar os segredos relevantes:

- Como procurar segredos gerenciados pelo `marketplace-deployment`.
- Como procurar segredos com a chave `aws:secretsmanager:owningService` e o valor `marketplace-deployment`.
- Como procurar segredos em que o nome secreto é prefixado com `marketplace-deployment!`.

Excluir o perfil vinculado a serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API da AWS para excluir o perfil vinculado ao serviço AWSServiceRoleForMarketplaceDeployment. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões suportadas por funções vinculadas ao serviço do AWS Marketplace

O AWS Marketplace oferece suporte a funções vinculadas a serviços em todas as regiões nas quais o serviço estiver disponível. Para obter mais informações, consulte Endpoints e cotas de AWS Marketplace.

Usando funções para configurar o Private Marketplace em AWS Marketplace

O AWS Marketplace utiliza perfis vinculados a serviço do AWS Identity and Access Management (IAM). O perfil vinculado a serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao AWS Marketplace. Os perfis vinculados a serviços são predefinidos pelo AWS Marketplace e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração do AWS Marketplace porque você não precisa adicionar as permissões necessárias manualmente. AWS Marketplace define as permissões de suas funções vinculadas ao serviço e, a menos que definido de outra forma, somente AWS

Marketplace pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões. Essa política não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros produtos que oferecem suporte às funções vinculadas a serviços, consulte Serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Yes (Sim) na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculada ao serviço AWS Marketplace

AWS Marketplaceusa a função vinculada ao serviço nomeada AWSServiceRoleForPrivateMarketplaceAdminpara descrever e atualizar os recursos do Private Marketplace e descrever. AWS Organizations

A função vinculada ao serviço AWSServiceRoleForPrivateMarketplaceAdmin confia nos seguintes serviços para aceitar a função:

- `private-marketplace.marketplace.amazonaws.com`

Use a política de permissões de função nomeada AWSServiceRoleForPrivateMarketplaceAdminPolicyAWS Marketplacepara permitir a execução das seguintes ações em recursos especificados.

> **Note**
>
> Para obter mais informações sobre as políticas gerenciadas do AWS Marketplace, consulte Políticas gerenciadas da AWS para AWS Marketplace compradores.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrivateMarketplaceCatalogDescribePermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeEntity"
            ],
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
```

```
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
            ]
        },
        {
            "Sid": "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PrivateMarketplaceCatalogListPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListEntities",
                "aws-marketplace:ListChangeSets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PrivateMarketplaceStartChangeSetPermissions",
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:StartChangeSet"
            ],
            "Condition": {
                "StringEquals": {
                    "catalog:ChangeType": [
                        "AssociateAudience",
                        "DisassociateAudience"
                    ]
                }
            },
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
            ]
        },
        {
            "Sid": "PrivateMarketplaceOrganizationPermissions",
            "Effect": "Allow",
```

```
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListChildren"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Você deve configurar permissões para permitir que seus usuários, grupos ou perfis criem, editem ou excluam um perfil vinculado ao serviço. Para ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Crie uma função vinculada ao serviço para o AWS Marketplace

Você não precisa criar manualmente o perfil vinculado ao serviço. Quando você ativa o Private Marketplace para sua organização, AWS Marketplace cria a função vinculada ao serviço para você.

> **Note**
>
> Essa função é necessária somente na conta de gerenciamento AWS Organizations e é criada somente na conta de gerenciamento.

Como criar um perfil vinculado ao serviço

1. Na página Introdução ao Private Marketplace, selecione as opções para habilitar o acesso confiável em toda a sua organização e criar uma função vinculada ao serviço do Private Marketplace. Essas opções estão disponíveis somente para a conta de gerenciamento.
2. Escolha Habilitar Private Marketplace.

Se você já é cliente do Private Marketplace, as opções para habilitar o acesso confiável em toda a sua organização e habilitar uma função vinculada ao serviço do Private Marketplace estarão disponíveis na página Configurações do painel administrativo do seu marketplace privado.

Se você excluir essa função vinculada ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar a função em sua conta.

Editar uma função vinculada ao serviço para o AWS Marketplace

O AWS Marketplace não permite que você edite a função vinculada ao serviço. Depois de criar uma função vinculada a serviço, você não poderá alterar o nome da função, já que várias entidades poderão fazer referência à função. No entanto, você poderá editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Marketplace

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

Antes de excluir a função vinculada ao serviço, você deve:

- Desative o acesso confiável em toda a sua organização.
- Desassocie todas as experiências de mercado privado.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API da AWS para excluir a função vinculada ao serviço AWSServiceRoleForPrivateMarketplaceAdmin. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões suportadas por funções vinculadas ao serviço do AWS Marketplace

O AWS Marketplace oferece suporte a funções vinculadas a serviços em todas as regiões nas quais o serviço estiver disponível. Para obter mais informações, consulte Endpoints e cotas de AWS Marketplace.

Criação de um administrador do mercado privado

Você pode criar um grupo de administradores para gerenciar as configurações do mercado privado de sua empresa. Depois que o mercado privado estiver habilitado para sua organização, os administradores do mercado privado poderão realizar várias tarefas, incluindo as seguintes:

- Visualize e crie experiências e públicos.
- Adicionar produtos às experiências do mercado privado.
- Remover produtos das experiências de mercado privado.
- Configurar a interface do usuário de experiências de mercado privado.
- Habilitar e desabilitar experiências de mercado privado.
- Chame o AWS Marketplace Catalog API para o para gerenciar experiências de mercado privado de forma programática.

Para criar vários administradores de mercados privados em que cada administrador está limitado a um subconjunto de tarefas, consulte the section called “Criação de políticas personalizadas para administradores de mercados privados”.

> **Note**
>
> Habilitar o mercado privado é uma ação única que deve ocorrer a partir da conta de gerenciamento. Para obter mais informações, consulte Introdução ao mercado privado.

Conceda permissões do AWS Identity and Access Management (IAM) para administrar seu mercado privado anexando the section called “AWSPrivateMarketplaceAdminFullAccess” a um usuário, grupo ou função. Recomendamos o uso de um grupo ou função. Para obter mais informações sobre como anexar a política, consulte Como anexar uma política a um grupo de usuários no Guia do usuário do IAM.

Para obter mais informações sobre as permissões na política `AWSPrivateMarketplaceAdminFullAccess`, consulte the section called “AWSPrivateMarketplaceAdminFullAccess”. Para saber mais sobre outras políticas para uso no AWS Marketplace, faça login no AWS Management Console e acesse a página de políticas do IAM. Na caixa de pesquisa, digite **`Marketplace`** para encontrar todas as políticas associadas ao AWS Marketplace.

Criação de políticas personalizadas para administradores de mercados privados

Sua organização pode criar vários administradores de mercados privados, onde cada administrador está limitado a um subconjunto de tarefas. Você pode ajustar as políticas do AWS Identity and

Access Management (IAM) para especificar chaves de condição e recursos nas ações do AWS Marketplace Catalog API listadas em Ações, recursos e chaves de condição do catálogo do AWS Marketplace. O mecanismo geral para usar tipos de AWS Marketplace Catalog API alteração e recursos para ajustar as políticas do IAM está descrito no guia da API do AWS Marketplace Catalog. Para obter uma lista de todos os tipos de alteração disponíveis no AWS Marketplace privado, consulte Como trabalhar com um mercado privado.

Para criar políticas gerenciadas pelo cliente, consulte Criação de políticas do IAM. Veja a seguir um exemplo de política JSON que você pode usar para criar um administrador que só pode adicionar ou remover produtos de mercados privados.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:ListEntities",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:StartChangeSet"
            ],
```

```
            "Condition": {
                "StringEquals": {
                    "catalog:ChangeType": [
                        "AllowProductProcurement",
                        "DenyProductProcurement"
                    ]
                }
            },
            "Resource": "*"
        }
    ]
}
```

Uma política também pode ser limitada para gerenciar um subconjunto de recursos do mercado privado. Veja a seguir um exemplo de política JSON que você pode usar para criar um administrador que só pode gerenciar uma experiência específica de mercado privado. Este exemplo usa uma string de recurso com `exp-1234example` como identificador `Experience`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:AssociateProductsWithPrivateMarketplace",
                "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:ListEntities",
                "aws-marketplace:DescribeEntity",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:StartChangeSet"
            ],
            "Resource": [
                "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/exp-1234example"
            ]
        }
    ]
}
```

Para obter detalhes sobre como os identificadores de entidade podem ser recuperados e para visualizar o conjunto de recursos do mercado privado, consulte Como trabalhar com um mercado privado.

Histórico do documento

A tabela a seguir descreve a documentação dessa versão do Guia do comprador do AWS Marketplace.

Para receber notificações sobre atualizações dessa documentação, você pode se inscrever em o feed RSS.

Alteração	Descrição	Data
Política atualizada de AWS Organizations suporte	Política gerenciada atualizada a `AWSPrivateMarketplaceAdminFullAccess` para permitir o acesso à leitura AWS Organizations de dados.	16 de fevereiro de 2024
Nova função vinculada a serviços para produtos no AWS Marketplace	AWS Marketplaceagora fornece uma função vinculada ao serviço para descrever e atualizar os recursos e descrever o Private Marketplace. AWS Organizations	16 de fevereiro de 2024
Nova experiência de mercado privado em AWS Marketplace	AWS Marketplaceagora oferece suporte à integração AWS Organizations e à capacidade de registrar administradores delegados para administrar experiências de mercado privado.	16 de fevereiro de 2024
Disponibilidade geral para contratos com data futura no AWS Marketplace	A funcionalidade de contratos com data futura para todos os ISVs SaaS e parceiros de canal agora está disponível no AWS Marketplace. Usando contratos com data futura,	16 de janeiro de 2024

	os clientes podem reservar negócios antecipadamente ou configurar renovações quando tiverem compras existentes na mesma lista de produtos com menor esforço operacional.	
Suporte para a região Oeste do Canadá (Calgary)	O AWS Marketplace agora atende à seguinte Região da AWS: Oeste do Canadá Oeste (Calgary).	20 de dezembro de 2023
Nova função vinculada a serviços para produtos no AWS Marketplace	O AWS Marketplace agora fornece uma função vinculada ao serviço para gerenciar parâmetros relacionados à implantação, que são armazenados como segredos no AWS Secrets Manager, em nome dos compradores.	29 de novembro de 2023
Nova opção de implantação de início rápido para compradores	Os compradores agora podem reduzir o tempo, os recursos e as etapas necessárias para configurar, implantar e lançar produtos de software como serviço (SaaS) aplicáveis no AWS Marketplace.	29 de novembro de 2023
Cronogramas de pagamento flexíveis estão disponíveis para ofertas privadas	Cronogramas de pagamento flexíveis (FPS) para ofertas privadas agora estão disponíveis para todos os clientes no AWS Marketplace.	17 de novembro de 2023

Complementos de terceiros do Amazon EKS	Agora, os clientes podem assinar complementos de terceiros no console do Amazon EKS sem serem redirecionados para o AWS Marketplace.	18 de outubro de 2023
Support para Amazon EventBridge	AWS Marketplaceagora está integrado com a Amazon EventBridge, anteriorm ente chamada de Amazon CloudWatch Events.	6 de setembro de 2023
Suporte para a região de Israel (Tel Aviv)	O AWS Marketplace agora é compatível com a seguinte Região da AWS: Israel (Tel Aviv).	1º de agosto de 2023
Suporte a pedidos de compra para contratos anuais da AMI	O AWS Marketplace agora é compatível com a funcional idade de pedido de compra para contratos anuais da imagem de máquina da Amazon (AMI).	29 de junho de 2023
Disponibilidade do pedido de compra no console do AWS Billing	Agora, os compradores podem gerenciar todos os pedidos de compra no AWS Billing console e reconciliar facilment e as faturas em PDF do contrato de out-of-cycle SaaS com os pedidos de compra correspondentes.	3 de fevereiro de 2023

Suporte para a região Ásia-Pacífico (Melbourne)	O AWS Marketplace agora é compatível com a seguinte Região da AWS: Ásia-Pacífico (Melbourne).	24 de janeiro de 2023
Políticas atualizadas para a página Ofertas privadas	Atualização das políticas gerenciadas `AWSMarketplaceRead-only` e `AWSMarketplaceManageSubscriptions` para permitir o acesso à página Ofertas privadas.	19 de janeiro de 2023
Página de ofertas privadas	Os compradores autenticados agora podem ver as ofertas privadas do AWS Marketplace estendidas para a Conta da AWS deles na página Ofertas privadas.	19 de janeiro de 2023
Atualização das notificações por e-mail para compradores	Agora, os compradores são notificados quando uma oferta privada é publicada.	22 de dezembro de 2022
As avaliações gratuitas de SaaS para assinaturas agora estão disponíveis para compradores no AWS Marketplace	Agora, os compradores podem assinar avaliações gratuitas de produtos SaaS por assinatura.	16 de dezembro de 2022
Os compradores podem aceitar um upgrade ou renovação de uma oferta privada de SaaS	Se um vendedor tiver atualizado ou renovado uma oferta privada anterior de SaaS, os compradores poderão aceitar uma nova oferta privada sem precisar cancelar o contrato existente.	13 de dezembro de 2022

O AWS Marketplace suporta o arquivamento de experiências de mercado privado	Agora, os compradores podem arquivar e reativar experiências de mercado privado no AWS Marketplace.	12 de dezembro de 2022
Atualização da política para o recurso de autorização baseada em tags do AWS Marketplace	Atualização da política `AWSPrivateMarketplaceAdminFullAccess` para oferecer suporte à autorização baseada em tags no AWS Marketplace.	9 de dezembro de 2022
Adição de novo tópico com informações sobre como cancelar sua assinatura	Adição de informações sobre como cancelar sua assinatura de produtos AMI, ML e SaaS no AWS Marketplace. Além disso, foram adicionadas informações sobre o cancelamento da renovação automática de um contrato SaaS.	08 de dezembro de 2022
Atualização do políticas para compradores no AWS Marketplace Vendor Insights	Atualização de políticas gerenciadas `AWSVendorInsightsAssessorFullAccess` e `AWSVendorInsightsAssessorReadOnly` para compradores do AWS Marketplace Vendor Insights.	30 de novembro de 2022
Controle do acesso dos compradores no AWS Marketplace Vendor Insights	Adição de um novo tópico no AWS Marketplace Vendor Insights para descrever as ações e permissões disponíveis para os compradores.	30 de novembro de 2022

Suporte para a região Ásia-Pacífico (Hyderabad)	O AWS Marketplace agora é compatível com a seguinte Região da AWS: Ásia-Pacífico (Hyderabad).	22 de novembro de 2022
Suporte para a região Europa (Espanha)	O AWS Marketplace agora é compatível com a seguinte Região da AWS: Europa (Espanha).	16 de novembro de 2022
Suporte para Europa (Zurique)	O AWS Marketplace agora é compatível com a seguinte Região da AWS: Europa (Zurique).	9 de novembro de 2022
Atualização do site do AWS Marketplace para IPv6 até dezembro de 2022	Os compradores que atualmente usam o endereço no formato IPv4 nas políticas do IAM são aconselhados a atualizar as políticas do IAM para endereços no formato IPv6 antes de 15 de dezembro de 2022.	29 de setembro de 2022
Permissões granulares do mercado privado do AWS Marketplace	Agora, os compradores têm permissões mais granulares para gerenciar experiências de mercado privado.	8 de setembro de 2022

Adição de duas políticas para o AWS Marketplace Vendor Insights.	Adição de duas políticas, `AWSVendorInsightsAssessorFullAccess` e `AWSVendorInsightsAssessorReadOnly` , para o AWS Marketplace Vendor Insights, um recurso que oferece avaliação de risco de software	26 de julho de 2022
AWS Marketplace Vendor Insights	AWS Marketplace Vendor Insights é um recurso que oferece avaliação de risco de software.	26 de julho de 2022
Atualização dos métodos de pagamento	Atualização somente da documentação para esclarecer como alterar as formas de pagamento no console de faturamento da AWS.	1º de junho de 2022
Avaliações gratuitas de SaaS para contratos	Agora, os compradores podem assinar avaliações gratuitas de SaaS para contratos para explorar produtos antes de fazer a transição para avaliações pagas.	31 de maio de 2022
Adição de tags de medição de fornecedores para produtos de AMI, contêiner e SaaS	Novo recurso que fornece tags para ajudar os clientes a entender o uso de recursos do AWS Marketplace em todas as métricas fornecidas pelo fornecedor.	27 de maio de 2022

Adição de notificações por e-mail às transações do comprador	Novo recurso que permite enviar notificações por e-mail ao comprador, verificando os acordos feitos no AWS Marketplace.	23 de maio de 2022
Aprovação automática de produtos gratuitos/BYOL para clientes de eProcurement habilitada	Os clientes podem usar os produtos imediatamente com a nova aprovação automática de produtos gratuitos/BYOL para clientes de eProcurement.	2 de maio de 2022
Modificações de contrato habilitadas para compradores em contratos de produtos de AMI e contêiner	Os contratos de produtos de AMI e contêiner podem ser modificados para comprar direitos adicionais ou habilitar a opção de renovação automática da assinatura.	6 de abril de 2022
Capacidade de rastrear o uso da licença	Agora, os compradores podem monitorar métricas de licença baseadas no uso de produtos de AMI e SaaS com o AWS License Manager.	28 de março de 2022
Atualizações para a versão da CLI do Helm	Atualização do documentação dos produtos de contêiner sobre a alteração da versão da CLI do Helm de 3.7.0 para 3.7.1. Essa é a única versão compatível no momento.	8 de março de 2022

Atualizações nas políticas gerenciadas existentes	As permissões que não eram mais necessárias foram removidas das seguintes políticas: `AWSMarketplaceFullAccess` e `AWSMarketplaceImageBuildFullAccess`.	4 de março de 2022
Capacidade de compradores baseados na EMEA comprarem produtos por meio da Amazon Web Services EMEA SARL	Os compradores do AWS Marketplace com Contas da AWS em países e territórios da Europa, Oriente Médio e África (EMEA), exceto Turquia e África do Sul, agora podem receber faturas do AWS Marketplace por meio da Amazon Web Services EMEA SARL para compras de vendedores qualificados para EMEA.	7 de janeiro de 2022
Suporte para a região Ásia-Pacífico (Jacarta)	O AWS Marketplace agora é compatível com a seguinte Região da AWS: Ásia-Pacífico (Jacarta).	13 de dezembro de 2021
Método de entrega Chart do Helm para produtos à base de contêiner	Agora, os compradores podem lançar produtos baseados em contêiner instalando um chart do Helm nos ambientes de execução.	29 de novembro de 2021

Atualizações gerais e reorganização da documentação do produto baseado em contêiner	Atualização da documentação do produto baseado em contêiner para adicionar mais informações e clareza sobre como encontrar, assinar e executar produtos baseados em contêiner.	29 de novembro de 2021
Documentação adicionada para QuickLaunch	Agora, os compradores podem usá-lo QuickLaunch ao lançar produtos baseados em contêineres com um método de entrega Helm Chart. QuickLaunch é um recurso AWS Marketplace que permite AWS CloudFormation criar rapidamente um novo cluster Amazon EKS e lançar um aplicativo baseado em contêiner nele.	29 de novembro de 2021
Preços contratuais para produtos baseados em AMI e produtos baseados em contêiner	Agora, os compradores podem comprar um produto baseado em AMI ou um produto baseado em contêiner com preços iniciais.	17 de novembro de 2021
Suporte para pedidos de compra em produtos de SaaS	O AWS Marketplace permite a adição de números de pedidos de compra às compras de contratos de software como serviço (SaaS).	28 de outubro de 2021
Suporte para integração com SAP Ariba	O AWS Marketplace permite a integração ao sistema de aquisições SAP Ariba.	13 de outubro de 2021

Suporte para aliases de AMI	O AWS Marketplace permite o uso de aliases para IDs de AMI que podem ser usados em várias regiões.	8 de setembro de 2021
Remoção de permissões não utilizadas na política gerenciada	As permissões não utilizadas da política gerenciada `AWSPrivateMarketplaceAdminFullAccess` AWS foram removidas.	27 de agosto de 2021
Suporte para compartilhamento de licenças por meio do AWS License Manager	Você pode compartilhar licenças de produtos comprados com outras contas em sua organização da AWS.	3 de dezembro de 2020
O AWS Marketplace dá suporte a ofertas de serviços profissionais	O AWS Marketplace agora permite a compra de serviços profissionais.	3 de dezembro de 2020
Suporte para moeda preferencial	Você pode pagar pelas compras do AWS Marketplace usando sua moeda preferida.	27 de julho de 2020
É possível revisar e aceitar atualizações e renovações de ofertas privadas	Os vendedores podem fornecer ofertas privadas de atualização e renovação para um contrato de SaaS e um contrato de SaaS com produtos de consumo que você pode revisar e aceitar enquanto um acordo existente estiver em vigor.	28 de maio de 2020
O AWS Marketplace oferece suporte a produtos de dados por meio do AWS Data Exchange	Agora você pode assinar produtos de dados do AWS Data Exchange no AWS Marketplace.	13 de novembro de 2019

O AWS Marketplace oferece suporte a contêineres pagos por hora	O AWS Marketplace agora é compatível com contêineres pagos por hora em execução no Amazon Elastic Kubernetes Service (Amazon EKS).	25 de setembro de 2019
Ofertas privadas atualizadas no AWS Marketplace	Conteúdo atualizado para fornecer mais informações sobre aceitar diferentes tipos de oferta privada.	29 de março de 2019
Segurança atualizada no AWS Marketplace	Atualização de informações de políticas do IAM. A seção foi reestruturada para legibilidade.	25 de março de 2019
Adição de conteúdo ao recurso de loja privada	Adicionado conteúdo com suporte para a versão do Private Marketplace.	27 de novembro de 2018
Versão inicial do guia do usuário para compradores	Versão inicial do Guia do comprador do AWS Marketplace.	16 de novembro de 2018

AWS Glossário

Para obter a AWS terminologia mais recente, consulte o AWS glossário na Glossário da AWS Referência.

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.