AWS Marketplace

Buyer Guide

AWS Marketplace: Buyer Guide

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

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is AWS Marketplace?

AWS Marketplace is a curated digital catalog that you can use to find, buy, deploy, and manage third-party software, data, and services that you need to build solutions and run your businesses. AWS Marketplace includes thousands of software listings from popular categories such as security, networking, storage, machine learning, IoT, business intelligence, database, and DevOps. AWS Marketplace also simplifies software licensing and procurement with flexible pricing options and multiple deployment methods. In addition, AWS Marketplace includes data products available from AWS Data Exchange.

You can quickly launch pre-configured software with just a few clicks, and choose software solutions in Amazon Machine Images (AMIs) and software as a service (SaaS) formats, as well as other formats. Additionally, you can browse and subscribe to data products. Flexible pricing options include free trial, hourly, monthly, annual, multi-year, and a Bring Your Own License (BYOL) model. All of these pricing options are billed from one source. AWS handles billing and payments, and charges appear on your AWS bill.

You can use AWS Marketplace as a buyer (subscriber) or as a seller (provider), or both. Anyone with an AWS account can use AWS Marketplace as a consumer and can register to become a seller. A seller can be an independent software vendor (ISV), value-added reseller, or individual that has something to offer that works with AWS products and services.

> **Note**
> Data product providers need to meet the AWS Data Exchange eligibility requirements. For more information, see Providing Data Products on AWS Data Exchange in the *AWS Data Exchange User Guide*.

Every software product in AWS Marketplace has been through a curation process. On the product page, there can be one or more offerings for the product. When the seller submits a product in AWS Marketplace, they define the price of the product, and the terms and conditions of use. Buyers agree to the pricing, and terms and conditions set for the offer.

The product can be free to use or can have an associated charge. The charge becomes part of your AWS bill, and after you pay, AWS Marketplace pays the seller.

> **Note**
> When buying from some non-US sellers, you may also receive a tax invoice from the seller. For more information, see AWS Marketplace Sellers on Amazon Web Service Tax Help.

Products can take many forms. For instance, a product can be offered as an Amazon Machine Image (AMI) that is instantiated using your AWS account. The product could also be configured to use AWS CloudFormation templates for delivery to the consumer. The product could also be software as a service (SaaS) offerings from an ISV, or a web ACL, set of rules, or conditions for AWS WAF.

You can purchase software products at the listed price using the ISV's standard end user license agreement (EULA) or from a private offer with custom pricing and EULA. You can also purchase products under a contract with specified time or usage boundaries. Once the product subscriptions are in place, you can copy the product to your AWS Service Catalog to manage how the product is accessed and used in your organization.

Using AWS Marketplace as a buyer

As a buyer, you go to AWS Marketplace to search, filter, and navigate to a product that runs on Amazon Web Services. You can also find AWS Marketplace products on Deloitte and DLT.

When you choose a software product, you are taken to the product's page. The page has information about the product, pricing, usage, support, and product reviews. To subscribe to the software product, you log in to your AWS account and are taken to a subscription page that has the EULA, terms and conditions of usage, and any options available for customizing your subscription.

Tip
Note the following tips about license terms and contracts:

- Many sellers offer the same standardized license terms on their listings, the *Standard Contract for AWS Marketplace (SCMP)*. Instead of reviewing custom EULAs for each purchase, you only need to review the SCMP once. The license terms are the same for all products that use the SCMP. To find product listings that offer standardized license terms, use the **Standard Contract** filter when searching for products.
- The *Enterprise Contract for AWS Marketplace (ECMP)* offers standardized license terms that address the unique requirements of large enterprise and regulated buyers.

To learn more, see Standardized License Terms.

After the subscription is processed, you can configure fulfillment options, software versions, and AWS Regions where you want to use the product, and then launch the software product. You can also find or launch your products by visiting Your Marketplace Software on the AWS Marketplace website, from your AWS Marketplace or Amazon Elastic Compute Cloud (Amazon EC2) console, or through AWS Service Catalog. For more information about products and product categories available using AWS Marketplace, see the following:

- Product categories (p. 10)
- Container products (p. 17)
- Desktop products (p. 19)
- Machine learning products (p. 19)
- Professional services products (p. 20)
- SaaS products (p. 21)
- AMI-based server products (p. 22)
- What is AWS Data Exchange? in the *AWS Data Exchange User Guide*

Getting started

The following topics outline the process of getting started with software products as an AWS Marketplace buyer.

Topics

For information about getting started with data products, see Subscribing to data products on AWS Data Exchange in the *AWS Data Exchange User Guide*.

The following tutorial describes the complete process of getting started with AWS Marketplace, using an Amazon Machine Image (AMI) product as an example.

Step 1: Choose your software

AWS Marketplace includes the following categories of software:

- Infrastructure software
- Developer tools
- Business software
- Machine learning
- IoT
- Professional services
- Desktop Applications
- Data products

For more information, see Product categories (p. 10).

Each major software category contains more specific subcategories. For example, the Infrastructure software category contains subcategories such as Application Development, Databases & Caching, and Operating Systems. Software is available as one of seven different product types, including Amazon Machine Images (AMIs) and software as a service (SaaS). For information about the different software types, see *Product types* (p. 15).

To aid you in choosing the software you need, AWS Marketplace provides the following information:

- Seller details
- Software version
- Type of software (AMI or SaaS), and information about the AMI if applicable
- Buyer rating
- Price
- Product information

To choose your software

1. Navigate to the AWS Marketplace website.

   Note
   You can shop, subscribe, and launch new instances from either the public AWS Marketplace website, at https://aws.amazon.com/marketplace, or through the AWS Marketplace in the AWS console, at https://console.aws.amazon.com/marketplace/home#/subscriptions.
   You can shop on the website without being signed in to your AWS account, but you must sign in to subscribe or launch products. You must be signed in to your account to view the AWS Marketplace console.
   The experiences across the two sites are similar. This procedure uses the AWS Marketplace website but notes any major differences when using the console.
2. The **Shop All Categories** pane contains the list of categories you can choose from. You can also choose software featured in the middle pane. For this tutorial, in the **Shop All Categories** pane, choose **Content Management**.
3. From the **Content Management** list, choose **WordPress Certified by Bitnami and Automattic**.
4. On the product details page, review the product information. The product details page includes additional information such as:
   - Buyer rating
   - Support offering
   - Highlights
   - Detailed product description
   - Pricing details for instance types in each AWS Region (for AMIs)
   - Additional resources to help you get started
5. Choose **Continue to Subscribe**.
6. If you aren't already signed in, you are directed to sign in to AWS Marketplace. If you already have an AWS account, you can use that account to sign in. If you don't already have an AWS account, use the following steps to create one:
   a. From the **Sign In or Create an Account** page, choose **Create a New Account**.
   b. Follow the on-screen instructions. As part of the sign-in procedure, you will receive a phone call and you must enter a PIN using your phone keypad.

      Note
      When you create an account, AWS automatically signs up the account for all AWS services. You are charged only for the services you use.
7. Read the Bitnami offer terms, then choose **Accept Terms** to agree to the subscription offer.
8. It may take a moment for the subscription action to complete. When it does, you receive an email message about the subscription terms, and then you're able to continue. Choose **Continue to Configuration** to configure and launch your software.

Subscribing to a product means that you have accepted the terms of the product. If the product has a monthly fee, then upon subscription you will be charged the fee, which will be prorated based on the

time remaining in the month. No other charges will be assessed until you launch an Amazon Elastic Compute Cloud (Amazon EC2) instance with the AMI you chose.

Note
As a subscriber to a product, your account will receive email messages when a new version of the software you're subscribed to is published.

Step 2: Select your software configuration

Because we chose software as an AMI, your next step is to configure the software, including selecting the delivery method, version, and AWS Region in which you want to use the software.

To configure your software

1. On the **Configure this software** page, select **64-bit (x86) Amazon Machine Image (AMI)** for the **Delivery Method**.
2. Choose the latest version available for **Software Version**.
3. Choose the **Region** you want to launch the product in, for example, **US East (N. Virginia)**.

   Note
   As you make changes to your configuration, you might notice that the **Ami Id** at the bottom of the screen updates. The AMI ID has the form *ami-<identifier>*, for example, `ami-123example456`. Each version of each product in each Region has a different AMI. This AMI ID allows you to specify the correct AMI to use when launching the product. The **Ami Alias** is a similar ID that is easier to use in automation.
   For more information about the AMI alias, see Using AMI aliases (p. 32).
4. Select **Continue to Launch**.

Step 3: Launch your software on Amazon EC2

Before you launch your Amazon EC2 instance, you need to decide if you want to launch with 1-Click launch or if you want to launch using the Amazon EC2 Console. 1-Click launch helps you launch quickly with recommended default options such as security groups and instance types. With 1-Click launch, you can also see your estimated monthly bill. If you prefer more options, such as launching in an Amazon Virtual Private Cloud (Amazon VPC) or using Spot Instances, then you should launch using the Amazon EC2 Console. The following procedures walk you through subscribing to the product and launching an EC2 instance using either 1-Click launch or the Amazon EC2 Console.

To launch on Amazon EC2 using 1-Click launch

1. On the **Launch this software** page, choose **Launch from website** in the **Choose Action** dropdown, and review the default settings. If you want to change any of them, do the following:
   - In the **EC2 Instance Type** dropdown list, choose an instance type.
   - In the **VPC Settings** and **Subnet Settings** dropdown lists, select the network settings you want to use.
   - In the **Security Group Settings**, choose an existing security group, or choose **Create New Based On Seller Settings** to accept the default settings. For more information about security groups, see Amazon EC2 security groups for Linux instances in the *Amazon EC2 User Guide for Linux Instances*.
   - Expand **Key Pair**, and choose an existing key pair if you have one. If you don't have a key pair, you're prompted to create one. For more information about Amazon EC2 key pairs, see Amazon EC2 key pairs.

2. When you're satisfied with your settings, choose **Launch**.

   Your new instance is launched with the *WordPress Certified by Bitnami and Automattic* software running on it. From here, you can view the instance details, create another instance, or view all instances of your software.

To launch on Amazon EC2 Using Launch with EC2 Console

1. On the **Launch on EC2** page, choose the **Launch with EC2 Console** view, and then select an AMI version from the **Select a Version** list.
2. Review the **Firewall Settings**, **Installation Instructions**, and **Release Notes**, and then choose **Launch with EC2 Console**.
3. In the EC2 console, launch your AMI using the Request Instance Wizard. Follow the instructions in Get started with Amazon EC2 Linux instances to navigate through the wizard.

Step 4: Manage your software

At any time, you can manage your software subscriptions in AWS Marketplace by using the **Manage Subscriptions** page of the AWS Marketplace console. On the **Manage subscriptions** page, you can do the following:

- View your instance status by product
- View your current monthly charges
- Run a new instance
- View seller profiles for your instance
- Manage your instances
- Link directly to your Amazon EC2 instance so you can configure your software

To manage your software

1. Navigate to the AWS Marketplace console, and choose **Manage subscriptions**.
2. Use the **Manage subscriptions** page to manage your software subscriptions.

Step 5: Terminate your instance

When you've decided that you no longer need the instance, you can terminate it.

> **Note**
> You can't restart a terminated instance. However, you can launch additional instances of the same AMI.

To terminate an instance

1. Navigate to the AWS Marketplace console, and choose **Manage subscriptions**.
2. On the **Manage subscriptions** page, choose the software subscription that you want to terminate an instance of, and select **Manage**.

3. On the specific subscription page, choose **View instances** from the **Actions** dropdown list.
4. Select the **Region** that the instance you want to terminate is in. This opens the Amazon EC2 Console and shows the instances in that Region in a new tab. If necessary, you can return to this tab to see the Instance ID for the instance to close.
5. In the Amazon EC2 Console, choose the **Instance ID** to open the **Instance details page**.
6. From the **Instance state** dropdown list, choose **Terminate instance**.
7. Choose **Terminate** when prompted for confirmation. Termination takes a few minutes to complete.

For more information

For more information about product categories and types, see *Product categories* (p. 10) and *Product types* (p. 15).

For more information about Amazon EC2, see the service documentation at Amazon Elastic Compute Cloud Documentation.

To learn more about AWS, see https://aws.amazon.com/.

Buying products

Buying a product means that you have accepted the terms of the product as shown on the product's listing page. This includes pricing terms and the seller's end user license agreement (EULA), and that you agree to use such product in accordance with the AWS Customer Agreement.

If the product has a monthly fee or is purchased with a subscription contract, you are charged the fee upon subscription, prorated based on the time remaining in the month. No other charges are assessed until you launch an Amazon EC2 instance with the product AMI, deploy the product using an AWS CloudFormation template, or register the product on the seller's website.

If the product has an annual subscription option, you are charged the full annual fee upon subscription. This charge covers product usage base, with subscription renewal due on the anniversary of the original subscription date. If you don't renew at the end of the annual subscription period, the subscription converts to an hourly subscription at the current hourly rate.

For more information about data product subscriptions, see Subscribing to Data Products on AWS Data Exchange in the *AWS Data Exchange User Guide*.

Launching software

After buying software, you can launch Amazon Machine Images (AMIs) that contain it by using the 1-Click Launch view in AWS Marketplace. You can also launch it using other Amazon Web Services (AWS) management tools, including the AWS Management Console, the Amazon Elastic Compute Cloud (Amazon EC2) console, Amazon EC2 APIs, or the AWS CloudFormation console.

The 1-Click Launch view allows you to quickly review, modify, and then launch a single instance of the software with settings recommended by the software seller. The **Launch with EC2 Console** view provides an easy way to find the AMI identification number and other pertinent information that is required to launch the AMI using the AWS Management Console, Amazon EC2 APIs, or other management tools.

For AWS Marketplace products with complex topologies, the **Custom Launch** view provides a **Launch with CloudFormation Console** button that loads the product in the AWS CloudFormation console

with the appropriate AWS CloudFormation template. You can then follow the steps in the AWS CloudFormation console wizard to create the cluster of AMIs and associated AWS resources for that product.

Software and services on AWS Marketplace

AWS Marketplace features many software categories including databases, application servers, testing tools, monitoring tools, content management, and business intelligence. You can select commercial software from well-known sellers, as well as many widely used open source offerings. When you find products you want, you can buy and deploy that software to your own Amazon EC2 instance with 1-Click. You can also leverage AWS CloudFormation to deploy a topology of the product.

Any AWS customer can shop on AWS Marketplace. Software prices and estimated infrastructure prices are displayed on the website. You can purchase most software immediately, using payment instruments already on file with AWS. Software charges appear on the same monthly bill as AWS infrastructure charges.

Notes

- There are many business products available in the AWS Marketplace, including both software-as-a-service (SaaS) and server-based products. The server-based products might require technical knowledge or IT support to set up and maintain.
- The information and tutorials in Getting Started with Amazon EC2 Linux Instances can help you learn what you need to know about Amazon EC2 basics. If you plan to launch complex topologies of AWS Marketplace products through AWS CloudFormation, Getting Started with AWS CloudFormation can help you learn useful AWS CloudFormation basics.

Differences between AWS Marketplace and Amazon DevPay

There are substantial differences between AWS Marketplace and Amazon DevPay. Both help customers buy software that runs on AWS, but AWS Marketplace offers a more comprehensive experience. For software buyers, the key differences are the following:

- AWS Marketplace offers a shopping experience more like Amazon.com, simplifying discovery of available software.
- AWS Marketplace products work with other AWS features such as VPC and can be run on Reserved and Spot Instances, in addition to normal On-Demand Instances.
- AWS Marketplace supports software backed by Amazon Elastic Block Store, and DevPay does not.

Additionally, software sellers benefit from the marketing outreach and ease of discovery of AWS Marketplace.

Supported Regions

For software products, the seller chooses which AWS Regions to make their software available in, as well as the instance types. We encourage making products available in all available Regions and on all instance types that make sense. The AWS Marketplace website is available worldwide and supports the following Regions:

- North America
  - US East (Ohio)
  - US East (N. Virginia)
  - US West (N. California)
  - US West (Oregon)
  - AWS GovCloud (US-East)
  - AWS GovCloud (US-West)
  - Canada (Central)

- Africa
  - Africa (Cape Town)

- South America
  - South America (São Paulo)

- EMEA
  - Europe (Frankfurt)
  - Europe (Ireland)
  - Europe (London)
  - Europe (Milan)
  - Europe (Paris)
  - Europe (Stockholm)

- APAC
  - Asia Pacific (Singapore)
  - Asia Pacific (Sydney)
  - Asia Pacific (Mumbai)
  - Asia Pacific (Tokyo)
  - Asia Pacific (Seoul)
  - Asia Pacific (Hong Kong)
  - Asia Pacific (Osaka)

- Middle East
  - Middle East (Bahrain)

For more information on supported Regions for data products, see Endpoints and AWS Regions in the *AWS Data Exchange User Guide*.

Product categories

AWS Marketplace is organized into seven primary categories, with subcategories under each. On the AWS Marketplace website, you can search and filter based on the categories and subcategories.

Topics

Infrastructure software

The products in this category provide infrastructure-related solutions.

Application Development

Products used for application development.

Application Servers

Servers used for application development.

Application Stacks

Stacks used for application development.

Big Data

Tools used for your big data projects.

Databases and Caching

Database and caching-related products.

High Performance Computing

High performance computing products.

Migration

Products used for migration projects.

Network Infrastructure

Products used to create networking solutions.

Operating Systems

Packaged Linux and Windows operating systems.

Security

Security products for your infrastructure.

Storage and Backup

Products used for storage and backup solutions.

Developer tools

The products in this category provide tools focused on developers and developer teams.

Issues and Bug Tracking

Products used by developer teams to track and manage software bugs.

Monitoring

Products used for monitoring operating software.

Log Analysis

Products used for logging and log analysis.

Source Control

Tools used to manage and maintain source control.

Testing

Products used for automated testing of software products.

Business software

The products in this category help you run your business.

Business Intelligence

Products used for enabling business intelligence in your organization.

Collaboration

Products used to enable collaboration in your business.

Content Management

Products focused on content management.

CRM

Tools focused on customer relationship management.

ecommerce

Products that provide ecommerce solutions.

Education and Research

Products aimed at providing education and research solutions.

Financial Services

Products that enable financial services in your organization.

Healthcare and Life Sciences

Products used in the healthcare and life sciences industries.

Media

Media-related products and solutions.

Project Management

Tools for project management.

Machine learning

The products in this category provide machine learning algorithms and model packages that work with Amazon SageMaker.

ML Solutions

Machine learning solutions.

Data Labeling Services

Products that provide data labeling capability.

Computer Vision

Products that enable computer vision capability.

Natural Language Processing

Products that enable natural language processing capability.

Speech Recognition

Products that enable speech recognition capability.

Text

Products that enable text learning capability. Examples include classification, clustering, edit/processing, embedding, generation, grammar/parsing, identification, names and entity recognition, sentiment analysis, summarization, text-to-speech, and translation.

Image

Products that enable image analysis capability. Examples include 3D, captioning, classification, edit/processing, embedding/feature extraction, generation, grammar/parsing, handwriting recognition, human/faces, object detection, segmentation/pixel labeling, and text/OCR.

Video

Products that enable video analysis capability. Examples include classification, object detection, edit/processing, anomaly detection, speaker identification, motion, reidentification, summarization, text/captioning, and tracking.

Audio

Products that enable audio analysis capability. Examples include speaker identification, speech-to-text, classification, song identification, and segmentation.

Structured

Products that enable structured analysis capability. Examples include classification, clustering, dimensionality reduction, factorization models, feature engineering, ranking, regression, and time-series forecasting.

IoT

Products used to create IoT-related solutions.

Analytics

Analytical products for IoT solutions.

Applications

Application products for the IoT solutions space.

Device Connectivity

Products used to manage device connectivity.

Device Management

Products used to manage devices.

Device Security

Products used to manage security for your IoT devices.

Industrial IoT

Products focused on providing industrial-related IoT solutions.

Smart Home and City

Products used to enable smart home and smart city solutions.

Professional services

The products in this category provide consulting services related to AWS Marketplace products.

Assessment

Evaluation of your current operating environment to find the the right solutions for your organization.

Implementation

Help with configuration, setup, and deployment of third-party software.

Premium support

Access to guidance and assistance from experts, designed for your needs.

Managed services

End-to-end environment management on your behalf.

Training

Tailored workshops, programs, and educational tools provided by experts to help your employees learn best practices.

Desktop applications

The products in this category provide infrastructure-related solutions.

Desktop Applications

Desktop applications and utilities for general productivity and specific job role enablement.

AP and Billing

Applications used for job roles focused on accounts payable and billing.

Application and the Web

General purpose and web environment applications.

Development

Applications used for development.

Business Intelligence

Applications used by job roles focused on managing business intelligence.

CAD and CAM

Applications used by job roles focused on computer-aided design and manufacture.

GIS and Mapping

Applications used by job roles focused on GIS and mapping.

Illustration and Design

Applications for job roles focused on illustration and design.

Media and Encoding

Application used for job roles involved in media and encoding.

Productivity and Collaboration

Applications focused on enabling productivity and enabling collaboration.

Project Management

Application for project manager job roles.

Security/Storage/Archiving

Applications focused on job roles involved in security, storage, and data archiving.

Utilities

Utility-focused applications for various job roles.

Data products

The products in this category are sets of file-based data. For more information, see the AWS Data Exchange User Guide.

Product types

AWS Marketplace includes popular open source and commercial software, as well as free and paid data products. These products are available in different ways: as individual Amazon Machine Images (AMIs), as a cluster of AMIs deployed through an AWS CloudFormation template, as software as a service (SaaS), as professional services, and as AWS Data Exchange data products.

For more details about these product types, see the following topics:

- Container products (p. 17)
- Desktop products (p. 19)
- Machine learning products (p. 19)
- Professional services products (p. 20)
- SaaS products (p. 21)
- AMI-based server products (p. 22) (including AMI and private image products)
- Data products (p. 33)

What is an AMI?

An Amazon Machine Image (AMI) is an image of a server, including an operating system and often additional software, which runs on AWS.

How are AMI products different than SaaS products?

Both AMI and SaaS product listings are from trusted sellers. AMI products run within a customer's AWS account. You retain more control over software configuration and over the servers that run the software, but you also have additional responsibilities regarding server configuration and maintenance.

Why do AWS Marketplace products have more than one AMI?

An AWS Marketplace product contains one AMI for each AWS Region in which the product is available. These AMIs are identical except for their location. Additionally, when sellers update their product with the latest patches and updates, they may add another set of AMIs to the product.

Some AWS Marketplace products may launch multiple instances of an AMI because they are deployed as a cluster using AWS CloudFormation templates. This cluster of instances, along with additional AWS infrastructure services configured by the AWS CloudFormation template, act as a single product deployment.

What is AWS CloudFormation?

AWS CloudFormation is a service that helps you model and set up your AWS resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. An AWS CloudFormation template describes the various AWS resources that you want, such at Amazon Elastic Compute Cloud (Amazon EC2) instances or Amazon Relational Database Service (Amazon RDS) database instances). AWS CloudFormation takes care of provisioning and configuring those resources for you. For more information, see Getting Started with AWS CloudFormation .

How can I use AWS CloudFormation templates to deploy software products from AWS Marketplace?

Software sellers may offer AWS CloudFormation templates to define a preferred deployment topology consisting of multiple AMI instances and other AWS resources. If an AWS CloudFormation template is available for a product it will be listed as a deployment option on the product listing page.

How is deploying an AMI different from deploying a cluster of AMIs using an AWS CloudFormation template?

You can use an AMI to deploy a single Amazon EC2 instance. You can use an AWS CloudFormation template to deploy multiple instances of an AMI that act as a cluster—along with AWS resources such as Amazon RDS, Amazon Simple Storage Service (Amazon S3), or any other AWS service—as a single solution.

How are these products different from the products I can find in the AWS Community AMI catalog?

The AWS Marketplace catalog contains a curated selection of open source and commercial software from well-known sellers. Many products on AWS Marketplace can be purchased by the hour.

The AMI catalog is a community resource where people and development teams can list and exchange software or projects under development, without having to go through extensive vetting. Listings in the community AMI catalog may or may not be from well-known sellers and generally have not undergone additional investigations.

Does AWS Marketplace also sell software for me to install on my on-premises servers or PCs?

No. The software listed in AWS Marketplace is only available to run on Amazon EC2. It is not available for download.

Container products

AWS Marketplace for containers enables you to discover, procure, and deploy free, bring-your-own-license (BYOL), and pay-as-you-go container products from sellers for use with supported runtimes and services, such as Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS). You can use either the AWS Marketplace website or the Amazon ECS console to find container products that you can try, buy, and launch. These are either standalone products fulfilled as Docker container images or container-based agents that work with existing AWS Marketplace software-as-a-service (SaaS) products. You can deploy many products to Amazon ECS or Amazon EKS by using ISV-supplied deployment templates, such as task definitions or Helm charts, and you can also access container images directly from private Amazon Elastic Container Registry (Amazon ECR) repositories after you have subscribed to those products.

Free, Paid and Bring Your Own License (BYOL) products are available for use on Amazon ECS and Amazon EKS. Amazon ECS can operate in two modes: Fargate launch type and EC2 launch type. For paid products, you are billed by AWS as with any AWS Marketplace product according to the pricing model, which might be a fixed monthly fee or an hourly price that is charged per second.

Pricing details will be shown on the detail page and when you subscribe to the product. If the product is paid, you'll pay for one of the following:

- A fixed monthly charge that provides unlimited usage
- Upfront for usage of the product for the duration of a long term contract
- As you go (typically hourly) based on usage of the product.

This guide explains how to use AWS Marketplace for containers to find, purchase, and launch container products, with examples of tasks you should perform, test, and validate to provide feedback to the AWS Marketplace team.

Docker containers and Kubernetes

Docker containers are an open-source software technology that provides an additional layer of abstraction and automation over virtualized operating systems such as Linux and Windows Server. Just as virtual machines are instances of server images, containers are instances of Docker container images. They wrap server application software in a file system that contains everything it needs to run: code, runtime, system tools, system libraries, and so on. This guarantees that the software always runs the same, regardless of its environment. Analogous to Java virtual machines, containers require an underlying platform to provide a translation and orchestration layer while being isolated from the operating system and each other. There are different Docker-compatible runtimes and orchestration services that you can use with Docker containers, including Amazon ECS, which is a highly scalable, high-performance orchestration service for AWS, and Amazon EKS, which makes it easy to deploy, manage, and scale containerized applications using Kubernetes, an open source management and orchestration service.

Finding and subscribing to container products

You can find container products by browsing the AWS Marketplace website. Container products are examples of server software products with a **Container** delivery method, so you can search for them by using the Search page and then filtering the delivery method by **Container**.

Using the Amazon ECS console

You can also find container products in the Amazon ECS console. The navigation pane has links to discover new products from AWS Marketplace and to see existing subscriptions.

Browsing product details

Once you have found a product you are interested in, choose the title to browse to the product detail page. Here you can find information on the software including product description, supported Amazon services (for example, Amazon ECS or Amazon EKS), pricing details, usage information, support information, and available fulfillment options. Products may be free, BYOL, or PAYG, with either a fixed monthly price or an hourly price that is charged per Amazon ECS task. Each product will have at least one fulfillment option, which is a set of one or more container images that are required to run the software. You can also read and write reviews for the product from this page. Choose **Continue to Subscribe** to proceed.

Subscribing to products

If you want to use a product, you will need to subscribe to it first. On the subscription page you can view pricing information for paid products, and access the end-user license agreement (EULA) for the software.

Choose **Accept Terms** to proceed. This will create a *subscription* to the product, which provides an *entitlement* to use the software. It will take a minute or two for the subscription to complete. Once you receive an entitlement to a paid product, if you start using the software you will be charged. If you cancel your subscription without terminating all running instances of the software, you will continue to be charged for any software usage. You may also incur infrastructure charges related to using the product. For example, if you create a new Amazon EKS cluster to host the software product, you will be charged for that service.

> **Note**
> For a walk-through showing how to subscribe to and deploy a container-based product, you can also refer to the video, Deploying AWS Marketplace Containers on Amazon ECS Clusters (3:34).

Launching a product

After you have an active subscription, choose **Continue to Configuration**, where you can select an available fulfillment option. For container products, there might be up to four fulfillment options, which represent different configurations for the software. For example, an ISV might create one fulfillment option that is a simple configuration used for testing the product, and another fulfillment option that is intended to be deployed at scale within an enterprise.

Each fulfillment option includes information about which services are supported (for example, Amazon ECS or Amazon EKS) and also provides software version details. After you have chosen the appropriate fulfillment option, you can choose **Continue to Fulfillment**.

> **Note**
> For a walk-through showing how to subscribe to and deploy a container-based product, you can also refer to the video, Deploying AWS Marketplace Containers on Amazon ECS Clusters (3:34).

Launch process

On the launch or fulfillment page for the product, deploy your selected fulfillment option, which is shown in the **Configuration Details** section. Choose **Usage Instructions** to see documentation from the ISV about how to use the product, such as how to sign in to a web server, or post-launch configuration.

If the ISV has provided deployment templates to simplify deploying your product on AWS, such as an AWS CloudFormation template, a task definition for Amazon ECS, or a Helm chart for Kubernetes, information is provided for obtaining those templates. There might be up to four deployment templates available for each fulfillment option.

If there are no deployment templates provided, or if you would prefer to create your own deployment template or manually configure how the product is launched, you can also access the container images

directly from within Amazon ECR, which is a fully managed container registry that makes it easy for developers to store, manage, and deploy Docker container images. Choose **View container image details** to open a dialog box with instructions for configuring your client to access the AWS Marketplace repository on Amazon ECR, and to see the appropriate Docker pull commands to use to retrieve the images.

After you have access to the deployment template or templates and container images, you can launch and run the software. If the product is free or BYOL, there are no software charges, but there might be charges for the AWS infrastructure on which the product runs. If the product is paid, either you pay a fixed monthly charge that provides unlimited usage, or you pay an hourly charge that is prorated per second with a one-minute minimum. Remember that if you cancel a subscription to a product, you are still charged for any running software until you terminate all instances of the software. After you cancel a subscription to a paid product, however, you cannot launch any new instances of that software.

To run a paid product, you must create an IAM role that grants permission for your container to call `RegisterUsage`. The following code can be used to configure these permissions. You must supply this IAM role in the Amazon ECS Task Role Developer Guide or in Amazon EKS IAM Roles for Service Accounts.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-marketplace:RegisterUsage"
                ],
                "Effect": "Allow",
                "Resource": "*"
        }
    ]
}
```

Canceling a subscription

To cancel a subscription to a product, use the **Your Software** page.

Desktop products

AWS Marketplace for Desktop Apps is a section of AWS Marketplace where you can find applications to use with Amazon WorkSpaces. AWS Marketplace for Desktop Apps includes applications you can subscribe to on a monthly basis, including applications from companies such as Microsoft, Corel, and Foxit Software, as well as popular open-source titles.

Machine learning products

AWS Marketplace has a category for machine learning products you can subscribe to through AWS Marketplace. The product category is Machine Learning. The products in this category include machine learning (ML) algorithms and model packages.

An **Amazon SageMaker *algorithm*** is a unique Amazon SageMaker entity that is identified by an Amazon Resource Name (ARN). An algorithm has two logical components: training and inference. Customers use the training component to create a training job or tuning job using your input dataset in Amazon SageMaker to build machine learning models. Amazon SageMaker saves the model artifacts generated by the algorithm during training to an Amazon Simple Storage Service (Amazon S3) bucket. Customers can build a model package using the algorithm's inference component and the model artifacts that are

stored in the S3 bucket. Customers can use this model package to build a model, which can then be used for running on hosting services or running batch transforms in Amazon SageMaker.

An **Amazon SageMaker *model package*** is a unique pretrained ML model that is identified by an ARN on Amazon SageMaker. Customers use a model package to create a model in Amazon SageMaker. Then, the model can be used with hosting services to run real-time inference or with batch transform to run batch inference in Amazon SageMaker.

You can browse and search for hundreds of ML algorithms and model packages from a broad range of subcategories, such as computer vision, natural language processing, speech recognition, text, data, voice, image, video analysis, fraud detection, and predictive analysis.

To assess the quality and suitability of a model, you can review product descriptions, usage instructions, customer reviews, sample Jupyter notebooks, pricing, and support information. You deploy models directly from the Amazon SageMaker console, through a Jupyter notebook, with the Amazon SageMaker SDK, or using the AWS Command Line Interface AWS CLI. Amazon SageMaker provides a secure environment to run your training and inference jobs by running a static scan on all marketplace products.

Find, subscribe, and deploy

To find, buy and deploy machine learning products, you find and subscribe to products on AWS Marketplaceand then deploy the product on Amazon SageMaker.

You pay only for your usage, with no minimum fees or upfront commitments. AWS Marketplace provides a consolidated bill for algorithms and model packages, and AWS infrastructure usage charges. To find, subscribe, and deploy Amazon SageMaker algorithms and model packages:

1. From the AWS Marketplace website, under **Find AWS Marketplace products that meet your needs**, use the **Categories** drop-down menu to find the subcategory under **Machine Learning** that you are interested in. You can refine your search results by applying resource type, category, and pricing filters. From search results, you can access the product detail page, which allows you to review the product description, usage instructions, customer reviews, data requirements, sample Jupyter notebooks, and pricing and support information.
2. To view the procurement page, from the product detail page, choose **Continue to subscribe**. After reviewing the product pricing information and the end user license agreement (EULA), you can subscribe. After subscribing, you can configure the product (for example, by selecting a specific version or deployment region) on the AWS Marketplace website.
3. After configuring the product, you can view the Amazon SageMaker product detail page by choosing **View in Amazon SageMaker**. From the Amazon SageMaker console, you can deploy the algorithms and model packages using the Amazon SageMaker console, Jupyter notebook, Amazon SageMaker CLI commands, or API operations.

To deploy a third-party algorithm/model package on Amazon SageMaker, you need a valid subscription. Find the suitable algorithm/model package from AWS Marketplace and then subscribe to the products. Navigate to Your Marketplace Software and make sure that you have a valid subscription to the algorithm you want to deploy.

For more information about deploying on Amazon SageMaker, see Getting Started.

Professional services products

AWS Marketplace includes products that are professional services from AWS Marketplace sellers. You can find these products in the *Professional Services* category when searching in AWS Marketplace. You subscribe and purchase these products through AWS Marketplace, but you will work with the seller to set up the professional services to meet your needs.

Purchasing professional services

You can search for professional services using the *Professional Services* category in AWS Marketplace. When you find a product that interests you, request an offer from the seller. Because professional services usually involve working together, you must provide some additional information to the seller in order to complete the purchase. You can also use this as an opportunity to negotiate pricing and any other details of the service that need to be resolved. You will receive a private offer for the product. For more information about private offers, see Private offers (p. 41).

To purchase a professional services product

1. Go to AWS Marketplace and sign in to your AWS account, then search and find a professional services product that you want to purchase.
2. On the product details page for the product, choose **Continue**.
3. On the **Request service** page, add the additional information that is required for the seller to create the offer, including your name, email address, company name, and any additional information that would be helpful to the seller, including business needs, timelines, and contract requirements.
4. The seller will contact you via the email address that you provided to work out the details of your offer. Once you have agreed, the seller will send you a link to the offer in AWS Marketplace. Open the link in a browser, and sign into your AWS account.
5. Review the offer details on the procurement page that you opened from the seller. Make sure that the offer is for the service you are expecting, and the price that you are expecting. Also check the terms—whether you pay a lump sum or a series of charges. If the offer is correct, continue. Otherwise, contact the seller to make changes.
6. Under **Configure contract**, choose the configuration that you would like to use for your contract. For example, if you are purchasing a support contract, there might be options for *Silver*, *Gold*, or *Platinum* contracts, with different prices.
7. Select **Create contract** to purchase the service. The seller should contact you within 2 business days with instructions for using the service.

SaaS products

For software as a service (SaaS) products, you subscribe to products through AWS Marketplace, but you access the product in the software seller's environment. AWS Marketplace offers two pricing models for SaaS listings: SaaS subscriptions and SaaS contracts.

SaaS subscriptions

With SaaS subscriptions, the software seller tracks your usage and you pay only for what you use. This pay-as-you go pricing model is similar to that of many Amazon Web Services (AWS) services. Billing for your usage of a SaaS product is managed through your AWS bill.

SaaS contracts

Some companies make SaaS contracts available for purchase through AWS Marketplace. This allows you to purchase discrete quantities of licenses or data ingest for these products and have them billed, in advance, through your AWS account. For example, you might purchase 10 user access licenses for a year, or you might purchase 10 GB of data ingest per day for a year.

You can purchase using the product's detail page on AWS Marketplace. If this option is available, **Software as a Service (SaaS) Contracts** appears for **Delivery Method** on the product's detail page. When you make the purchase, you will be directed to the product's website for account setup and configuration. The usage charges will then appear on your regular AWS account billing report.

To subscribe with a SaaS contract

1. Choose **Continue** to start the subscription. You can choose the quantities or units you want, length of subscription (if multiple options are available), and automatic renewal.
2. After you have made your selections, choose **Create Contract**.
3. Choose **Set Up Your Account**, which takes you to the company's website. While your account is being configured and the payment is being verified, you will see your contract is pending on the AWS Marketplace details page for the product.

After configuration is complete, if you return to the product page, you'll find a link to set up your account. The software will appear under **Your Marketplace Software** when you are signed in to your AWS Marketplace account. You can now start using the software. If you do not complete the setup process for your account, you will be prompted to do so when you revisit that product on AWS Marketplace.

You access the software subscription from the software company's website using the account you created on their website. You can also find website links for any software subscriptions you purchased through AWS Marketplace under **Your Marketplace Software** when you are signed in to your AWS Marketplace account.

AMI-based server products

On AWS Marketplace, you can search for Amazon Machine Images (AMIs) (with search suggestions), view product reviews submitted by other customers, subscribe and launch AMIs, and manage your subscriptions. All AWS Marketplace products have been verified for quality and pre-configured for 1-Click launch capability on Amazon Web Services (AWS) infrastructure.

Topics

AMI subscriptions

Some AMI-based software products offer an annual subscription pricing model, in which you make a one-time upfront payment and then pay no hourly usage fee for the next 12 months. You can apply one annual subscription to an AWS Marketplace software product to one Amazon EC2 instance. You can also continue to launch and run AWS Marketplace software products using hourly pricing. Charges for using Amazon EC2 and other services from AWS are separate and in addition to what you pay to purchase AWS Marketplace software products.

Metering-enabled AMI products

Some products listed on AWS Marketplace are billed on usage measured by the software application. Examples of metered usage dimensions include Data usage, Host/Agent usage, or Bandwidth usage. These products require extra configuration to function correctly. An IAM role with the permission to meter usage must be associated with your AWS Marketplace Amazon Elastic Compute Cloud (Amazon EC2) instance at the time of launch. For more information about IAM roles for Amazon EC2, see IAM Roles for Amazon EC2.

Cost allocation tagging in AMI products

AWS Marketplace supports cost allocation tagging for Amazon Machine Image (AMI)-based software products. New and existing Amazon Elastic Compute Cloud (Amazon EC2) instance tags automatically populate against corresponding AWS Marketplace AMI usage. You can use activated cost allocation tags to identify and track AMI usage through AWS Cost Explorer, the AWS Cost and Usage Reports, AWS Budgets, or other cloud spend analysis tools.

The vendor that provided the AMI may also record other custom tags in the metering for AMI-based products, based on information specific to the product. For more details, see Cost allocation tagging (p. 35).

You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs.

Cost allocation tagging only tracks costs from the time when the tags were activated in the Billing and Cost Management console. Only AWS account owners, AWS Organizations management account owners, and AWS Identity and Access Management (IAM) users with the appropriate permissions can access the Billing and Cost Management console for an account. Regardless of whether you use cost allocation tagging, there's no change to how much you're billed. Whether you use cost allocation tags has no impact on the functionality of your AMI-based software products.

Tracking cost allocation tags for one AMI across multiple instances

Each launched Amazon EC2 instance for a AWS Marketplace AMI subscription has a corresponding AWS Marketplace software usage line item in the AWS Cost and Usage report. Your AWS Marketplace usage will always reflect the specific tags applied to the corresponding Amazon EC2 instance. This allows you to distinguish your AWS Marketplace usage costs based on the different tag values that were assigned, at an instance level.

You can also sum up your tag-based usage costs to equal the AMI software usage charge reflected in your bill with either the Cost Explorer or the AWS Cost and Usage report.

Finding budgets with cost allocated tagged instances

If you already have active budgets filtered on cost allocation tags over a number of Amazon EC2 instances in the Billing and Cost Management console, it might be difficult to find all of them. The following Python script returns a list of budgets which contain Amazon EC2 instances from the AWS Marketplace in your current AWS Region.

You can use this script to be aware of a potential impact to your budget, and where overruns might occur from this change. Note that the billed amount doesn't change, but the cost allocations will be reflected more accurately, which can impact budgets.

```
#! /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()
```

Example output

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

Budgets containing tagged Marketplace EC2 instances:
EC2 simple
```

```
MP-test-2
```

Related topics

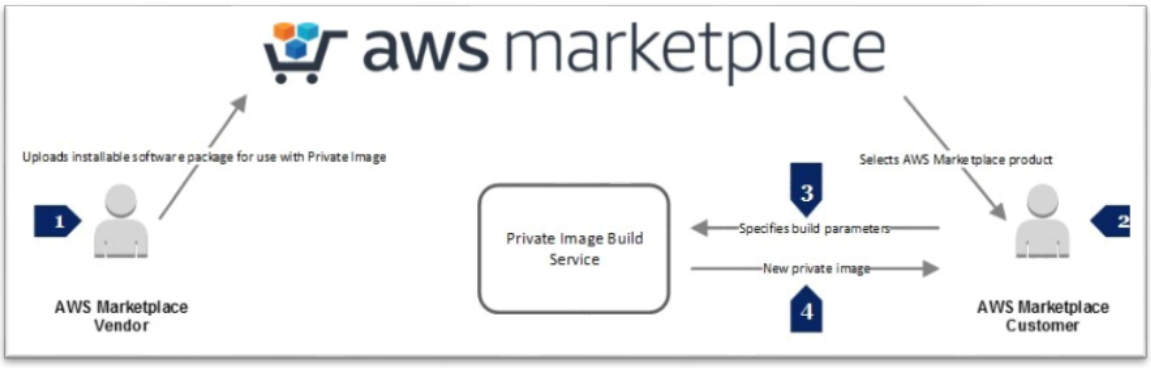
For more information, see the following topics:

- Using Cost Allocation Tags in the *AWS Billing and Cost Management User Guide*.
- Activating the AWS-Generated Cost Allocation Tags in the *AWS Billing and Cost Management User Guide*.
- Tagging Your Amazon EC2 Resources in the Amazon EC2 User Guide for Linux Instances.

Private image build

AWS Marketplace Private Image Build enables you to purchase installable software products through AWS Marketplace and then install those products on a gold image or AMI that you choose from the images available to your AWS account. For the purposes of this content, a *gold image* is a server image that includes a base operating system (OS) with modifications applied so that each server launched from that image adheres to your IT standards you define. You choose the software from AWS Marketplace that you want to install and the base AMI for the build. Then you use the AWS Marketplace Image Build Service to build and deliver a new AMI as a private image available only to your AWS account.

This service helps you to better meet your internal security, compliance, and management requirements by enabling you to run AWS Marketplace products on a base operating system that meets your IT standards.



Sellers participating in AWS Marketplace Private Image Build create installable versions of their product for specific OS platforms, operating systems, and OS versions. When a seller submits a set of software packages for their product, the AWS Marketplace Image Build Service installs and scans the product on the specified OS before publishing the product in AWS Marketplace. When you purchase a product enabled for AWS Marketplace Private Image Build, you may choose an existing AMI to build a new private image on. Once you have used the AWS Marketplace Image Build Service to build a new image, it becomes available in your Amazon Elastic Compute Cloud (Amazon EC2) console as an image that you own. You can build an image using the AWS Marketplace website, or you can use the AWS Marketplace Image Build Service API.

There is a software and infrastructure charge for the AWS services that you use to complete the build process, which may take 1-2 hours depending on the product. However, there is no additional charge for using the AWS Marketplace Image Build Service to create private images. Once the image is built, you don't incur charges for product or AWS resource usage until you use the product.

AWS Marketplace Private Image Build uses AWS Identity and Access Management (IAM) to create IAM roles and policies that grant limited permissions to end users to build and view private images. Completing the prerequisite steps requires administrative-level privileges.

Completing prerequisite steps

The prerequisite steps described here require administrative-level permissions that configure IAM so that you can grant the ability to build private images to other users. Once the IAM policies and roles are created you can attach them to group (or user) accounts so the associated users can build private images.

IAM is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources. You create identities (users, groups, and roles) and add the users to the groups so you can then manage groups instead of individual users. An IAM role is similar to a user in that it's an identity with permission policies that determine what the identity can and can't do in AWS. However, a role doesn't have any credentials (password or access keys) associated with it. Instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. An IAM user can assume a role to temporarily take on different permissions for a specific task.

The access management portion of IAM helps you to define what a user or other entity is allowed to do in an account, often referred to as *authorization*. Permissions are granted through policies. A policy is an entity in AWS that, when attached to an identity or resource, defines their permissions. AWS evaluates these policies when a principal, such as a user, makes a request. Permissions in the policies determine whether the request is allowed or denied. Policies are stored in AWS as JSON documents attached to principals as *identity-based policies* or to resources as *resource-based policies*.You give permissions by defining permission policies and assigning the policy to a group.

Identity-based policies are permission policies that you can attach to a principal (or identity), such as an IAM user, role, or group. Resource-based policies are JSON policy documents that you attach to a resource such as an Amazon Simple Storage Service (Amazon S3) bucket. Identity-based policies control what actions that identity can perform, on which resources, and under what conditions. Identity-based policies can be categorized into *AWS managed policies*, *customer managed policies*, and *inline policies*.

Resource-based policies control what actions a specified principal can perform on that resource and under what conditions. Resource-based policies are inline policies, and there are no managed resource-based policies. Although IAM identities are technically AWS resources, you can't attach a resource-based policy to an IAM identity. You must use identity-based policies in IAM. *Trust policies* are resource-based policies that are attached to a role that define which principals can assume the role. When you create a role in IAM, the role must have two things: a trust policy that indicates who can assume the role and a permission policy that indicates what they can do with that role. Remember that adding an account to the trust policy of a role is only half of establishing the trust relationship. By default, no users in the trusted accounts can assume the role until the administrator for that account grants the users the permission to assume the role.

The AWS Marketplace Image Building Service uses two IAM roles, and each role has a permissions policy and a trust policy. If you have IAM users access the AWS Marketplace website to build private images, those users also need IAM permissions to list and assign the roles needed to create and view the private images they build.

As an administrator, you create the two roles that are required and their associated policies. The first role is an instance profile that is attached to the instance created during the image build process. An instance profile is a container for an IAM role that you can use to pass role information to an Amazon EC2 instance when the instance starts. The second is an IAM role that provides access to AWS Systems Manager and Amazon EC2. To configure the instance profile, attach a permissions policy that provides the required permissions. Then edit the trust policy for the role to grant permission for Amazon EC2 and AWS Systems Manager to assume the role.

Creating an instance profile role

To create the instance profile role through the IAM console:

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.

2. In the navigation pane of the IAM console, choose **Roles** and then choose **Create role**.
3. For **Select type of trusted entity**, choose **AWS service**.
4. For **Choose the service that will use this role**, choose **EC2** and then choose **Next: Permissions**.
5. For **Create policy**, choose **Next: Review**.
6. For **Role name**, type a role name or role name suffix to help you identify the purpose of this role, for example *MyInstanceRole*. Role names must be unique in your AWS account.
7. Review the role and then choose **Create role**.
8. On the **Roles** page, choose the role that you created.
9. For **Permissions**, choose **Add inline policy**.
10. Choose the **JSON** tab and replace all of the text with the following InstanceRolePermissionsPolicy text.

    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
You'll need to create the bucket, *DOC-EXAMPLE-BUCKET* before you begin this process.

11. Choose **Review policy**.
12. For **Policy name**, type a name to help you identify the purpose of this policy, for example *MyInstanceRolePolicy*, and choose **Create policy**.

To edit the trust relationship for the role:

1. On the **Roles** page, choose the role that you created.
2. Choose the **Trust relationships** tab and then choose **Edit trust relationship**.
3. Select all of the text in the **Policy Document** text box and replace it with the following InstanceRoleTrustPolicy text.

   InstanceRoleTrustPolicy:

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

4. Choose **Update Trust Policy**.

Creating an AWS Systems Manager automation role

To create the AWS Systems Automation role:

1. In the navigation pane of the IAM console, choose **Roles** and then choose **Create role**.
2. For **Select type of trusted entity**, choose **AWS service**.
3. For **Choose the service that will use this role**, choose **EC2** and then choose **Next: Permissions**.
4. For **Create policy**, choose **Next: Review**.
5. For **Role name**, type a role name or role name suffix to help you identify the purpose of this role, for example *MyAutomationRole*. Role names must be unique in your AWS account.
6. Review the role and then choose **Create role**.
7. On the **Roles** page, choose the role that you created.
8. For **Permissions**, choose **Add inline policy**.
9. Choose the **JSON** tab and replace all the text with the following AutomationRolePermissionsPolicy text.

   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
You must replace *{{ Instance Profile }}* with the Amazon Resource Name (ARN) for the instance policy role that you created earlier. Locate the role in the IAM management console and choose it. On the summary page for the role, the **Role ARN** is the first item listed, for example, **arn:aws:iam::123456789012:role/MyInstanceRole**.

To edit the trust relationship for the role:

1. On the **Roles** page, choose the role that you created.
2. Choose the **Trust relationships** tab and then choose **Edit trust relationship**.
3. Replace all the text in the **Policy Document** text box with the following InstanceRoleTrustPolicy text.

AutomationRoleTrustPolicy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm.amazonaws.com",
```

```
          "ec2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Choose **Update Trust Policy**.

You have now created the two roles and associated policies that you will use during the private image build process.

Using a policy to access the AWS Marketplace website

Most organizations don't allow users to log in with root account credentials. Instead, they create IAM users with limited permissions based on organizational roles or tasks that only certain people can perform. AWS Marketplace provides two primary IAM managed policies for working with AWS Marketplace tools. Use these two managed policies to provide the ability to perform the described tasks:

- **AWSMarketplaceFullAccess** - Provides the ability to subscribe and unsubscribe to AWS Marketplace software, allows users to manage Marketplace software instances from the Marketplace 'Your Software' page, and provides administrative access to EC2.
- **AWSMarketplaceRead-only** – Provides the ability to review AWS subscriptions.

You can add the managed policy named AWSMarketplaceFullAccess to an IAM user, group, or role to provide all of the permissions needed to access the AWS Marketplace website and perform the tasks associated with AWS Marketplace Private Image Build. To add the policy to a user, group or role:

1. Sign in to the AWS Management Console and open the AWS IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the AWS IAM console, choose **Policies**.
3. Next to **Filter policies**, enter *AWSMarketplaceFullAccess*. The policy should be listed in the results.
4. In the **Results** pane, choose **AWSMarketplaceFullAccess**.
5. In the **Policy actions** pulldown menu, choose **Attach**.
6. Select the users, groups and roles you want to attach this policy to, and then choose **Attach Policy**.

The next time that a user or member of a group or role you selected accesses the AWS Marketplace website, they can perform the tasks associated with the private image build process.

Building a private image

When you create a private image, you select the software package in AWS Marketplace and the base AMI in your Amazon EC2 console that you will use to create the new private image. Before starting the build process you must configure your AWS environment so that you can provide:

- The AMI ID for the base image that you will install the AWS Marketplace product on
- The name of an Amazon S3 bucket to store the build logs in. The S3 bucket must be in the region that the AMI will be available in
- The Amazon EC2 instance profile that the package will be installed with (see the previous section)
- The IAM automation role that the image creation process will use to create the AMI (see the previous section)
- The name of the new private image

If you have experience using AWS services, you are likely familiar with choosing regions, finding the AMI ID on your Amazon EC2 dashboard, and working with Amazon S3 buckets.

To find a product that supports building a private image, go to the AWS Marketplace product search page and, for the **Delivery Method** search filter, choose **Private Amazon Machine Image**. From the detail page for the product, you configure procurement, configuration, and fulfillment options. The product that you build is added to your AWS account.

In addition to the prerequisites specified in the previous section, your base AMI must meet the following requirements:

- Linux AMIs must have either Wget or cURL installed and configured. Windows AMIs must have PowerShell installed.
- Linux AMIs must either be able to execute EC2 User Data scripts or have the SSM agent pre-installed.
- Windows AMIs must have the SSM Agent pre-installed.

To build a private image:

1. In AWS Marketplace, from the product's detail page, choose **Continue to Subscribe**.
2. On the **Subscribe to this software** page, under **Terms and Conditions**, choose **Show Details** to view the product instance type, software usage costs, and the end user license agreement (EULA). Depending on the product, you might see various types of subscriptions. Once you choose the type of subscription, choose **Accept Terms**.
3. Choose **Continue to Configuration**.
4. On the **Configure this software** page, for **Fulfillment Option**, choose **Private Amazon Machine Image**.
5. In the **Private Image** section, for **1. Choose a region**, choose your region. For **2. Choose a private image to launch**, choose **Create New Private Image**.
6. In the **Create New Private Image** section, for **Select a base AMI to use**, choose **Owned by me**, **Public Images**, or **Private images**.
   a. **Owned by me** – AMIs that are specifically owned by your AWS account
   b. **Public Images** – AMIs that have been shared with all AWS accounts
   c. **Private images** – AMIs that have been shared with your AWS account
7. For **Input public base AMI ID** or **Input private base AMI ID**, either type the AMI ID or use the Amazon EC2 console to copy and paste the AMI ID for the image that you want to use as the base AMI.
8. For **Instance Profile**, choose the instance role that you created as a prerequisite step.
9. For **Automation Role**, choose the automation role that you created as a prerequisite step.
10. For **Build Logs**, type the name of an Amazon S3 bucket that you want the logs to be stored in. This is the simple bucket name, for example *DOC-EXAMPLE-BUCKET*, rather than the full DNS name.
11. For **Private Image Name**, type the name for the new private image.

AWS Marketplace recommends using a naming convention for the private images you create to make the images easier to identify. Also, when the AWS Marketplace Image Building Service creates a new private image, it adds an *AWSMarketplaceFulfillmentID* tag, which can be helpful in later identifying your private images. You can also complete the following optional steps to provide additional detail, or you can start the build process by choosing **Start Build**.

(Optional) To provide additional details about the private image:

1. For **Description Notes**, type any relevant information that you want included for the instance that will be used when building the private image.
2. For **Instance Type**, choose the instance type that you want to use when building the private image.

3. For **VPC**, choose the VPC that you want the instance to use when building the private image and then choose the security group and subnet.
4. For **Enable Simple Notification System**, choose an existing topic or create a new topic to receive notifications when the build status changes.
5. Choose **Start Build**.

The build process takes 1-2 hours to complete. Note the following information about the process:

- The charges for services used during the build process will appear in the AWS account used to start the private image build process. This includes the instance that runs while the AWS Marketplace product is being installed on the private image and the S3 bucket used for logs.
- You can view the status of the build process or receive Amazon SNS messages.
- Once the build is complete, the new private image is added to your AWS account and is available through the Amazon EC2 console as an AMI listed under **Owned by me**.
- Repositories used to complete the build process must be local.
- During the build, the process blocks access to the Internet.

Using AMI aliases

An Amazon Machine Image (AMI) is identified with an `AMI ID`. You can use the `AMI ID` to indicate which AMI you want to use when launching a product. The `AMI ID` has the form `ami-<identifier>`, for example, ami-123example456. Each version of each product in each AWS Region has a different AMI (and different `AMI ID`).

When you launch a product from AWS Marketplace, the `AMI ID` is automatically filled in for you. Having the `AMI ID` is useful if you want to automate launching products from the AWS Command Line Interface (AWS CLI) or by using Amazon Elastic Compute Cloud (Amazon EC2). You can find the `AMI ID` when you configure your software at launch time. For more information, see Step 2: Select your software configuration (p. 5).

The `Ami Alias` is also in the same location as the `AMI ID`, when configuring your software. The `Ami Alias` is a similar ID to the `AMI ID`, but it's easier to use in automation. An `AMI alias` has the form `aws/service/marketplace/prod-<identifier>/<version>` , for example, `aws/service/marketplace/prod-1234example5678/12.2`. You can use this `Ami Alias` Id in any Region, and AWS automatically maps it to the correct Regional `AMI ID`.

If you want to use the most recent version of a product, use the term **`latest`** in place of the version in the `AMI alias` so that AWS chooses the most recent version of the product for you, for example, **`aws/service/marketplace/prod-1234example5678/latest`**.

> **Warning**
> Using the **`latest`** option gives you the most recently released version of the software. However, use this feature with caution. For example, if a product has versions 1.x and 2.x available, you might be using 2.x. However, the most recently released version of the product might be a bug fix for 1.x.

Examples of using AMI aliases

AMI aliases are useful in automation. You can use them in the AWS CLI or in AWS CloudFormation templates.

The following example shows using an AMI alias to launch an instance by using the AWS CLI.

```
aws ec2 run-instances
--image-id resolve:ssm:/aws/service/marketplace/<identifier>/version-7.1
```

```
--instance-type m5.xlarge
--key-name MyKeyPair
```

The following example shows a CloudFormation template that accepts the AMI alias as an input parameter to create an instance.

```
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
```

Data products

You can use AWS Marketplace to find and subscribe to data products available through AWS Data Exchange. For more information, see Subscribing to Data Products on AWS Data Exchange in the *AWS Data Exchange User Guide*.

Paying for products

Your AWS Marketplace purchases are displayed in the currency you specified for your AWS account. You can change your preferred currency for your AWS account in the AWS Billing and Cost Management console. For instructions, see Changing which currency you use to pay your bill in the *AWS Billing and Cost Management User Guide*.

> **Note**
> Changing your preferred currency changes your remittance instructions. To view updated remittance instructions, see your AWS Marketplace invoice or view the **Account Settings** page in the AWS Billing and Cost Management console.

At the beginning of the month, you receive a bill from Amazon Web Services (AWS) for your AWS Marketplace charges. For software products, the bill includes a calculation of the hourly fee for the software multiplied by the number of hours any Amazon Machine Image (AMI) instance with this software runs. You also receive a bill for usage of AWS infrastructure services such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS), and bandwidth.

AWS Marketplace products using complex topologies may incur charges for clusters of AMIs and other AWS infrastructure services launched by the provided AWS CloudFormation template.

For example, suppose that you run software for 720 hours on an EC2 small instance type. The seller's fee for software usage is $0.12/hr and the EC2 charges are $0.085/hr. At the end of the month, you are billed $147.60.

For more information about subscribing to data products, see Subscribing to Data Products on AWS Data Exchange in the *AWS Data Exchange User Guide*.

For more information about paying your AWS bill, see the AWS Billing and Cost Management User Guide.

Information about refunds

For information about refunds related to your AWS Marketplace purchases, see the following pages in the *AWS Marketplace Seller Guide*:

- Refunds
- Product pricing

> **Note**
> For all refunds related to private offers, contact the seller.

Cost allocation tagging

AWS Marketplace supports cost allocation tagging for software products that you purchase. You can use activated cost allocation tags to identify and track AWS Marketplace resource usage through AWS Cost Explorer, AWS Cost and Usage Reports, AWS Budgets, or other cloud cost analysis tools. To make it easier for you to categorize and track your AWS Marketplace costs, you can use cost allocation tags to organize your resource costs on your cost allocation report.

Cost allocation tags in AWS Marketplace come from the following two sources:

- Amazon Machine Image (AMI) software product costs that are associated with an Amazon Elastic Compute Cloud (Amazon EC2) instance with tags inherit those same tags. You can activate these tags as cost allocated tags in the AWS Billing and Cost Management console for an account. For more information about using cost allocation tags with AMI products, see Cost allocation tagging in AMI products (p. 23).
- AMI, container, and SaaS products may have vendor-provided tags. For example, a software as a service (SaaS) product that bills by the number of users could use a tag to identify the usage by department. For more information about using these tags, see Vendor-metered tags (p. 35).

Cost allocation tagging only tracks costs from the time when the tags were activated in the Billing and Cost Management console. Only AWS account owners, AWS Organizations management account owners, and AWS Identity and Access Management (IAM) users with the appropriate permissions can access the Billing and Cost Management console for an account. Regardless of whether you use cost allocation tagging, there's no change to how much you're billed. Whether you use cost allocation tags has no impact on the functionality of your AWS Marketplace software products.

Vendor-metered tags

AWS Marketplace products with vendor metering (including AMI, container, and SaaS products) may have tags provided by the software vendor. These tags are cost-allocation tags that help you understand your AWS Marketplace resource usage across vendor-provided metrics.

Some things to remember when you use vendor-metered tags include the following:

- Find vendor-metered tags in the Billing and Cost Management console (available at https://console.aws.amazon.com/billing/home) by choosing **Cost allocation tags**, and then the **AWS-generated cost allocation tags** tab.
- Vendor-metered tag key names start with *aws:marketplace:isv:…* to make them easier to find.
- Before you can use vendor-metered tags to track your usage as cost allocation tags, you must activate them in the Billing and Cost Management console.

Related topics

For more information, see the following topics:

- Using Cost Allocation Tags in the *AWS Billing and Cost Management User Guide*
- Activating the AWS-Generated Cost Allocation Tags in the *AWS Billing and Cost Management User Guide*

Private marketplaces

A private marketplace controls which products users in your AWS account, such as business users and engineering teams, can procure from AWS Marketplace. It is built on top of AWS Marketplace, and enables your administrators to create and customize curated digital catalogs of approved independent software vendors (ISVs) and products that conform to their in-house policies. Users in your AWS account can find, buy, and deploy approved products from your private marketplace, and ensure that all available products comply with your organization's policies and standards.

Your private marketplace is shared across your organization. With AWS Organizations, you can create a series of accounts linked for permissions and payments. You can create one or more private marketplace experiences that are associated with one or more accounts in your organization, each with its own set of approved products. Your administrators can also apply company branding to each private marketplace experience with your company or team's logo, messaging, and color scheme.

A private marketplace provides you with a broad catalog of products available in AWS Marketplace to choose from, in addition to fine-grained control of those products.

This section describes using private marketplace as a product purchaser. For information about managing private marketplaces as an administrator, see Creating and managing a private marketplace (p. 37).

Notes

- You can't add desktop products (p. 19) to a private marketplace.
- You can add private products that have been shared with you (via a private offer) to a private marketplace. For more information, see Subscribing to a private product in a private marketplace (p. 37).
- In a private marketplace, customers are automatically entitled to any products whose EULAs are governed by the AWS Customer Agreement or other agreement with AWS governing use of AWS services. Customers are already entitled to these products by default; therefore, they are not included in the list of products that you approved within your private marketplace. Customers can use AWS Service Catalog to manage the deployment of these products.

Viewing product detail pages

Users can only subscribe to products you have allowed in the private marketplace that governs the account. They can browse and see the detail page for any product, but subscription is enabled only for products you have added to your private marketplace. If a product is not currently in your private marketplace, the user sees a red banner at the top of the page, noting that the product is not approved for procurement in AWS Marketplace.

If software requests are enabled, users can choose **Create request** on the product details page. When users choose **Create request**, they submit a request to the administrator to make the product available on your private marketplace. For more information about this feature, see Managing user requests (p. 40).

Subscribing to a product in a private marketplace

To subscribe to a product in your private marketplace as a user, navigate to the product's details page and choose **Continue**. This redirects you to the product's subscription page. On the subscription page, you can make your configuration selections, and then choose **Subscribe**.

If the product is not approved in your private marketplace, **Subscribe** isn't available. A red banner at the top of the page indicates that the product is not currently approved for procurement. If software requests are enabled, you can choose **Create request** to submit a request to your administrator requesting that the product be added to your private marketplace.

Subscribing to a private product in a private marketplace

Some products are not publicly available to browse in AWS Marketplace. These products can only be seen when you are given a private offer from the seller. However, you can only subscribe if your private marketplace administrator first adds the product to your private marketplace. Because of this, the private offer must be extended to both your AWS account and the account that includes your organization's private marketplace administrator. After the private offer has been extended to both the user account and the administrator's account, the private marketplace administrator can add the product to your private marketplace. After the product has been approved, you can subscribe to the product like any other private offer.

Requesting a product be added to your private marketplace

As a user, you can request that your administrator add a product that is not in your private marketplace. To make a request, navigate to the product's details page, choose **Create request**, enter a request to your administrator that the product be added to your private marketplace, and then submit your request. To track your request status, on the left dropdown menu, choose **Your Private Marketplace Requests**.

Creating and managing a private marketplace

To create and manage a private marketplace, you must have the AWS Identity and Access Management (IAM) permissions in the AWSPrivateMarketplaceAdminFullAccess IAM policy. For more information about applying this policy to IAM users, groups, and roles, see the section called “Creating a private marketplace administrator” (p. 78).

This section includes tasks that you can complete as a private marketplace administrator through the AWS Marketplace website. You can also manage private marketplaces using the AWS Marketplace Catalog API. For more information, see Working with a private marketplace in the *AWS Marketplace Catalog API Reference*.

Creating a private marketplace experience

Your private marketplace is made up of one or more private marketplace experiences. Each experience is associated with one or more accounts in your organization (if your AWS account is not a member of an organization, then you have one private marketplace experience associated with one account). To create your private marketplace, navigate to Private Marketplace, select the **Experiences** page on the left, and choose **Create experience**.

Note
If your AWS account is part of an organization, then you must create the first private marketplace experience from the management account of your organization. After it is created,

you can manage the experience, or create other experiences from any account that has the correct IAM permissions.

After you have created your private marketplace, you can return to the private marketplace administration page by selecting **Your Private Marketplace** from the **Hello, <user name>** dropdown in the top right of any AWS Marketplace page.

Your private marketplace experience is created with no approved products, no branding elements, and is associated with no accounts in your organization. It is not live by default. The following topics describe managing your private marketplace experience, including enabling it.

Adding products to your private marketplace experience

To add products to a private marketplace experience

1. From the **Private Marketplace** administrator's page, select **Experiences** in the left navigation pane. Then, on the **Products** tab, choose **All AWS Marketplace products**. You can search by product name or seller name.
2. Select the check box next to each product to add to your private marketplace and then choose **Add to Private Marketplace**.

   Note
   You can also add a product directly from the product details page by choosing the **Add to Private Marketplace** button on the red banner. If the red banner is not on the product's detail page, the product is already in your private marketplace.

You can also add multiple products to multiple experiences at one time by choosing **Bulk add/remove products** from the left navigation pane.

Verifying products in your private marketplace experience

To verify a product is approved in your private marketplace experience

1. From the **Private Marketplace** administrator's page, select **Experiences** in the left navigation pane.
2. Choose **Approved products**. All approved products display in the approved list.

   Note
   If you are using an account that has been associated with the experience you are editing, and the experience is enabled, then you can also view the products directly in the AWS Marketplace console (https://console.aws.amazon.com/marketplace). All products in any search results show an *approved for procurement* badge if they are part of your private marketplace.

Customizing your private marketplace experience

On the **Private Marketplace** administrator's page, select **Experiences** in the left navigation pane, and then choose the **Profile** tab to configure your organization's private marketplace profile. You can add a logo, add a title, and customize the user interface to use your organization's color scheme. Instructions to customize your private marketplace are available on the **Profile** page.

Adding accounts to the private marketplace experience

A single private marketplace experience can govern one or more accounts in your organization. To manage this, you can create account groups and associate them with a private marketplace experience.

An account group is a list of accounts that you want to work with the same experience. To create an account group, from the **AWS Private Marketplace** administrator's page, select **Account groups** in the left navigation pane. Choose **Create account group**, and enter the name, description, and list of account IDs for the accounts you want to be in the group. Select a private marketplace experience to associate the account group with.

> **Note**
> Accounts in organizations are hierarchical. If you add an account to an account group, its child accounts will be in the account group by default. You can override this by putting them into another account group that is associated with a different private marketplace experience.

To create a single account group for all accounts in your organization, you can simply add the root account ID.

> **Note**
> Private marketplace administrators who created a private marketplace prior to January 2021 have a default account group that includes only their organization management account as a member. This applies to all accounts. Use the directions above to create additional account groups for other accounts in your organization.

An account may only be in a single account group.

Configuring your private marketplace

After you are satisfied with the experience's product list, the marketplace's branding settings, and the associated account groups, then you can make your private marketplace live. From the **AWS Private Marketplace** administrator's page, select **Experience** in the left navigation pane, then select the experience you want to enable. On the **Settings** tab, you can change the private marketplace status between **Live** (enabled) and **Not live** (disabled).

You can also choose to allow users to submit software requests with **Software requests**. If software requests are **On** (enabled), end users can choose **Create request** on the product details page to submit a request to the administrator to make the product available on your private marketplace. Software requests are enabled by default, and the setting can only be modified while the private marketplace is enabled.

When your private marketplace is live, end users can buy only the products that you have approved. When your private marketplace is disabled, you retain the list of products. However, disabling a private marketplace removes the restriction from users in your AWS Organizations organization. As a result, they can subscribe to any products in the public AWS Marketplace.

Making a private marketplace live does not disrupt active Amazon Machine Images (AMIs) running on Amazon Elastic Compute Cloud (Amazon EC2) instances. As a best practice, ensure that all AWS Marketplace products currently in use across your organization are included in your private marketplace. It's also a best practice to have a plan in place to discontinue use of unapproved products before making the private marketplace live. After the private marketplace is live, all new subscriptions or renewals are governed by the products approved in the private marketplace catalog.

> **Warning**
> Existing product usage may be disrupted when enabling your private marketplace, if those products are not included in the private marketplace. Users can't subscribe to a product that isn't in your private marketplace, even to replace or update an existing product.

Working with private products

Some products are not publicly available to browse in AWS Marketplace. These products can only be seen when you are given a private offer from the seller. The private offer from the seller includes a link to the product. You can add the product to the private marketplace from the banner at the top of the page.

> **Note**
> If you want to subscribe to a private product from a different account in your organization, the seller must include both your AWS account (to add the product to the private marketplace) and the user's account (to subscribe to the product) in the private offer.

To remove a private product from your private marketplace, you must contact AWS Marketplace Support.

Managing user requests

You can allow users to submit requests for products to be added to their private marketplace catalog with the software request feature. To do so, navigate to the administrator's page for your private marketplace, select **Experiences** in the left navigation pane, and choose the experience you want to manage. From the **Products** tab, choose **Pending requests**. From here you can review requests your users have made for products to be added to their private marketplace catalog.

You can add any number of requested products from this page by first selecting the check box next to the name of each requested product, and then choosing **Add to Private Marketplace**. Similarly, you can also decline one or more selected requests by choosing **Decline**. To view more information about a product (or its software request), choose **View details** in the **Details** column for that request.

When you decline a product request, you can add a reason and prevent future requests (block) for this product. Blocking a product won't prevent you from adding the product to your private marketplace, but it does prevent your users from requesting the product.

Private offers

The AWS Marketplace seller private offer feature enables you to receive product pricing from a seller that isn't publicly available. You negotiate pricing and terms with the seller, and the seller creates a private offer for the AWS account that you designate. You accept the private offer and start receiving the negotiated price and terms of use.

Each private offer has pricing and licensing terms specifically offered to your account. The seller of the product extends a private offer to you, and the offer has a set expiration date. If you don't accept the private offer by the expiration date, depending on the type of product the private offer is for, you're either automatically moved to the product's public offer or no longer subscribed to the product.

If you're using the consolidated billing feature in AWS Organizations, you can accept the private offer from either the organization's management account or from a member account. If you accept from the management account, the private offer is shared to all member accounts in the organization. Member accounts that were previously subscribed to the product automatically accept the private offer's pricing. Member accounts that weren't previously subscribed to the product must accept the private offer to be able to deploy the product.

For more information on consolidated billing, see Consolidated Billing for Organizations in the *AWS Billing and Cost Management User Guide*. The following are key points to remember as you start using your private offers.

- AWS Marketplace buyers can access third-party financing services for private offers. For more information, see Customer financing is now available in AWS Marketplace.
- There is no difference in the software product you purchase using a private offer. The software that you purchase using a private offer behaves the same as it would if you purchased the software without a private offer.
- Products subscriptions you purchase with a private offer show up like any other AWS Marketplace product in your monthly bill. You can use detailed billing to view your usage for each of your AWS Marketplace-purchased products. Each of your private offers has a line item corresponding to each kind of usage.
- Subscribing to a private offer doesn't require launching a new instance of the software. Accepting the private offer modifies the price to correspond to your private offer price. If a product offers 1-click launch, you can deploy a new instance of the software. If a product defaults to 1-click launch, you can accept a private offer without launching a new instance. To launch without deploying a new instance, choose **Manual Launch** on the fulfillment page. You can use the Amazon Elastic Compute Cloud console to deploy additional instances, just as you would for other AWS Marketplace products.
- When a seller extends a private offer to you, you receive confirmation on the account the seller included in a private offer. Private offers are linked to the specific software buyer's account listed. The software seller creates the private offer for the account that you specify. Each private offer can be made to up to 25 accounts.
- When you accept a private offer, it becomes an *agreement* (also known as *contract* or *subscription*) between you and the seller.
- Sellers may offer to upgrade or renew your purchase of an SaaS contract or SaaS contract with consumption product. For example, a seller can create a new private offer to grant new entitlements, offer pricing discounts, adjust payment schedules, or change the end user license agreement (EULA) to use standardized license terms.

  These renewals or upgrades are changes to the original private offer that you accepted, and you use the same process for accepting them. If you accept the new upgrade or renewal private offer, the new agreement terms take effect immediately, without any break in software service. Any previous terms or remaining scheduled payments are cancelled and replaced by this new agreement's terms.
- You can review all of your annual software subscriptions in AWS Marketplace under **Your Software**. If an annual subscription is purchased by one account using AWS Organizations for consolidated

billing, it is shared across the entire linked account family. If the purchasing account doesn't have any running instances, the annual subscription is counted toward the usage in another linked account running that software. For more information about annual subscriptions, see the section called “AMI subscriptions” (p. 22).

- When a private offer expires, you can't subscribe to it. However, you can contact the seller and ask them to create a new private offer for you. The seller also has the option of authorizing AWS Marketplace to extend the offer. If you're interested in trying to get the expiration date extended, contact <mpcustdesk@amazon.com>.

Product types eligible for private offers

You can get private offers for the following product types.

Offer type	Description
Data products	For more information, see Accepting a Private Offer in the *AWS Data Exchange User Guide*.
SaaS contract	With a software as a service (SaaS) contract, you can commit to upfront payment for your expected usage of a SaaS product, or negotiate a flexible payment schedule with the seller. Contract durations are one-month, one-year, two-year, or three-year terms, or select a custom duration in months, up to 60 months. If you commit to an upfront payment, you are billed in advance for the use of the product software. If the seller offers a flexible payment schedule, you are billed along the payment schedule dates at the amounts listed on the private offer. The seller may also include negotiated pay-as-you-go pricing for usage above your contracted usage.
SaaS subscription	With a SaaS subscription, you agree to a price for use of a product. The seller tracks and reports your usage to AWS Marketplace, and you're billed for what you use.
AMI hourly	With Amazon Machine Image (AMI) hourly, you negotiate an hourly rate for using an AMI, rounded up to the nearest hour.
AMI annual	With AMI annual, you negotiate the hourly and total contract duration prices with upfront payment, or flexible payment schedule over any custom contract duration of up to three years, and specified number of licenses for the AMI. If you commit to an upfront payment, you are billed in advance for the use of the AMI. If the ISV offers a flexible payment schedule, you are billed along the payment schedule dates at the amounts listed on the private offer.

Offer type	Description
Container products	With container products, you negotiate hourly or annual pricing for the container products that you use, by pod, task, or custom unit, matching the product that you are purchasing. Container product private offers match AMI product private offers.
Professional services	All professional services offers are private offers. You must work with the buyer to create the private offer. See Professional services products (p. 20) for more information.

Preparing to accept a private offer

When a typical private offer is negotiated, you pay the entire amount of the offer when you accept it, unless you are using third-party financing. With third-party financing, the financier pays the contract on your behalf and invoices you based on the agreed payment schedule. Before you accept a private offer, verify the billing structure for your company, your method of payment for AWS billing, and your tax settings.

Verifying your AWS Billing and Cost Management preferences

Billing and Cost Management is the service that you use to pay your AWS bill, monitor your usage, and budget your costs. You can use the consolidated billing feature in AWS Organizations to consolidate billing and payment for multiple accounts or multiple Amazon Internet Services Pvt. Ltd (AISPL) accounts. Every organization in AWS Organizations has a management account that pays the charges of all the member accounts. The management account is called a payer account, and the member account is called a linked account. Before negotiating a private offer, verify how your company pays their AWS bill and which AWS account the private offer is made to.

Verifying your payment method

Before accepting a private offer, verify that your payment method supports paying the entire cost of the private offer. To verify your payment method, open the Billing and Cost Management console at https://console.aws.amazon.com/billing/.

> **Note**
> If the private offer is a SaaS or AMI contract with a flexible payment schedule, you must have invoicing in place before you accept the offer.

Verifying your tax settings

If your company qualifies for a tax exemption, verify your tax settings. To view or modify your tax settings, sign in to the AWS Management Console and, in your account settings, view the tax settings. For more information on tax registration, see How do I add or update my tax registration number or business legal address for my AWS account?.

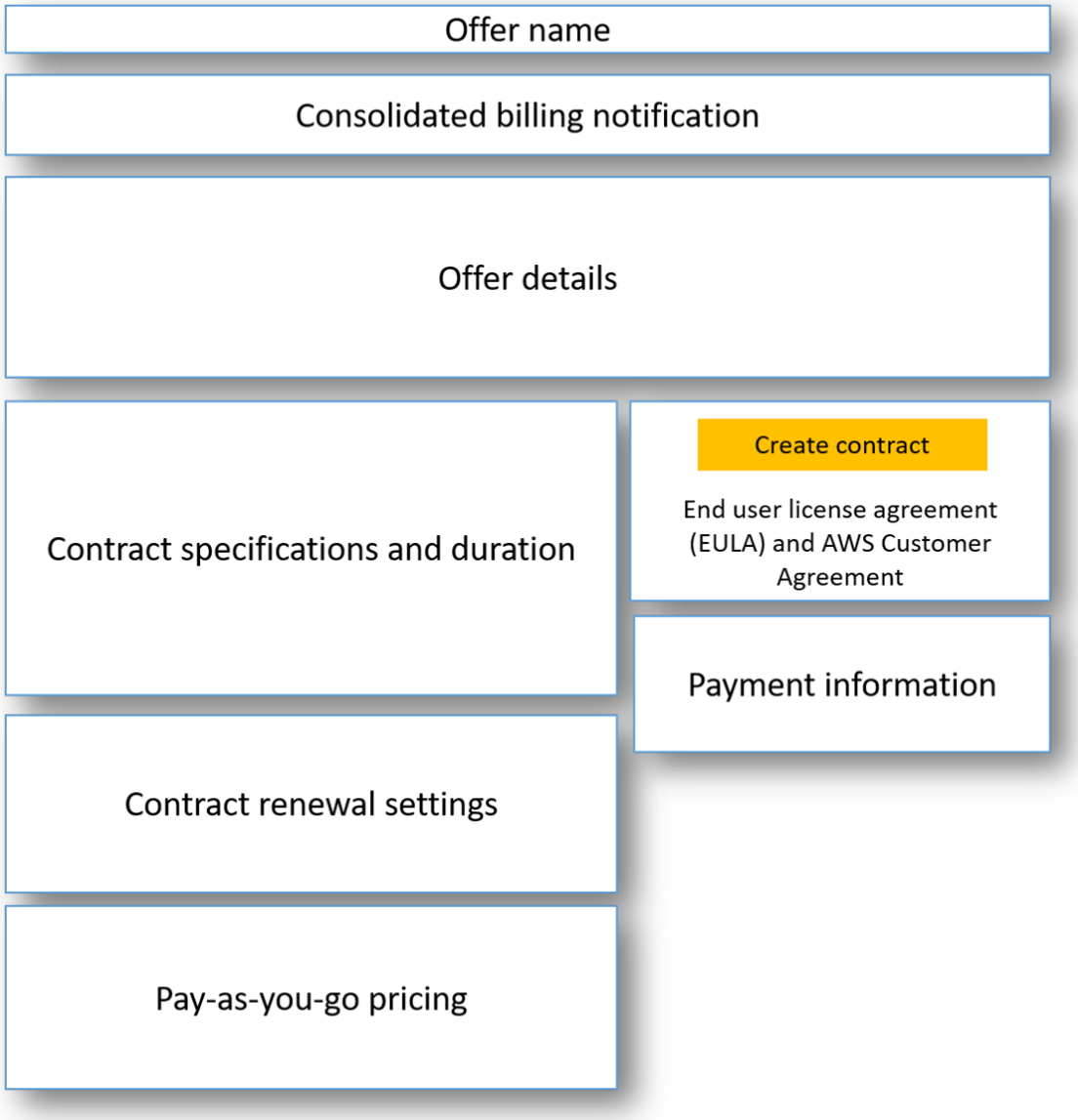
Viewing and subscribing to a private offer

With all private offers, you view and accept the offer by logging in to AWS Marketplace and navigating to the offer page for the product. To view the offer page, you can either:

- **Use the link the seller provided** – The seller might have sent you a link that takes you directly to the private offer. If so, use that link to directly access the private offer.
- **Navigate to the product page** – Sign in to AWS Marketplace and navigate to the product page for the product. During the subscription process, you see a banner at the top of the page showing the private offer, offer ID, and expiration for the offer. If you have more than one private offer for that product, each offer appears under **Offer name**.

Subscribing to a SaaS private offer

To navigate to the private offer page, either follow the link that the seller sent you or navigate to the product's page in AWS Marketplace. The panes and configuration options available for a SaaS private offer depend on the contract that you negotiate. The following image shows the private offer page layout and brief description of each of the areas that you might negotiate with the seller.



Pane	Description
Offer name	This is the name that the seller gave your private offer when they created it.
Consolidated billing notification	This notification appears if you're using consolidated billing with your AWS accounts.
Offer details	If you have one or more offers for this product, they appear here. Additional information includes the seller name, offer ID, and offer expiration date. The offer expiration date is how long the offer is valid for. If you don't accept the offer

Pane	Description
	by the expiration date, the offer is no longer available to you.
Contract specification and duration	This pane shows the duration of the offer and the dimensions that define the offer. The dimensions describe how the usage is measured and the duration how long the negotiated pricing is in effect: for example, 5 GB/day for 12 months or $0.01 per user per hour. If the private offer is a contract, you pay for an agreed-to amount of usage over the duration of the contract. If the private offer is a subscription, you pay for your measured usage at the agreed-to rate.
Contract renewal settings	You can't set private offers to be renewed automatically. For private offers on SaaS products, this pane always indicates that there is no renewal for this offer.
Pay-as-you-go pricing	If you negotiate pricing for product usage beyond what is defined in your private offer, the specifications for how much additional usage costs appear here. For example, if you agreed to a SaaS contract for data storage of 5 GB/day for 12 months and you use 10 GB/day, the first 5 GB fall under the contract. The additional 5 GB/day are charged at the pay-as-you-go price. With SaaS subscriptions, you have an agreed-to rate for however much you use during the duration of your contract.
End user license agreement (EULA) and contract creation button	This is where you can view the license agreement that the seller uploaded for this private offer. This is also where you accept the contract after you have viewed all of the private offer specifications and are ready to enter into the contract.
Payment information	This pane describes when payment is due and, if you negotiated a payment schedule, the date and times when payment is due.

Important
Any pane that doesn't appear isn't a negotiated part of the private offer.

To accept the private offer

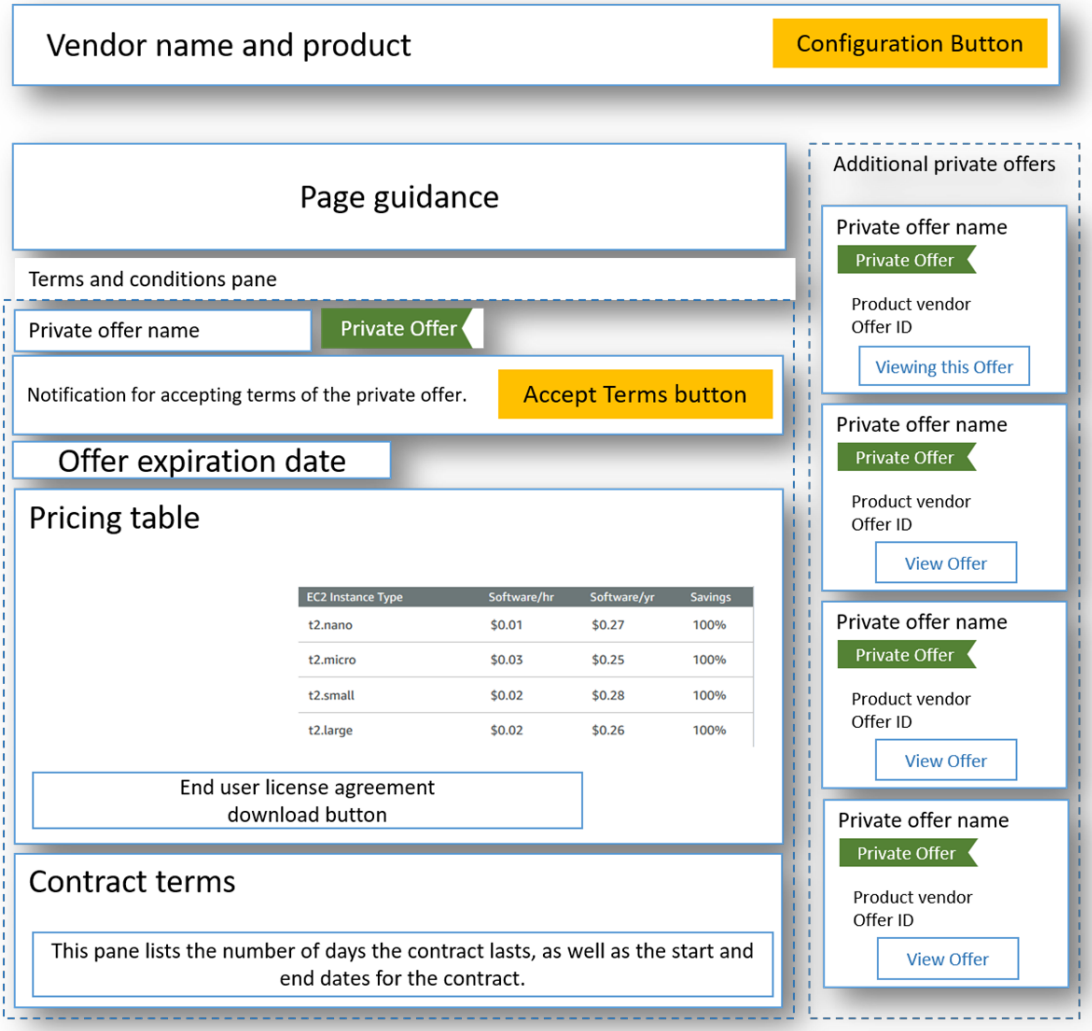
1. In the offer details pane, verify that you choose the correct private offer. You might have multiple offers for the product.
2. In the contract specification and duration pane, verify that the contract duration and contract details are what you negotiated. If not, verify that you have selected the correct private offer or contact the seller who created the offer.
3. If you negotiated pay-as-you-go pricing, there should be a pane with information that describes the terms that you negotiated. Verify the information, or if it's missing (and you expect it), contact the seller.

4. In the payment information pane, verify the payment information. If you negotiated a flexible payment schedule, the payment dates and amounts are listed. If you didn't, the total amount of the contract is billed when you accept the offer.
5. In the EULA and contract creation pane, validate that the EULA is the one you negotiated with the seller. After you review all of the terms and conditions for the contract, choose **Create contract** to accept the offer.

After you accept the offer, a confirmation page opens, indicating that you successfully subscribed to the product. Choose **Set Up Your Account** to be redirected to the seller's page and finish configuring your account on the seller's website.

Subscribing to an AMI private offer

The panes and configuration options available for your AMI private offer depend on the contract that you negotiate. The following image shows the private offer page layout for AMI private offers and a brief description of each of the areas that you might negotiate with the product vendor.



Pane	Description
Vendor name and product	This is the name of the vendor and the product that the private offer is for. On the right is the configuration button for the product. The **Configuration** button is dimmed until you accept the terms of the private offer.
Page guidance	This area has guidance for completing the tasks on this page and accepting the private offer.
Terms and conditions	This pane has the following key pieces of information: • In the upper left is the name of the private offer and a flag indicating that this is a private offer. • Below that is a notification for accepting the terms of the private offer and the button that you use to accept the private offer. • Below that is the offer expiration date, as well as the instance pricing that you negotiated. • Next is the end user license agreement (EULA). You can download it or view it on your screen.
Contract terms	This pane shows the number of days that the contract lasts and the start and end date of the contract.
Additional private offers	On the right are thumbnails of any other private offers that you have from this vendor for this product.

Important
The **Configuration** button is dimmed until you review the contents of the page and choose **Accept Terms**.

After you have reviewed and agreed with all of the details for your private offer, choose **Accept Terms**. Choose **Continue to Configuration** to accept the private offer and continue to the configuration process for your AMI.

Subscribing to an AMI private offer

You must accept the private offer on the AWS Marketplace website. You can't accept it on the AWS Marketplace console or the Amazon EC2 console.

To accept the private offer

1. Verify that you're viewing the correct private offer. The vendor can create multiple private offers to you for their product. Any additional private offers appear in the additional private offers pane. Validate that the offer that you want to accept appears as **Viewing This Offer**.
2. Verify that the offer expiration date and the pricing information are what you negotiated for the private offer. If they aren't, verify that you're viewing the correct private offer.
3. Download the EULA and verify that it's what you negotiated for the private offer.
4. In the contract terms pane, verify that the terms for the private offer are what you negotiated.

5. After you have verified the details for the private offer, in the terms and conditions pane, choose **Accept Terms**. When you do so, you don't incur any charges. Charges for AMI usage are consumption-based, so you're billed as you use the AMI.
6. To accept the private offer, choose **Continue to Subscribe**. A message appears, stating that your request is being processed.

When you're ready to configure the AMI, choose **Continue to Configuration**. You must complete the subscription process for each use of the product.

Subscribing to an annual AMI private offer

You must accept the private offer on the AWS Marketplace website. You can't accept it on the AWS Marketplace console or the Amazon EC2 console.

> **Note**
> The process to accept a private offer with a flexible payment schedule uses this process. The schedule is presented as part of the review and acceptance process.

To accept the annual private offer

1. Verify that you're viewing the correct private offer. The vendor can create multiple private offers to you for their product. Any additional private offers appear in the additional private offers pane. Validate that the offer that you want to accept appears as **Viewing This Offer**.

   > **Note**
   > In many cases, the payer account isn't the account that uses the product. We recommend that you launch the product manually rather than selecting the one-click option if you accept the offer using the payer account.
2. Verify that the offer expiration date and the pricing information are what you negotiated for the private offer. If they aren't, verify that you're viewing the correct private offer.
3. Download the EULA and verify that it's what you negotiated for the private offer.
4. In the contract terms pane, verify that the terms for the private offer are what you negotiated.
5. After you have verified the details for the private offer, in the terms and conditions pane, choose **Accept Terms**. When you do so, you don't incur any charges. Charges for AMI usage are consumption-based, so you're billed as you use the AMI.
6. Choose **View options**.
7. In the **Annual License** pane, for **Instance Type**, choose the instance type that you want. For **Number of subscriptions**, enter the number of subscriptions that you want to purchase and then choose **Add**.

   > **Note**
   > Optionally, you can add additional instance types during this step.
8. The total prices of the contract appear in the upper-right portion of the screen. After you verify the information, choose **Purchase** to purchase the subscription.
9. In the **Confirm annual subscription purchase** dialog box, choose **Confirm order**.

When you're ready to configure the AMI, choose **Continue to Configuration**. You must complete the subscription process for each use of the product.

Subscribing to a custom duration or multi-year AMI private offer

You must accept the private offer on the AWS Marketplace website. You can't accept it on the You can't accept it on the AWS Marketplace console or the Amazon EC2 console.

To accept the annual private offer

1. Sign in to your AWS account the offer was made to and verify that you're viewing the correct private offer. The vendor can create multiple private offers to you for their product. Any additional private offers appear in the additional private offers pane. Check that the offer that you want to accept appears under **Your Current Terms**.

   Note
   In many cases, the payer account isn't the account that uses the product. We recommend that if you accept the offer using the payer account, you launch the product manually rather than choosing the one-click option.
2. Verify that the offer details are what you negotiated for the private offer, and then choose **Accept Terms**. If they aren't, verify that you're viewing the correct private offer.
3. On the **Subscribe to this software** page, under **Instance type**, choose from the list of available instance types. Under **Quantity**, choose the number of licenses.
4. Review your selections, and when you are satisfied, choose **Create Contract**, and then choose **Confirm**.

When you're ready to configure the AMI, choose **Continue to Configuration**. You must complete the subscription process for each use of the product.

Modifying or unsubscribing from a private offer

You can update from standard subscriptions to private offers, and you can also modify certain existing private offers. The process varies based on the agreement in place. If you have a contract with a flexible payment schedule, you can't modify it because of the established invoicing of the payment schedule.

For many subscriptions, when you shift from public pricing to a private offer, you negotiate the offer with the ISV or your channel partner. After you accept the private offer, your related existing subscription or subscriptions automatically move to the private offer pricing model. This doesn't require any further action from you. Use the following guidance to identify your scenario and the steps to start receiving the pricing for your private offer.

Changing from public to private offer pricing

After you accept the private offer, no further action is needed for the IAM user account that accepted the offer. They are switched to the pricing, terms, and conditions defined in the private offer. To switch to the pricing, terms, and conditions for the private offer, each linked IAM user account using the product must accept the private offer. Any IAM user account that starts using the product must also accept the private offer to get the pricing, terms, and conditions defined in the private offer.

Changing SaaS dimensions or adding more users

If you have a software as a service (SaaS) contract in place, you can change SaaS dimensions or add more users to an existing private offer. When you accept the updated private offer, the rates of the contract edits are prorated for the time left on the contract. After you accept the change to the contract, no further action is necessary. If you negotiated a flexible payment schedule, you can't change SaaS dimensions or add more users.

Changing from a SaaS subscription to a SaaS contract

To shift from a SaaS subscription to a SaaS contract, you must first unsubscribe from the SaaS subscription. Then you accept the private offer for the SaaS contract. To view your existing SaaS subscriptions, choose **Your Marketplace Software** in the upper-right corner of AWS Marketplace.

Changing from an existing SaaS or AMI contract to a new contract

If you have a SaaS or Amazon Machine Image (AMI) contract in place from a previous private offer and you want to accept a new private offer for the same product, you must do one of the following:

- Wait for the current contract to expire before accepting the new one
- Work with the product vendor and the AWS Marketplace customer support team to terminate your current contract
- Accept the private offer using a different AWS account from the one that has the contract

Changing from AMI hourly to AMI annual

When you move from an AMI hourly subscription to an AMI annual subscription, the subscription works similar to a voucher system. Each hour of AMI usage is offset by one unit in the AMI annual subscription. When you purchase the annual subscription through a private offer, all associated accounts that are subscribed to the product are automatically switched to the pricing negotiated in the private offer. Linked accounts that start a subscription after the private offer is in place must subscribe to the private offer when they subscribe.

> **Note**
> The annual licenses on your old offer are deactivated immediately upon acceptance of the terms of the new offer. Work with the ISV to discuss compensation for the old licenses and how to proceed forward with the new offer.

Changing from AMI annual to AMI hourly

When your annual subscription expires, any linked accounts subscribed to the product are automatically switched to the AMI hourly pricing. If an annual subscription is in place, the linked account can't switch to an hourly subscription for that product without canceling the subscription.

Sharing subscriptions in an organization

When you subscribe to products in AWS Marketplace, an agreement is created that grants you license to use those products. If your AWS account is a member of an organization, you can share that license for AMI, container, and machine learning products with the other accounts in that organization. You must set up license support in AWS Marketplace, and then share from within AWS License Manager.

> **Note**
> For more information about AWS Organizations, see the AWS Organizations User Guide.
> For more information about sharing licenses with your organization in AWS License Manager, see Granted licenses in the *AWS License Manager User Guide*. For a walkthrough of the license sharing experience, you can refer to this video, Distribute your AWS Marketplace License Entitlements (3:56).

The following topics outline the process of sharing the licenses across accounts.

Topics

Prerequisites for license sharing

Before you can share licenses in AWS Marketplace you must set up license sharing for your organization. Complete the following tasks to set up license sharing for your organization:

- Give AWS Marketplace permission to manage licenses on your behalf so that it can create the associated license grants when you purchase or share your licenses. For more information, see Service-linked roles for AWS Marketplace (p. 76).
- Set up AWS License Manager for first use. For more information, see Getting started with AWS License Manager in the *AWS License Manager User Guide*.

Viewing and sharing your licenses

AWS Marketplace automatically creates licenses for AMI, container, machine learning, and data products that you purchase. You can share those licenses with other accounts in your organization.

You manage and share licenses using AWS License Manager. However, you can use AWS Marketplace to view the licenses for products that you purchased from within AWS Marketplace.

To view licenses for your subscribed products

1. In AWS Marketplace, sign in and choose **Manage Subscriptions**.
2. You can view all licenses or view the license for a specific subscription.
   - To view all licenses
     - From the **Actions** menu, select **View Licenses** to view all AWS Marketplace managed licenses in the License Manager console.

- To view licenses for a single subscription

  a. Choose the card of the product that you want to view to go to its product details page.
  b. From the **Actions** menu, select **View License** to view the license for that product in the License Manager console.

Note
Subscriptions in AWS Marketplace have an **Access level** shown in the product details. Products with an **Agreement** level have a license that you can use and share with other accounts in your organization. Products with an **Entitlement** level are licenses that have been shared with your account—you can use these products, but you can't share them.
Only AMI, container, and machine learning products will have licences that can be shared.

From License Manager, you can share your license with other accounts in your organization. For more details about using License Manager with AWS managed licenses, see the Granted licenses and Seller issued licenses topics in the *AWS License Manager User Guide*.

Note
For products that are restricted to specific regions, an account you share your license with will only be able to activate the license if the account is within an allowed region.

Integrating AWS Marketplace with procurement systems

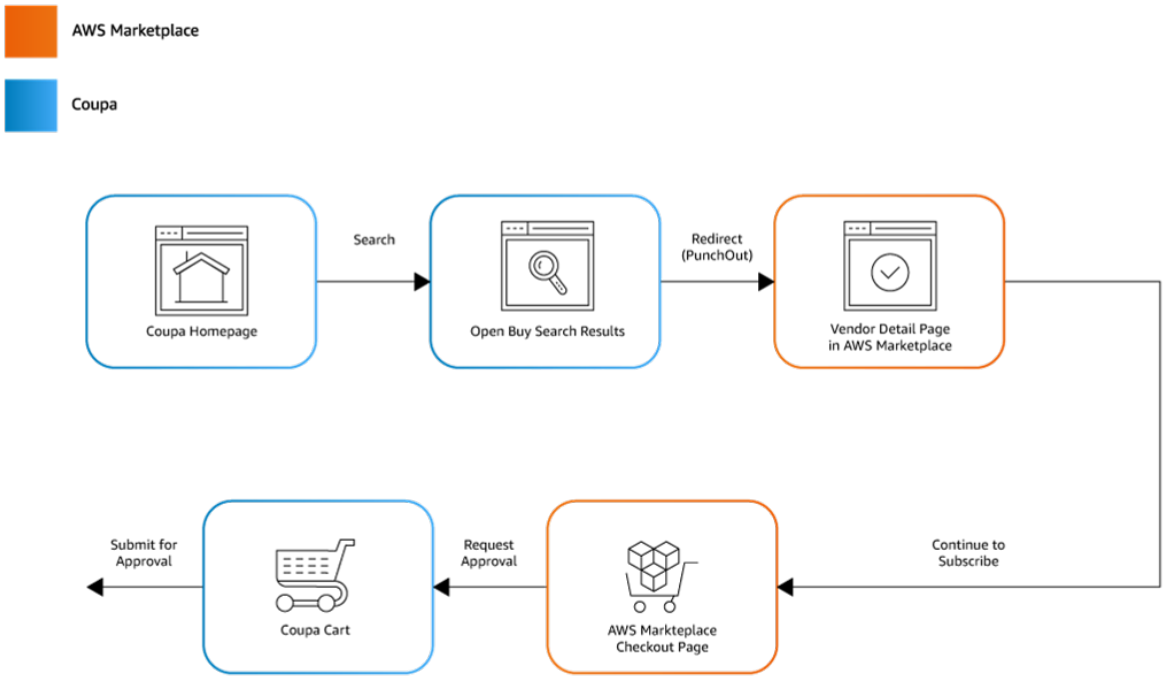
You can configure the integration of AWS Marketplace and your Coupa or SAP Ariba (beta) procurement software. After you complete the configuration, users in your organization can use your procurement software to search and request a subscription to AWS Marketplace products. After the subscription request is approved, the transaction is completed, and the user is notified that the software subscription is available. When the user signs in to AWS Marketplace, the software product is listed as a purchased subscription and is available for use.

Important
If you'd like to participate in our beta to integrate with SAP Ariba, contact us at `<awsmp-eprocurement@amazon.com>` and we'll help you configure a level 1 punchout.

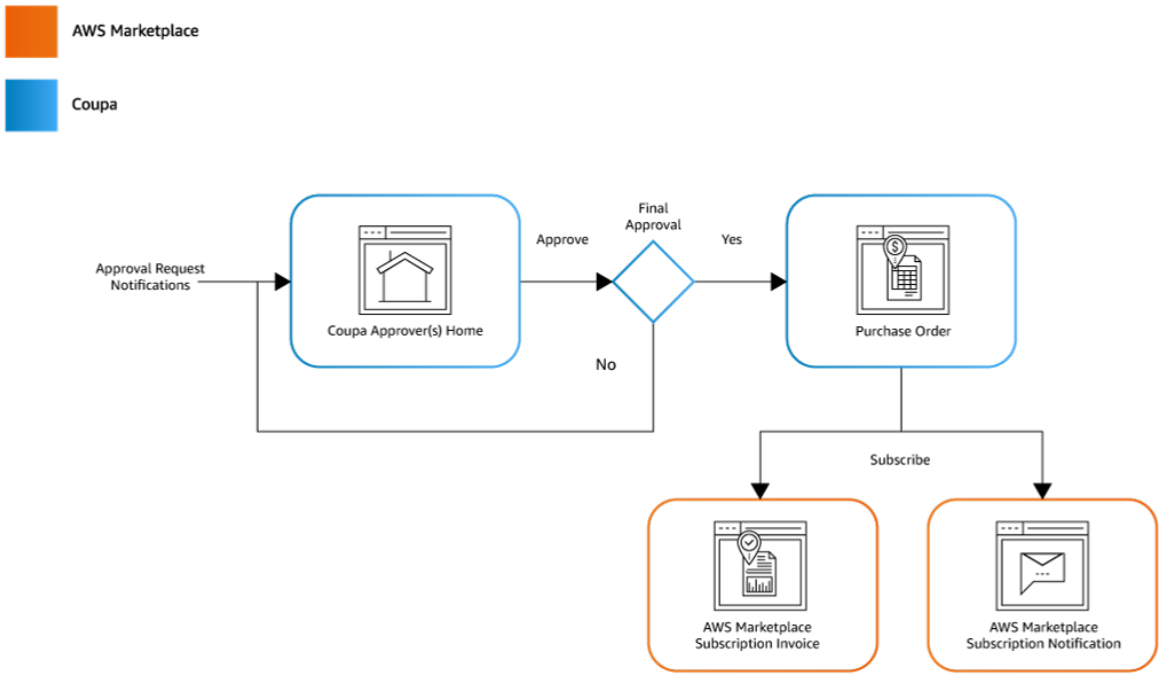
How Coupa integration works

You can configure Coupa procurement software to integrate with AWS Marketplace following the commerce extensible markup language (cXML) protocol. This integration creates an access point into a third party's catalog, or a *punchout*. Open Buy is a feature of Coupa that allows users to search AWS Marketplace, directly from Coupa. Coupa displays search results, and when the user chooses a result, they're redirected to AWS Marketplace. After an administrator configures the punchout integration, users of Coupa's procurement software can discover the AWS Marketplace catalog in the **Shop Online** section of their home page. They can also use the Coupa Open Buy feature and search the AWS Marketplace catalog directly from Coupa's search function.

If the user wants to see more detail about a product, they choose the product and are automatically redirected to AWS Marketplace. When the user wants to purchase a subscription, they complete the subscription request on AWS Marketplace. On the product's subscription page, instead of a button that completes the purchase, the user has a button to request approval. The request is sent back to a shopping cart in the Coupa system to complete the approval process. The following image shows the process for an Open Buy subscription request.



When the Coupa procurement system receives the request from AWS Marketplace, the procurement system starts a workflow to complete the approval process. After the request is approved, the procurement system's purchase order system automatically completes the transaction on AWS Marketplace and notifies the user that their subscription is ready to deploy. AWS Marketplace sends an email to the AWS account used to access AWS Marketplace that the subscription succeeded and the software is available through AWS Marketplace. The following image shows the approval process for an Open Buy subscription request.



Setting up Coupa integration

To configure the integration between AWS Marketplace and Coupa, you start the process in AWS Marketplace and complete it in Coupa. You use the information generated in AWS Marketplace to configure the Coupa punchout. To complete the configuration, the accounts that you use must meet the following requirements:

- The account used to complete the AWS Marketplace configuration must be the payer account and have the IAM permissions defined in the `AWSMarketplaceProcurementSystemAdminFullAccess` managed policy.
- The account used to complete the Coupa configuration must have Coupa administration access to set up a contract, supplier, and punchout.

Configuring IAM permissions

The following AWS Identity and Access Management (IAM) permissions are in the `AWSMarketplaceProcurementSystemAdminFullAccess` managed policy and are required to configure the integration between AWS Marketplace and Coupa.

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

We recommend that you use IAM managed permissions rather than manually configuring permissions. Using this approach is less prone to human error, and if the permissions change, the managed policy is updated. For more information about configuring and using IAM, see the following topics:

- For more information about managing IAM users and groups, see Identities (Users, Groups, and Roles) in the *IAM User Guide*
- For more information about managing IAM permissions and policies, see Controlling Access Using Policies in the *IAM User Guide*
- For a description of AWS Marketplace managed policies, see the section called “AWS managed policies for AWS Marketplace ” (p. 66)
- For more information about signing in as an IAM user, see the section called “Signing in as an IAM user” (p. 75).

Configuring AWS Marketplace

To configure AWS Marketplace to integrate with Coupa, navigate to **Manage procurement**. In the **Manage procurement systems** pane, enter a name and description for the punchout, and can also

configure integrated invoicing. You can also switch the integration to test mode so that users can't make valid subscriptions until you're ready. To configure the AWS Marketplace portion of the integration, complete the following procedure.

To configure AWS Marketplace for integrating with Coupa

1. From AWS Marketplace Manage Procurement Systems, under **Procurement systems**, choose **Set up Coupa integration**.
2. On the **Manage Coupa integration** page, under **Account information**, enter the name and description of your integration.

You use the information generated on this page to configure the punchout in your Coupa system. The configuration defaults to test mode being enabled. This helps you complete the configuration and enable the punchout in a planned manner.

You can also enable electronic invoicing from AWS Marketplace by entering a URL that you want the invoices delivered to. This is likely a URL for the Coupa system.

Configuring Coupa

To configure the integration with AWS Marketplace in your Coupa system, copy the information from the **Purchase information** pane of the **Manage Coupa integration** page in AWS Marketplace. Use this information to complete the steps in the following links and guide you through configuring your Coupa procurement system.

- Punchout Setup
- Configuring a Supplier for cXML Purchase Orders

AWS Marketplace includes the following United Nations standard products and services code (UNSPSC) codes for the software listings sent back to Coupa's cart:

- Software-as-a-service (SaaS) products: 81162000
- Application server products: 43232701
- Other software, such as containers, AWS WAF rules, and machine learning (ML) algorithms: 43230000

Free trials

Some products listed on AWS Marketplace offer free trials. The free trial enables you to try-before-you-buy software. Free trials are limited to a certain amount of free usage.

Using AWS free usage tier with AWS Marketplace

To help new Amazon Web Services (AWS) customers get started in the cloud, AWS introduced a free usage tier. The free tier can be used for anything you want to run in the cloud: launch new applications, test existing applications in the cloud, or simply gain hands-on experience with AWS. When the free usage period expires (or if the application use exceeds the free usage tier limits), you simply pay the standard, pay-as-you-go service rates. For more information, see AWS Free Tier.

AWS Free Tier customers are eligible to use free AWS Marketplace software for up to 750 hours of Amazon Elastic Compute Cloud (Amazon EC2) usage each month for one year. To get started, see AWS Marketplace.

Adding AWS Marketplace subscriptions to AWS Service Catalog

AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on Amazon Web Services (AWS). These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows you to centrally manage commonly deployed IT services. AWS Service Catalog helps you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

For more information, see Adding AWS Marketplace products to your portfolio in the *AWS Service Catalog Administrator Guide*.

Product reviews

AWS Marketplace wants buyers to get the information they need to make smart buying choices. As an AWS customer, you can submit written reviews for items listed in AWS Marketplace. We encourage you to share your opinions, both favorable and unfavorable.

Note
Data products don't support product reviews.

Guidelines

Anyone with an AWS Marketplace subscription to a product can create a review for it. Use the following guidelines for writing product reviews:

- *Include reasons* – The best reviews include not only whether you liked or disliked a product, but also why. You can discuss related products and how this item compares to them.
- *Be specific* – Focus on specific features of the product and your experience with it. For video reviews, write a brief introduction.
- *Be concise* – Written reviews must be at least 20 words and are limited to 5,000 words. The ideal length is 75–500 words.
- *Be sincere* – Your honest opinion about the product, positive or negative, is appreciated. Helpful information can inform our customers' buying decisions.
- *Be transparent* – If you received a free product in exchange for your review, clearly and conspicuously disclose that.

Restrictions

AWS reserves the right to remove reviews that include any of the following content.

- Objectional material, including:
  - Obscene or distasteful content
  - Profanity or spiteful remarks
  - Promotion of illegal or immoral conduct
- Promotional content, including:
  - Advertisements, promotional material, or repeated posts that make the same point
  - Sentiments by or on behalf of a person or company with a financial interest in the product or a directly competing product (including reviews by authors, publishers, manufacturers, or third-party merchants selling the product)
  - Reviews written for any form of compensation other than a free copy of the product, including reviews that are part of a paid publicity package
  - Reviews written by a customer without a verifiable subscription to the product
- Inappropriate content, including:
  - Content copied from others, including excessive quotations
  - Contact information or URLs external to Amazon.com
  - Details about availability or alternate ordering/shipping
  - Videos with watermarks

  - Comments on other reviews visible on the page, because page visibility is subject to change without notice
  - Foreign language content, unless there is a clear connection to the product
  - Text with formatting issues
- Off-topic information, including:
  - Feedback on the seller or your shipment experience
  - Feedback about typos or inaccuracies in our catalog or product description; instead, use the feedback form at the bottom of the product page

For questions about customer reviews, contact us.

Getting support

For general AWS Marketplace issues, contact us. For questions about the software you purchase through AWS Marketplace, contact the software seller.

Security on AWS Marketplace

We list software from high-quality sellers, and actively work to maintain the quality of our selection. Because every customer is different, our goal is to provide enough information about the products listed on AWS Marketplace so that customers can make good purchasing decisions.

Note
For information about security for data products from AWS Data Exchange, see Security in the *AWS Data Exchange User Guide*.
For information about security for sellers on AWS Marketplace, see AWS Marketplace Security in the *AWS Marketplace Seller Guide*.

Subscriber information shared with sellers

We may share your contact information with our sellers for the following reasons:

- If it is necessary for them to provide customer training and technical support.
- For software activation, configuration, and customization of content.
- Compensate their sales teams internally.

In addition, we may share information such as company name, full address and usage fees with sellers in order for sellers to compensate their sales teams. We may also share certain information with sellers to help them evaluate the effectiveness of their marketing campaigns. Sellers may use this information along with information that they already possess to determine rewards for their sales teams or usage for a particular buyer.

Otherwise, we generally do not share customer information with sellers, and any information shared is not personally identifiable, unless you have given us permission to share such information, or we believe that providing the information to sellers is necessary to comply with laws or regulations.

Control access to subscriptions

Use AWS Identity and Access Management (IAM) to create IAM users and assign them permissions to work with your subscriptions. This can include listing subscriptions, subscribing to product, and launching instances of subscribed software. Others can then log in to AWS Marketplace using the user name and password that you give them, and they have only the permissions that you assigned.

Working with subscriptions

If your organization is using IAM, your account owner probably set you up with user information that includes account credentials and a URL for logging in. The URL looks like `https://123456789012.signin.aws.amazon.com/console` but with a different number. After you have the URL and credentials, navigate to the login URL, log in using your credentials, and navigate to AWS Marketplace. The owner might have restricted the tasks that you can perform.

Controlling access to AWS Marketplace subscriptions

The recommended way to let other people in your organization manage subscriptions is to use AWS Identity and Access Management (IAM) to create users and groups. For example, if John should be allowed only to view your subscriptions, you can create an IAM user for him and add his IAM user to the read-only group. If John's role in your organization changes or he leaves the company, you can change the group that his IAM user belongs to, or you can change his user's settings in IAM.

Important
All of your users work on the same AWS Marketplace account. Any change that a user makes to manage a software subscription is global and applies to all of your users for that subscription.

Creating users

To allow people in your company to manage subscriptions, we recommend that you create an IAM user for each person. For more information, see IAM Users in the *IAM User Guide*. We also recommend you create a user name and password for yourself, even though you are the AWS account owner. It is a recommended best practice for everyone to work in AWS Marketplace as an IAM user, even the account owner. To learn how to create an IAM user for yourself that has administrative permissions, see Creating Your First IAM Admin User and Group. For more information about recommended practices for using IAM, see IAM Best Practices.

Creating groups for AWS Marketplace access and adding users to the groups

To create groups for assigning AWS Marketplace permissions

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose **Groups** and then choose **Create New Group**.
3. For **Group Name**, enter a name for the group, such as *MarketplaceReadOnly* or *MarketplaceFullAccess*, and choose **Next Step**.
4. On the **Attach Policy** page, select the check box next to one of the following policies:
   - To allow permissions only to view subscriptions (but not change them), choose **AWS MarketplaceRead-only**
   - To allow permissions to subscribe and unsubscribe, choose **AWSMarketplaceManageSubscriptions**
   - To allow complete control of your subscriptions, choose **AWSMarketplaceFullAccess**
5. Choose **Next Step**, and then choose **Create Group**.

To add users to the groups you just created

1. In the list of groups, choose the name of the group.
2. For **Users**, choose **Add Users to Group**.
3. Select the users to add to the group, and then choose **Add Users**.

Repeat the preceding steps to create more groups with different permissions and assign users to those groups.

You're not limited to the permissions in the AWS managed policies that are described here. You can use IAM to create policies with custom permissions and then add those policies to IAM groups. For more information, see Managing IAM Policies and Attaching a Policy to an IAM Group in the *IAM User Guide*.

AWS managed policies for AWS Marketplace

After creating users, we recommend that you create groups and apply AWS managed policies to provide basic AWS Marketplace permissions. Then, for any unique scenarios, you can create your own policies and apply them to the groups with the specific requirements for your scenario. The following basic AWS Marketplace managed policies are available to you to control who has which permissions:

- `AWSMarketplaceRead-only`
- `AWSMarketplaceManageSubscriptions`
- `AWSPrivateMarketplaceRequests`
- `AWSPrivateMarketplaceAdminFullAccess`
- `AWSMarketplaceFullAccess`

AWS Marketplace also provides specialized managed policies for specific scenarios. For a full list of AWS managed policies for AWS Marketplace buyers, as well as descriptions of what permissions they provide, see AWS managed policies for AWS Marketplace buyers (p. 66).

Permissions for working with License Manager

AWS Marketplace integrates with AWS License Manager to manage and share licenses for products that you subscribe to between accounts in your organization. To view the full details of your subscriptions in AWS Marketplace, a user must be able to list license information from AWS License Manager.

To make sure that your users have the permissions they need to see all the data about their AWS Marketplace products and subscriptions, add the following permission:

- license-manager:ListReceivedLicenses

For more information about setting permissions, see Managing IAM Policies in the *IAM User Guide*.

Additional resources

For more information about managing IAM users and groups, see Identities (Users, Groups, and Roles) in the *IAM User Guide*.

For more information about managing IAM permissions and policies, see Controlling Access Using Policies in the *IAM User Guide*.

For more information about managing IAM permissions and policies for data products in AWS Data Exchange, see Identity and Access Management in AWS Data Exchange in the *AWS Data Exchange User Guide*.

AWS managed policies for AWS Marketplace buyers

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your

team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

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

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

This section lists each of the policies used to manage buyer access to AWS Marketplace. For information about seller policies, see AWS managed policies for AWS Marketplace sellers in the *AWS Marketplace Seller Guide*.

Topics

AWS managed policy: AWSMarketplaceFullAccess

You can attach the `AWSMarketplaceFullAccess` policy to your IAM identities.

This policy grants administrative permissions that allow full access to AWS Marketplace and related services, both as a buyer and a seller. These permissions include the ability to subscribe and unsubscribe to AWS Marketplace software, manage AWS Marketplace software instances from the AWS Marketplace, creating and managing private marketplace in your account, as well as access to Amazon EC2, AWS CloudFormation, and Amazon EC2 Systems Manager.

Permissions details

```
{
    "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:UpdateDocumentDefaultVersion",
            "ssm:CreateDocument",
            "ssm:StartAutomationExecution",
            "ssm:ListDocuments",
            "ssm:UpdateDocument",
            "ssm:DescribeDocument",
            "sns:ListTopics",
            "sns:GetTopicAttributes",
            "sns:CreateTopic",
            "iam:GetRole",
            "iam:GetInstanceProfile",
            "iam:ListRoles",
            "iam:ListInstanceProfiles"
        ],
        "Resource": "*"
    },
    {
        "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",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

AWS managed policy: AWSMarketplaceImageBuildFullAccess

You can attach the `AWSMarketplaceImageBuildFullAccess` policy to your IAM identities.

This policy grants contributor permissions that allow full access to the AWS Marketplace private image build feature. In addition to creating private images, it also provides permisions to add tags to images, and to launch and terminate Amazon EC2 instances.

Permissions details

```
{
    "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",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:CreateDocument",
                "ssm:StartAutomationExecution",
                "ssm:ListDocuments",
                "ssm:UpdateDocument",
                "ssm:UpdateDocumentDefaultVersion",
                "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": [
                "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*"
            ]
        }
    ]
```

```
}
```

AWS managed policy: AWSMarketplaceLicenseManagementServiceRolePolicy

You can't attach AWSMarketplaceLicenseManagementServiceRolePolicy to your IAM entities. This policy is attached to a service-linked role that allows AWS Marketplace to perform actions on your behalf. For more information, see Service-linked roles for AWS Marketplace (p. 76).

This policy grants contributor permissions that allow AWS Marketplace to manage licenses on your behalf.

Permissions details

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

AWS managed policy: AWSMarketplaceManageSubscriptions

You can attach the `AWSMarketplaceManageSubscriptions` policy to your IAM identities.

This policy grants contributor permissions that allow subscribing and unsubscribing to AWS Marketplace products.

Permissions details

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

AWS managed policy: AWSMarketplaceProcurementSystemAdminFullAccess

You can attach the `AWSMarketplaceProcurementSystemAdminFullAccess` policy to your IAM identities.

This policy grants admin permissions that allow managing all aspects of an AWS Marketplace eProcurement integration, including listing the accounts in your organization. For more information about eProcurement integrations, see Integrating AWS Marketplace with procurement systems (p. 54) .

Permissions details

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

AWS managed policy: AWSMarketplaceRead-only

You can attach the `AWSMarketplaceRead-only` policy to your IAM identities.

This policy grants read-only permissions that allows viewing products and subscriptions for your account on AWS Marketplace, as well as viewing the Amazon EC2, AWS Identity and Access Management, and Amazon SNS resources in the account.

Permissions details

```
{
    "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"
            ]
        }
    ]
}
```

AWS managed policy: AWSPrivateMarketplaceAdminFullAccess

You can attach the `AWSPrivateMarketplaceAdminFullAccess` policy to your IAM identities.

This policy grants admin permissions that allow full access to manage private marketplaces in your account (or organization).

Permissions details

```
{
    "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:StartChangeSet",
                "aws-marketplace:ListChangeSets",
                "aws-marketplace:DescribeChangeSet",
                "aws-marketplace:CancelChangeSet"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS managed policy: AWSPrivateMarketplaceRequests

You can attach the `AWSPrivateMarketplaceRequests` policy to your IAM identities.

This policy grants contributor permissions that allow access to request products be added to your private marketplace, and to view those requests. These requests must be approved or denied by a private marketplace administrator.

Permissions details

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aws-marketplace:CreatePrivateMarketplaceRequests",
                "aws-marketplace:ListPrivateMarketplaceRequests",
                "aws-marketplace:DescribePrivateMarketplaceRequests"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Marketplace updates to AWS managed policies

View details about updates to AWS managed policies for AWS Marketplace since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Marketplace Document history (p. 79) page.

Change	Description	Date
AWSPrivateMarketplaceAdminFullAccess (p. 73) – Update to an existing policy	AWS Marketplace removed unused permissions in the `AWSPrivateMarketplaceAdminFullAccess` policy.	August 27, 2021
AWSMarketplaceFullAccess (p. 67) – Update to an existing policy	AWS Marketplace removed a duplicate	July 20, 2021

Change	Description	Date
	`ec2:DescribeAccountAttributes` permission from `AWSMarketplaceFullAccess` policy.	
AWS Marketplace started tracking changes	AWS Marketplace started tracking changes for its AWS managed policies.	April 20, 2021

Signing in as an IAM user

After you have created users in IAM, users can sign in with their own user names and passwords. To do so, they need to use a unique URL that is associated with your AWS account.

To get your account's unique sign-in URL

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Dashboard**.
3. Near the top of the content pane, find **IAM users sign-in link:** and take note of the sign-in link, which has a format like this:

   ```
   https://AWS_account_ID.signin.aws.amazon.com/console/
   ```

   Note
   If you want the URL for your sign-in page to contain your company name (or other friendly identifier) instead of your AWS account ID, you can create an alias for your account by choosing **Customize**. For more information, see Your AWS Account ID and Its Alias in the *IAM User Guide*.
4. Distribute this URL to the people at your company who can work with the AWS Marketplace, along with the user name and password that you created for each. Instruct them to use your account's unique sign-in URL to sign in before they access the AWS Marketplace.

As users work in AWS Marketplace, AWS enforces the appropriate permissions. For example, user John might belong to a group that has only read-only permissions to work with your subscriptions. When he signs in to AWS Marketplace, he can choose the **Your Software** link at the top of the page.

When John does this, a message tells him that he doesn't have permissions to manage software, as shown in the following image.

Finding the account number for customer support

If you or your users need to contact customer service, you need your AWS account number.

To get your AWS account number

1. Sign in to the AWS Management Console with your IAM user name.
2. In the top navigation bar, choose **Support** and then choose **Support Center**.

Your AWS account ID (account number) appears below the top navigation bar.

Service-linked roles for AWS Marketplace

AWS Marketplace uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to AWS Marketplace. Service-linked roles are predefined by AWS Marketplace and include all the permissions that the service requires to call other AWS services on your behalf.

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

To share your AWS Marketplace subscriptions to other accounts in your AWS organization with AWS License Manager, you must give AWS Marketplace permissions for each account you want to share with. Do this by using the **AWSServiceRoleForMarketplaceLicenseManagement** role. See Creating a service-linked role for AWS Marketplace (p. 77) for more details.

For information about other services that support service-linked roles, see AWS services that work with IAM, and look for the services with **Yes** in the **Service-linked roles** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for AWS Marketplace

AWS Marketplace uses the service-linked role named **AWSServiceRoleForMarketplaceLicenseManagement**. This role provides AWS Marketplace with permissions to create and manage licenses in AWS License Manager for the products that you subscribe to in AWS Marketplace.

This service-linked role trusts the following service to perform actions in License Manager on your behalf:

- `license-management.marketplace.amazonaws.com`

The role permissions policy allows AWS Marketplace to complete the following actions on the specified resources:

- Actions:
  - `"organizations:DescribeOrganization"`
  - `"license-manager:ListReceivedGrants"`
  - `"license-manager:ListDistributedGrants"`
  - `"license-manager:GetGrant"`
  - `"license-manager:CreateGrant"`
  - `"license-manager:CreateGrantVersion"`
  - `"license-manager:DeleteGrant"`
  - `"license-manager:AcceptGrant"`

- Resources:
  - All resources (`"*"`)

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating a service-linked role for AWS Marketplace

AWS Marketplace creates the service-linked role for you when you setup integration with AWS License Manager.

You can specify that AWS Marketplace create the service-linked role for all accounts in your organization at once, or you can create the service-linked role for one account at a time. The option to create service-linked roles across all accounts will only be available if your organization has **All features** enabled. For more details, see Enabling all features in your organization in the *AWS Organizations User Guide*.

To create service-linked roles across all accounts

1. In AWS Marketplace console, sign in and choose **Settings**.
2. In the **AWS Organizations integration** section, select **Create integration**.
3. On the **Create AWS Organizations integration** page, select **Enable trusted access across your organization**, then choose **Create integration**.

   Note
   This setting enables trust within AWS Organizations. As a result, in addition to the current action, future accounts that are added to the organization will have the service-linked role added automatically.

To create service-linked roles for the current account

1. In AWS Marketplace console, sign in and choose **Settings**.
2. In the **AWS Organizations integration** section, select **Create integration**.
3. On the **Create AWS Organizations integration** page, select **AWS Marketplace license management service-linked role for this Account**, then choose **Create integration** .

   Important
   If you choose to create the service-linked role only for the current account, it does not enable trusted access across your organization. You must repeat these steps for each account that wants to share (giving or receiving) licenses in AWS Marketplace. This includes accounts that are added to the organization in the future.

Editing a service-linked role for AWS Marketplace

AWS Marketplace doesn't allow you to edit the service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the *IAM User Guide*.

Deleting a Service-Linked Role for AWS Marketplace

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored

or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

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

To manually delete the service-linked role using IAM

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

Creating a private marketplace administrator

You can create an administrators group to manage your company's private marketplace (p. 36) settings. After the first private marketplace experience is created for your organization, administrators for the private marketplace can perform many tasks including the following:

- View and create experiences and account groups.
- Add products to private marketplace experiences.
- Remove products from private marketplace experiences.
- Configure the user interface of private marketplace experiences.
- Enable and disable private marketplace experiences.
- Call the AWS Marketplace Catalog API to manage private marketplace experiences programmatically.

> **Note**
> Creating the first private marketplace experience also enables private marketplaces in your organization. This is a one-time action. For accounts that are part of an organization, the initial experience creation must happen from the management account. For more information, see Creating a private marketplace experience (p. 37).

You grant AWS Identity and Access Management (IAM) permissions to administer your private marketplace by attaching the AWSPrivateMarketplaceAdminFullAccess policy to an IAM user, group, or role. We recommend using a group or role. For more information about recommended practices for using IAM, see IAM Best Practices.

To learn more about the permissions in the AWSPrivateMarketplaceAdminFullAccess policy, or to learn about other policies for use in AWS Marketplace, sign in to the AWS Management Console, and go to the IAM policies page. In the search box, enter **`Marketplace`** to find all of the policies that are associated with AWS Marketplace.

Document history

The following table describes the documentation for this release of the *AWS Marketplace Buyer Guide*.

update-history-change	update-history-description	update-history-date
Support for AMI aliases	AWS Marketplace supports using aliases for AMI IDs that can be used across regions.	September 8, 2021
Removed unused permissions in managed policy	Unused permissions from `AWSPrivateMarketplaceAdminFullAccess` AWS managed policy have been removed.	August 27, 2021
Support for sharing licenses through AWS License Manager	You can share licenses to products that you purchase with other accounts in your AWS organization.	December 3, 2020
AWS Marketplace supports professional services offerings	AWS Marketplace now supports purchasing professional services.	December 3, 2020
Support for preferred currency	You can pay for AWS Marketplace purchases using your preferred currency.	July 27, 2020
You can review and accept private offer upgrades and renewals	Sellers can provide upgrade and renewal private offers for SaaS contract and SaaS contract with consumption products that you can review and accept while on an existing agreement.	May 28, 2020
AWS Marketplace supports data products through AWS Data Exchange	You can now subscribe to AWS Data Exchange data products in AWS Marketplace.	November 13, 2019
AWS Marketplace supports paid hourly containers	AWS Marketplace now supports paid hourly containers running on Amazon Elastic Kubernetes Service (Amazon EKS).	September 25, 2019
Updated private offers on AWS Marketplace	Updated content to provide more information on accepting different types of private offers.	March 29, 2019
Updated Security on AWS Marketplace	Updated IAM policies information, restructured section for readability.	March 25, 2019
Added content for the private marketplace feature	Added content supporting the release of *Private Marketplace*.	November 27, 2018
Initial release of the user guide for buyers	Initial release of the *AWS Marketplace Buyer Guide*.	November 16, 2018

AWS glossary

For the latest AWS terminology, see the AWS glossary in the *AWS General Reference*.