
Amazon EKS

User Guide



Amazon EKS: User Guide

Copyright © 2023 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 Amazon EKS?	1
Features	1
Get started	1
Pricing	2
Common use cases	2
Architecture	3
Control plane	3
Compute	4
Deployment options	4
Getting started with Amazon EKS	6
Installing kubectl	6
Installing eksctl	13
Create your first cluster – eksctl	13
Prerequisites	13
Step 1: Create cluster and nodes	14
Step 2: View Kubernetes resources	15
Step 3: Delete cluster and nodes	16
Next steps	16
Create your first cluster – AWS Management Console	16
Prerequisites	17
Step 1: Create cluster	17
Step 2: Configure cluster communication	19
Step 3: Create nodes	19
Step 4: View resources	23
Step 5: Delete resources	23
Next steps	24
Clusters	25
Creating a cluster	25
Updating Kubernetes version	34
Update the Kubernetes version for your Amazon EKS cluster	34
Deleting a cluster	38
Configuring endpoint access	41
Modifying cluster endpoint access	42
Accessing a private only API server	46
Enabling secret encryption	46
Enabling Windows support	49
Enabling Windows support	50
Removing legacy Windows support	51
Disabling Windows support	52
Deploying Pods	52
Enabling legacy Windows support	53
Supporting higher Pod density on Windows nodes	58
Private cluster requirements	58
.....	59
Kubernetes versions	60
Available versions on standard support	61
Available versions on extended support	61
Amazon EKS Kubernetes release calendar	61
Amazon EKS version FAQs	62
Amazon extended support FAQs	63
Standard support versions	64
Platform versions	71
Kubernetes version 1.28	72
Kubernetes version 1.27	72

Kubernetes version 1.26	72
Kubernetes version 1.25	73
Kubernetes version 1.24	74
Kubernetes version 1.23	75
Autoscaling	75
Nodes	77
Managed node groups	81
Managed node groups concepts	81
Managed node group capacity types	83
Creating a managed node group	85
Updating a managed node group	91
Node taints on managed node groups	97
Customizing managed nodes with launch templates	98
Deleting a managed node group	107
Self-managed nodes	108
Amazon Linux	108
Bottlerocket	114
Windows	117
Updates	122
AWS Fargate	131
Fargate considerations	131
Getting started with Fargate	133
Fargate profile	136
Fargate Pod configuration	140
Fargate OS patching	142
Fargate metrics	143
Fargate logging	145
Instance types	152
Maximum Pods	154
Amazon EKS optimized AMIs	155
Docker shim deprecation	155
Amazon Linux	156
Bottlerocket	174
Ubuntu Linux	184
Windows	184
Storage	228
Amazon EBS CSI driver	228
Create an IAM role	228
Manage the Amazon EKS add-on	234
Deploy a sample application	239
CSI migration FAQ	241
Amazon EFS CSI driver	244
Creating an IAM role	245
Installing the Amazon EFS CSI driver	249
Creating an Amazon EFS file system	249
Deploying a sample application	249
Amazon FSx for Lustre CSI driver	249
Amazon FSx for NetApp ONTAP CSI driver	254
Amazon FSx for OpenZFS CSI driver	254
Amazon File Cache CSI driver	255
Networking	256
VPC and subnet requirements	256
VPC requirements and considerations	256
Subnet requirements and considerations	257
Shared subnet requirements and considerations	259
Creating a VPC	259
Security group requirements	263

Add-ons	265
Amazon VPC CNI plugin for Kubernetes	266
AWS Load Balancer Controller	333
CoreDNS	341
kube-proxy	347
Calico network policy engine	350
AWS PrivateLink	353
Considerations	354
Create an interface endpoint	354
Workloads	356
Sample application deployment	356
Vertical Pod Autoscaler	363
Deploy the Vertical Pod Autoscaler	363
Test your Vertical Pod Autoscaler installation	364
Horizontal Pod Autoscaler	367
Run a Horizontal Pod Autoscaler test application	367
Network load balancing	369
Create a network load balancer	371
(Optional) Deploy a sample application	373
Application load balancing	375
(Optional) Deploy a sample application	377
Restrict service external IP address assignment	379
Copy an image to a repository	381
Amazon container image registries	383
Amazon EKS add-ons	385
Available Amazon EKS add-ons from Amazon EKS	386
Additional Amazon EKS add-ons from independent software vendors	390
Managing add-ons	393
Kubernetes field management	406
Verify container images	409
Machine learning training	409
Create node group	410
(Optional) Deploy a sample EFA compatible application	414
Machine learning inference	415
Prerequisites	415
Create a cluster	416
(Optional) Deploy a TensorFlow Serving application image	416
(Optional) Make predictions against your TensorFlow Serving service	419
Cluster authentication	420
Enabling IAM principal access	420
Add IAM principals	421
Apply the aws-authConfigMap to your cluster	426
OIDC identity provider authentication	427
Associate an OIDC identity provider	428
Disassociate an OIDC identity provider from your cluster	429
Example IAM policy	430
Partner validated OIDC identity providers	431
Creating kubeconfig file	431
Create kubeconfig file automatically	432
Create kubeconfig file manually	433
Installing aws-iam-authenticator	436
Default Kubernetes roles and users	440
Cluster management	444
Cost monitoring	444
Remove Kubecost	447
Frequently asked questions	447
Metrics server	450

Using Helm	450
Tagging your resources	451
Tag basics	452
Tagging your resources	452
Tag restrictions	453
Tagging your resources for billing	453
Working with tags using the console	454
Working with tags using the CLI, API, or eksctl	454
Service quotas	455
Service quotas	456
AWS Fargate service quotas	457
Security	459
Certificate signing	460
CSR example	460
CSRs in Kubernetes 1.24	461
Kubernetes service accounts	462
Service account tokens	462
Cluster add-ons	463
IAM roles for service accounts	464
Identity and access management	478
Audience	479
Authenticating with identities	479
Managing access using policies	481
How Amazon EKS works with IAM	482
Identity-based policy examples	485
Using service-linked roles	490
Cluster IAM role	499
Node IAM role	501
Pod execution IAM role	504
Connector IAM role	508
AWS managed policies	510
Troubleshooting	517
Compliance validation	519
Resilience	520
Infrastructure security	520
Configuration and vulnerability analysis	521
Security best practices	522
Pod security policy	522
Amazon EKS default Pod security policy	522
Delete default policy	523
Install or restore default policy	524
1.25 Pod security policy removal FAQ	525
Managing Kubernetes secrets	527
Amazon EKS Connector considerations	527
AWS responsibilities	528
Customer responsibilities	528
View Kubernetes resources	529
Required permissions	529
Observability	534
Logging and monitoring	534
Amazon EKS logging and monitoring tools	535
Configuring logging	536
Enabling and disabling control plane logs	537
Viewing cluster control plane logs	539
Prometheus metrics	540
Viewing the raw metrics	540
Deploying Prometheus	540

Store your Prometheus metrics in Amazon Managed Service for Prometheus	543
Logging Amazon EKS API calls with AWS CloudTrail	543
Amazon EKS information in CloudTrail	543
Understanding Amazon EKS log file entries	544
Enable Auto Scaling group metrics collection	546
Amazon EKS add-on support for ADOT Operator	549
ADOT prerequisites and considerations	550
Create an IAM role	550
Manage the ADOT Operator	551
Deploy a sample application	553
Deploy the ADOT Collector	555
Troubleshooting	557
Working with other services	559
Creating Amazon EKS resources with AWS CloudFormation	559
Amazon EKS and AWS CloudFormation templates	559
Learn more about AWS CloudFormation	559
Amazon EKS and AWS Local Zones	560
Deep Learning Containers	560
Amazon VPC Lattice	560
AWS Resilience Hub	561
Amazon GuardDuty	561
Amazon Detective	561
Troubleshooting	562
Insufficient capacity	562
Nodes fail to join cluster	562
Unauthorized or access denied (<code>kubectl</code>)	563
<code>aws-iam-authenticator</code> Not found	563
hostname doesn't match	564
<code>getsockopt: no route to host</code>	564
Instances failed to join the Kubernetes cluster	564
Managed node group error codes	564
Not authorized for images	568
CNI log collection tool	568
Container runtime network not ready	569
TLS handshake timeout	569
<code>InvalidClientTokenId</code>	569
VPC admission webhook certificate expiration	570
Node groups must match Kubernetes version before updating control plane	570
When launching many nodes, there are Too Many Requests errors	570
HTTP 401 unauthorized errors	571
Old platform version	571
Amazon EKS Connector	574
Considerations	574
Required IAM permissions	574
Connecting a cluster	575
Connector methods	575
Prerequisites	575
Step 1: Registering the cluster	575
Step 2: Installing the agent	577
Next steps	578
Granting access to an IAM principal to view Kubernetes resources on a cluster	579
Prerequisites	579
Deregister a cluster	580
To deregister the Kubernetes cluster	580
To clean up the resources in your Kubernetes cluster	581
Amazon EKS Connector Troubleshooting	581
Basic troubleshooting	581

Helm issue: 403 Forbidden	583
Cluster stuck in Pending state	583
Service account can't impersonate "users" in API group	583
User can't list resource in API group	584
Amazon EKS can't communicate with API server	584
Amazon EKS connector Pods are crash looping	584
Failed to initiate eks-connector: InvalidActivation	585
Cluster node is missing outbound connectivity	586
Amazon EKS connector Pods are in ImagePullBackOff state	586
Frequently asked questions	586
Amazon EKS on AWS Outposts	588
When to use each deployment option	588
Comparing the deployment options	589
Local clusters	590
Creating a local cluster	591
Platform versions	597
VPC and subnet requirements	601
Network disconnects	604
Capacity considerations	607
Troubleshooting	608
Launching nodes	614
Related projects	621
Management tools	621
eksctl	621
AWS controllers for Kubernetes	621
Flux CD	621
CDK for Kubernetes	621
Networking	622
Amazon VPC CNI plugin for Kubernetes	622
AWS Load Balancer Controller for Kubernetes	622
ExternalDNS	622
Security	622
AWS IAM authenticator	622
Machine learning	622
Kubeflow	623
Auto Scaling	623
Cluster autoscaler	623
Escalator	623
Monitoring	623
Prometheus	623
Continuous integration / continuous deployment	623
Jenkins X	623
Amazon EKS new features and roadmap	625
Document history	626

What is Amazon EKS?

Amazon Elastic Kubernetes Service (Amazon EKS) is a managed service that eliminates the need to install, operate, and maintain your own Kubernetes control plane on Amazon Web Services (AWS). [Kubernetes](#) is an open-source system that automates the management, scaling, and deployment of containerized applications.

Features of Amazon EKS

The following are key features of Amazon EKS:

Secure networking and authentication

Amazon EKS integrates your Kubernetes workloads with AWS [networking \(p. 256\)](#) and security services. It also integrates with AWS Identity and Access Management (IAM) to provide [authentication \(p. 420\)](#) for your Kubernetes clusters.

Easy cluster scaling

Amazon EKS enables you to scale your Kubernetes clusters up and down easily based on the demand of your workloads. Amazon EKS supports [horizontal Pod autoscaling \(p. 367\)](#) based on CPU or custom metrics, and [cluster autoscaling \(p. 75\)](#) based on the demand of the entire workload.

Managed Kubernetes experience

You can make changes to your Kubernetes clusters using [eksctl](#), [AWS Management Console](#), [AWS Command Line Interface \(AWS CLI\)](#), [the API](#), [kubectl \(p. 6\)](#), and [Terraform](#).

High availability

Amazon EKS provides [high availability \(p. 520\)](#) for your control plane across multiple Availability Zones.

Integration with AWS services

Amazon EKS integrates with other [AWS services \(p. 559\)](#), providing a comprehensive platform for deploying and managing your containerized applications. You can also more easily troubleshoot your Kubernetes workloads with various [observability \(p. 534\)](#) tools.

For details about other features of Amazon EKS, see [Amazon EKS features](#).

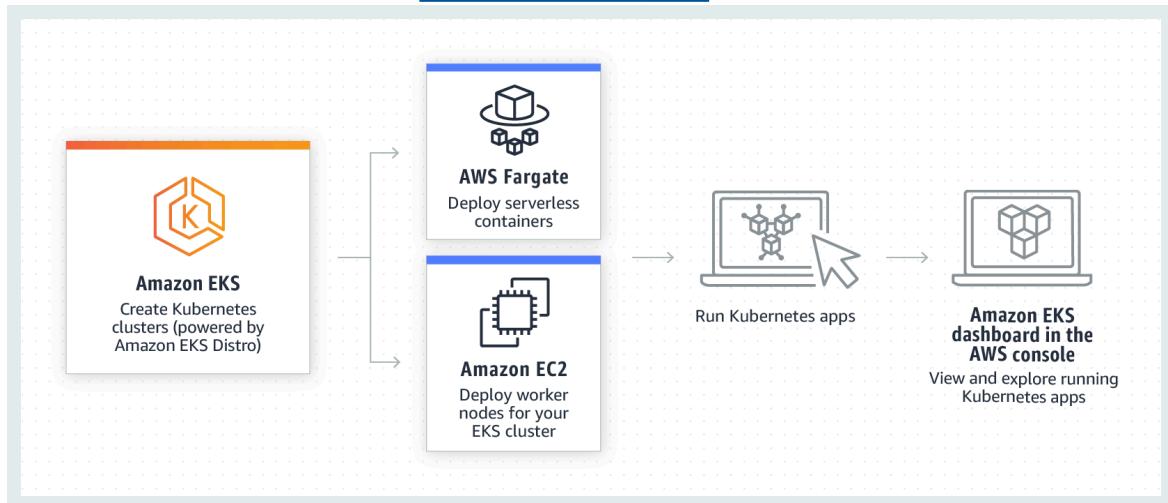
Get started with Amazon EKS

To create your first cluster and its associated resources, see [Getting started with Amazon EKS \(p. 6\)](#). In general, getting started with Amazon EKS involves the following steps.

1. **Create a cluster** – Start by creating your cluster using eksctl, AWS Management Console, AWS CLI, or one of the AWS SDKs.
2. **Choose your approach to compute resources** – Decide between AWS Fargate, Karpenter, managed node groups, and self-managed nodes.
3. **Setup** – Set up the necessary controllers, drivers, and services.
4. **Deploy workloads** – Tailor your Kubernetes workloads to best utilize the resources and capabilities of your chosen node type.

5. **Management** – Oversee your workloads, integrating AWS services to streamline operations and enhance workload performance. You can view information about your workloads using the AWS Management Console.

The following diagram shows a basic flow of running Amazon EKS in the cloud. To learn about other Kubernetes deployment options, see [Deployment options \(p. 4\)](#).



Pricing for Amazon EKS

An Amazon EKS cluster consists of a control plane and the [Amazon Elastic Compute Cloud](#) (Amazon EC2) or Fargate compute that you run Pods on. For more information about pricing for the control plane, see [Amazon EKS pricing](#). Both Amazon EC2 and Fargate provide:

On-Demand Instances

Pay for the instances that you use by the second, with no long-term commitments or upfront payments. For more information, see [Amazon EC2 On-Demand Pricing](#) and [AWS Fargate Pricing](#).

Savings Plans

You can reduce your costs by making a commitment to a consistent amount of usage, in USD per hour, for a term of one or three years. For more information, see [Pricing with Savings Plans](#).

Common use cases in Amazon EKS

Amazon EKS offers robust managed Kubernetes services on AWS, designed to optimize containerized applications. The following are a few of the most common use cases of Amazon EKS, helping you leverage its strengths for your specific needs.

Deploying high-availability applications

Using [Elastic Load Balancing](#), you can make sure that your applications are highly available across multiple [Availability Zones](#).

Building microservices architectures

Use Kubernetes service discovery features with [AWS Cloud Map](#) or [Amazon VPC Lattice](#) to build resilient systems.

Automating software release process

Manage continuous integration and continuous deployment (CI/CD) pipelines that simplify the process of automated building, testing, and deployment of applications.

Running serverless applications

Use [AWS Fargate](#) with Amazon EKS to run serverless applications. This means you can focus solely on application development, while Amazon EKS and Fargate handle the underlying infrastructure.

Executing machine learning workloads

Amazon EKS is compatible with popular machine learning frameworks such as [TensorFlow](#), [MXNet](#), and [PyTorch](#). With GPU support, you can handle even complex machine learning tasks effectively.

Deploying consistently on premises and in the cloud

Use [Amazon EKS Anywhere](#) to operate Kubernetes clusters on your own infrastructure using tools that are consistent with Amazon EKS in the cloud.

Running cost-effective batch processing and big data workloads

Utilize [Spot Instances](#) to run your batch processing and big data workloads such as [Apache Hadoop](#) and [Spark](#), at a fraction of the cost. This lets you take advantage of unused Amazon EC2 capacity at discounted prices.

Securing application and ensuring compliance

Implement strong security practices and maintain compliance with Amazon EKS, which integrates with AWS security services such as [AWS Identity and Access Management](#) (IAM), [Amazon Virtual Private Cloud](#) (Amazon VPC), and [AWS Key Management Service](#) (AWS KMS). This ensures data privacy and protection as per industry standards.

Amazon EKS architecture

Amazon EKS aligns with the general cluster architecture of Kubernetes. For more information, see [Kubernetes Components](#) in the Kubernetes documentation. The following sections summarize some extra architecture details for Amazon EKS.

Control plane

Amazon EKS ensures every cluster has its own unique Kubernetes control plane. This design keeps each cluster's infrastructure separate, with no overlaps between clusters or AWS accounts. The setup includes:

Distributed components

The control plane positions at least two API server instances and three [etcd](#) instances across three AWS Availability Zones within an AWS Region.

Optimal performance

Amazon EKS actively monitors and adjusts control plane instances to maintain peak performance.

Resilience

If a control plane instance falters, Amazon EKS quickly replaces it, using different Availability Zone if needed.

Consistent uptime

By running clusters across multiple Availability Zones, a reliable [API server endpoint availability Service Level Agreement \(SLA\)](#) is achieved.

Amazon EKS uses Amazon Virtual Private Cloud (Amazon VPC) to limit traffic between control plane components within a single cluster. Cluster components can't view or receive communication from other clusters or AWS accounts, except when authorized by Kubernetes role-based access control (RBAC) policies.

Compute

In addition to the control plane, an Amazon EKS cluster has a set of worker machines called nodes. Selecting the appropriate Amazon EKS cluster node type is crucial for meeting your specific requirements and optimizing resource utilization. Amazon EKS offers the following primary node types:

AWS Fargate

[Fargate \(p. 131\)](#) is a serverless compute engine for containers that eliminates the need to manage the underlying instances. With Fargate, you specify your application's resource needs, and AWS automatically provisions, scales, and maintains the infrastructure. This option is ideal for users who prioritize ease-of-use and want to concentrate on application development and deployment rather than managing infrastructure.

Karpenter

[Karpenter](#) is a flexible, high-performance Kubernetes cluster autoscaler that helps improve application availability and cluster efficiency. Karpenter launches right-sized compute resources in response to changing application load. This option can provision just-in-time compute resources that meet the requirements of your workload.

Managed node groups

[Managed node groups \(p. 81\)](#) are a blend of automation and customization for managing a collection of Amazon EC2 instances within an Amazon EKS cluster. AWS takes care of tasks like patching, updating, and scaling nodes, easing operational aspects. In parallel, custom kubelet arguments are supported, opening up possibilities for advanced CPU and memory management policies. Moreover, they enhance security via AWS Identity and Access Management (IAM) roles for service accounts, while curbing the need for separate permissions per cluster.

Self-managed nodes

[Self-managed nodes \(p. 108\)](#) offer full control over your Amazon EC2 instances within an Amazon EKS cluster. You are in charge of managing, scaling, and maintaining the nodes, giving you total control over the underlying infrastructure. This option is suitable for users who need granular control and customization of their nodes and are ready to invest time in managing and maintaining their infrastructure.

Deployment options

You can deploy Amazon EKS using any of the following options:

Amazon EKS in the cloud

You can run Kubernetes in the AWS cloud without needing to install, operate, and maintain your own Kubernetes control plane or nodes. This option is what is covered in this guide.

Amazon EKS on Outposts

AWS Outposts enables native AWS services, infrastructure, and operating models in your on-premises facilities. With Amazon EKS on Outposts, you can choose to run extended or local clusters. With extended clusters, the Kubernetes control plane runs in an AWS Region, and the nodes run on Outposts. With local clusters, the entire Kubernetes cluster runs locally on Outposts, including

both the Kubernetes control plane and nodes. For more information, see [Amazon EKS on AWS Outposts \(p. 588\)](#).

Amazon EKS Anywhere

Amazon EKS Anywhere is a deployment option for Amazon EKS that enables you to easily create and operate Kubernetes clusters on-premises. Both Amazon EKS and Amazon EKS Anywhere are built on the [Amazon EKS Distro](#). To learn more about Amazon EKS Anywhere, and its differences with Amazon EKS, see [Overview](#) and [Comparing Amazon EKS Anywhere to Amazon EKS](#) in the Amazon EKS Anywhere documentation. For answers to some common questions, see [Amazon EKS Anywhere FAQs](#).

Amazon EKS Distro

Amazon EKS Distro is a distribution of the same open-source Kubernetes software and dependencies deployed by Amazon EKS in the cloud. Amazon EKS Distro follows the same Kubernetes version release cycle as Amazon EKS and is provided as an open-source project. To learn more, see [Amazon EKS Distro](#). You can also view and download the source code for the [Amazon EKS Distro](#) on GitHub.

When choosing which deployment options to use for your Kubernetes cluster, consider the following:

Feature	Amazon EKS	Amazon EKS on Outposts	Amazon EKS Anywhere	Amazon EKS Distro
Hardware	AWS-supplied	AWS-supplied	Supplied by you	Supplied by you
Deployment location	AWS cloud	Your data center	Your data center	Your data center
Kubernetes control plane location	AWS cloud	AWS cloud or your data center	Your data center	Your data center
Kubernetes data plane location	AWS cloud	Your data center	Your data center	Your data center
Support	AWS Support	AWS Support	AWS Support	OSS community support

Getting started with Amazon EKS

Many procedures of this user guide use the following command line tools:

- **kubectl** – A command line tool for working with Kubernetes clusters. For more information, see [Installing or updating kubectl \(p. 6\)](#).
- **eksctl** – A command line tool for working with EKS clusters that automates many individual tasks. For more information, see [Installing or updating eksctl \(p. 13\)](#).
- **AWS CLI** – A command line tool for working with AWS services, including Amazon EKS. For more information, see [Installing, updating, and uninstalling the AWS CLI](#) in the AWS Command Line Interface User Guide. After installing the AWS CLI, we recommend that you also configure it. For more information, see [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide.

There are two getting started guides available for creating a new Kubernetes cluster with nodes in Amazon EKS:

- [Getting started with Amazon EKS – eksctl \(p. 13\)](#) – This getting started guide helps you to install all of the required resources to get started with Amazon EKS using eksctl, a simple command line utility for creating and managing Kubernetes clusters on Amazon EKS. At the end of the tutorial, you will have a running Amazon EKS cluster that you can deploy applications to. This is the fastest and simplest way to get started with Amazon EKS.
- [Getting started with Amazon EKS – AWS Management Console and AWS CLI \(p. 16\)](#) – This getting started guide helps you to create all of the required resources to get started with Amazon EKS using the AWS Management Console and AWS CLI. At the end of the tutorial, you will have a running Amazon EKS cluster that you can deploy applications to. In this guide, you manually create each resource required for an Amazon EKS cluster. The procedures give you visibility into how each resource is created and how they interact with each other.

Installing or updating kubectl

Kubectl is a command line tool that you use to communicate with the Kubernetes API server. The kubectl binary is available in many operating system package managers. Using a package manager for your installation is often easier than a manual download and install process.

This topic helps you to download and install, or update, the kubectl binary on your device. The binary is identical to the [upstream community versions](#). The binary is not unique to Amazon EKS or AWS.

Note

You must use a kubectl version that is within one minor version difference of your Amazon EKS cluster control plane. For example, a 1.27 kubectl client works with Kubernetes 1.26, 1.27, and 1.28 clusters.

To install or update kubectl

1. Determine whether you already have kubectl installed on your device.

```
kubectl version --short --client
```

If you have kubectl installed in the path of your device, the example output includes the following line. You can ignore the message explaining that --short will become the default in the future. If

If you want to update the version that you currently have installed with a later version, complete the next step, making sure to install the new version in the same location that your current version is in.

```
Client Version: v1.28.X-eks-1234567
```

If you receive no output, then you either don't have kubectl installed, or it's not installed in a location that's in your device's path.

2. Install or update kubectl on macOS, Linux, and Windows operating systems.

macOS

To install or update kubectl on macOS

1. Download the binary for your cluster's Kubernetes version from Amazon S3.

- Kubernetes 1.28

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.1/2023-09-14/bin/darwin/amd64/kubectl
```

- Kubernetes 1.27

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.5/2023-09-14/bin/darwin/amd64/kubectl
```

- Kubernetes 1.26

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.8/2023-09-14/bin/darwin/amd64/kubectl
```

- Kubernetes 1.25

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.25.13/2023-09-14/bin/darwin/amd64/kubectl
```

- Kubernetes 1.24

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.24.17/2023-09-14/bin/darwin/amd64/kubectl
```

- Kubernetes 1.23

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.23.17/2023-09-14/bin/darwin/amd64/kubectl
```

2. (Optional) Verify the downloaded binary with the SHA-256 checksum for your binary.

- a. Download the SHA-256 checksum for your cluster's Kubernetes version.

- Kubernetes 1.28

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.1/2023-09-14/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.27

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.5/2023-09-14/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.26

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.8/2023-09-14/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.25

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.25.13/2023-09-14/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.24

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.24.17/2023-09-14/bin/darwin/amd64/kubectl.sha256
```

- Kubernetes 1.23

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.23.17/2023-09-14/bin/darwin/amd64/kubectl.sha256
```

- a. Check the SHA-256 checksum for your downloaded binary.

```
openssl sha1 -sha256 kubectl
```

- c. Make sure that the generated checksum in the output matches in the checksum in the downloaded kubectl.sha256 file.

3. Apply execute permissions to the binary.

```
chmod +x ./kubectl
```

4. Copy the binary to a folder in your PATH. If you have already installed a version of kubectl, then we recommend creating a \$HOME/bin/kubectl and ensuring that \$HOME/bin comes first in your \$PATH.

```
mkdir -p $HOME/bin && cp ./kubectl $HOME/bin/kubectl && export PATH=$HOME/bin:$PATH
```

5. (Optional) Add the \$HOME/bin path to your shell initialization file so that it is configured when you open a shell.

```
echo 'export PATH=$HOME/bin:$PATH' >> ~/.bash_profile
```

Linux

To install or update kubectl on Linux

1. Download the kubectl binary for your cluster's Kubernetes version from Amazon S3 using the command for your device's hardware platform. The first link for each version is for amd64 and the second link is for arm64.
 - Kubernetes 1.28

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.1/2023-09-14/bin/linux/amd64/kubectl
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.1/2023-09-14/bin/linux/arm64/kubectl
```

- Kubernetes 1.27

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.5/2023-09-14/bin/linux/amd64/kubectl
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.5/2023-09-14/bin/linux/arm64/kubectl
```

- Kubernetes 1.26

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.8/2023-09-14/bin/linux/amd64/kubectl
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.8/2023-09-14/bin/linux/arm64/kubectl
```

- Kubernetes 1.25

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.25.13/2023-09-14/bin/linux/amd64/kubectl
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.25.13/2023-09-14/bin/linux/arm64/kubectl
```

- Kubernetes 1.24

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.24.17/2023-09-14/bin/linux/amd64/kubectl
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.24.17/2023-09-14/bin/linux/arm64/kubectl
```

- Kubernetes 1.23

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.23.17/2023-09-14/bin/linux/amd64/kubectl
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.23.17/2023-09-14/bin/linux/arm64/kubectl
```

2. (Optional) Verify the downloaded binary with the SHA-256 checksum for your binary.

- a. Download the SHA-256 checksum for your cluster's Kubernetes version from Amazon S3 using the command for your device's hardware platform. The first link for each version is for amd64 and the second link is for arm64.

- Kubernetes 1.28

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.1/2023-09-14/bin/linux/amd64/kubectl.sha256
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.1/2023-09-14/bin/linux/arm64/kubectl.sha256
```

- Kubernetes 1.27

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.5/2023-09-14/bin/linux/amd64/kubectl.sha256
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.5/2023-09-14/bin/linux/arm64/kubectl.sha256
```

- Kubernetes 1.26

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.8/2023-09-14/bin/linux/amd64/kubectl.sha256
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.8/2023-09-14/bin/linux/arm64/kubectl.sha256
```

- Kubernetes 1.25

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.25.13/2023-09-14/bin/linux/amd64/kubectl.sha256
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.25.13/2023-09-14/bin/linux/arm64/kubectl.sha256
```

- Kubernetes 1.24

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.24.17/2023-09-14/bin/linux/amd64/kubectl.sha256
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.24.17/2023-09-14/bin/linux/arm64/kubectl.sha256
```

- Kubernetes 1.23

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.23.17/2023-09-14/bin/linux/amd64/kubectl.sha256
```

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.23.17/2023-09-14/bin/linux/arm64/kubectl.sha256
```

- a. Download the SHA-256 checksum for your desired Kubernetes version from the [Amazon EKS documentation](#).
- b. Check the SHA-256 checksum for your downloaded binary with one of the following commands.

- `sha256sum -c kubectl.sha256`

When using this command, make sure that you see the following output:

```
kubectl: OK
```

- `openssl sha1 -sha256 kubectl`

When using this command, make sure that the generated checksum in the output matches in the checksum in the downloaded `kubectl.sha256` file.

3. Apply execute permissions to the binary.

```
chmod +x ./kubectl
```

4. Copy the binary to a folder in your PATH. If you have already installed a version of `kubectl`, then we recommend creating a `$HOME/bin/kubectl` and ensuring that `$HOME/bin` comes first in your `$PATH`.

```
mkdir -p $HOME/bin && cp ./kubectl $HOME/bin/kubectl && export PATH=$HOME/bin:$PATH
```

5. (Optional) Add the `$HOME/bin` path to your shell initialization file so that it is configured when you open a shell.

Note

This step assumes you are using the Bash shell; if you are using another shell, change the command to use your specific shell initialization file.

```
echo 'export PATH=$HOME/bin:$PATH' >> ~/.bashrc
```

Windows

To install or update kubectl on Windows

1. Open a PowerShell terminal.
2. Download the `kubectl` binary for your cluster's Kubernetes version from Amazon S3.
 - Kubernetes 1.28

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.1/2023-09-14/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.27

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.5/2023-09-14/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.26

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.8/2023-09-14/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.25

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.25.13/2023-09-14/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.24

```
curl.exe -O https://s3.us-west-2.amazonaws.com/amazon-eks/1.24.17/2023-09-14/bin/windows/amd64/kubectl.exe
```

- Kubernetes 1.23

```
curl.exe -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.23.17/2023-09-14/bin/windows/amd64/kubectl.exe
```

3. (Optional) Verify the downloaded binary with the SHA-256 checksum for your binary.

- a. Download the SHA-256 checksum for your cluster's Kubernetes version for Windows.

- Kubernetes 1.28

```
curl.exe -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.28.1/2023-09-14/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.27

```
curl.exe -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.27.5/2023-09-14/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.26

```
curl.exe -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.26.8/2023-09-14/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.25

```
curl.exe -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.25.13/2023-09-14/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.24

```
curl.exe -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.24.17/2023-09-14/bin/windows/amd64/kubectl.exe.sha256
```

- Kubernetes 1.23

```
curl.exe -0 https://s3.us-west-2.amazonaws.com/amazon-eks/1.23.17/2023-09-14/bin/windows/amd64/kubectl.exe.sha256
```

- b. Check the SHA-256 checksum for your downloaded binary.

```
Get-FileHash kubectl.exe
```

- c. Make sure that the generated checksum in the output matches in the checksum in the downloaded kubectl.sha256 file. The PowerShell output should be an uppercase equivalent string of characters.

4. Copy the binary to a folder in your PATH. If you have an existing directory in your PATH that you use for command line utilities, copy the binary to that directory. Otherwise, complete the following steps.

- a. Create a new directory for your command line binaries, such as C:\bin.

- b. Copy the kubectl.exe binary to your new directory.

- c. Edit your user or system PATH environment variable to add the new directory to your PATH.

- d. Close your PowerShell terminal and open a new one to pick up the new PATH variable.

3. After you install kubectl, you can verify its version.

```
kubectl version --short --client
```

You can ignore the message explaining that `--short` will become the default in the future.

When first installing `kubectl`, it isn't yet configured to communicate with any server. We will cover this configuration as needed in other procedures. If you ever need to update the configuration to communicate with a particular cluster, you can run the following command. Replace `region-code` with the AWS Region that your cluster is in. Replace `my-cluster` with the name of your cluster.

```
aws eks update-kubeconfig --region region-code --name my-cluster
```

Installing or updating eksctl

`eksctl` is a simple command line tool for creating and managing Kubernetes clusters on Amazon EKS. `eksctl` provides the fastest and easiest way to create a new cluster with nodes for Amazon EKS. For the official documentation, see <https://eksctl.io/>.

Determine whether you already have `eksctl` installed on your device.

```
eksctl version
```

If you have `eksctl` installed in the path of your device, the example output is as follows. If you want to update the version that you currently have installed with a later version, make sure to install the new version in the same location that your current version is in.

```
0.160.0
```

If you receive no output, then you either don't have `eksctl` installed, or it's not installed in a location that's in your device's path.

For instructions on installing or updating `eksctl`, see [Installation](#) in the `eksctl` documentation.

Getting started with Amazon EKS – eksctl

This guide helps you to create all of the required resources to get started with Amazon Elastic Kubernetes Service (Amazon EKS) using `eksctl`, a simple command line utility for creating and managing Kubernetes clusters on Amazon EKS. At the end of this tutorial, you will have a running Amazon EKS cluster that you can deploy applications to.

The procedures in this guide create several resources for you automatically that you have to create manually when you create your cluster using the AWS Management Console. If you'd rather manually create most of the resources to better understand how they interact with each other, then use the AWS Management Console to create your cluster and compute. For more information, see [Getting started with Amazon EKS – AWS Management Console and AWS CLI \(p. 16\)](#).

Prerequisites

Before starting this tutorial, you must install and configure the following tools and resources that you need to create and manage an Amazon EKS cluster.

- **kubectl** – A command line tool for working with Kubernetes clusters. For more information, see [Installing or updating kubectl \(p. 6\)](#).
- **eksctl** – A command line tool for working with EKS clusters that automates many individual tasks. For more information, see [Installing or updating eksctl \(p. 13\)](#).
- **Required IAM permissions** – The IAM security principal that you're using must have permissions to work with Amazon EKS IAM roles, service linked roles, AWS CloudFormation, a VPC, and related resources. For more information, see [Actions, resources, and condition keys for Amazon Elastic Container Service for Kubernetes](#) and [Using service-linked roles](#) in the IAM User Guide. You must complete all steps in this guide as the same user. To check the current user, run the following command:

```
aws sts get-caller-identity
```

Step 1: Create your Amazon EKS cluster and nodes

Important

To get started as simply and quickly as possible, this topic includes steps to create a cluster and nodes with default settings. Before creating a cluster and nodes for production use, we recommend that you familiarize yourself with all settings and deploy a cluster and nodes with the settings that meet your requirements. For more information, see [Creating an Amazon EKS cluster \(p. 25\)](#) and [Amazon EKS nodes \(p. 77\)](#). Some settings can only be enabled when creating your cluster and nodes.

You can create a cluster with one of the following node types. To learn more about each type, see [Amazon EKS nodes \(p. 77\)](#). After your cluster is deployed, you can add other node types.

- **Fargate – Linux** – Select this type of node if you want to run Linux applications on [AWS Fargate \(p. 131\)](#). Fargate is a serverless compute engine that lets you deploy Kubernetes Pods without managing Amazon EC2 instances.
- **Managed nodes – Linux** – Select this type of node if you want to run Amazon Linux applications on Amazon EC2 instances. Though not covered in this guide, you can also add [Windows self-managed \(p. 117\)](#) and [Bottlerocket \(p. 114\)](#) nodes to your cluster.

Create your Amazon EKS cluster with the following command. You can replace *my-cluster* with your own value. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters. Replace *region-code* with any AWS Region that is supported by Amazon EKS. For a list of AWS Regions, see [Amazon EKS endpoints and quotas](#) in the AWS General Reference guide.

Fargate – Linux

```
eksctl create cluster --name my-cluster --region region-code --fargate
```

Managed nodes – Linux

```
eksctl create cluster --name my-cluster --region region-code
```

Cluster creation takes several minutes. During creation you'll see several lines of output. The last line of output is similar to the following example line.

```
[...]
```

```
[#] EKS cluster "my-cluster" in "region-code" region is ready
```

eksctl created a kubectl config file in `~/.kube` or added the new cluster's configuration within an existing config file in `~/.kube` on your computer.

After cluster creation is complete, view the AWS CloudFormation stack named `eksctl-my-cluster-cluster` in the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation> to see all of the resources that were created.

Step 2: View Kubernetes resources

1. View your cluster nodes.

```
kubectl get nodes -o wide
```

An example output is as follows.

Fargate – Linux

NAME	INTERNAL-IP	EXTERNAL-IP	OS-IMAGE	STATUS	ROLES	AGE	KERNEL-VERSION
VERSION	CONTAINER-RUNTIME						
fargate-ip-192-0-2-0. <i>region-code</i> .compute.internal	v1.2.3-eks-1234567	192.0.2.0	<none>	Ready	<none>	8m3s	Amazon Linux 2
	1.23.456-789.012.amzn2.x86_64		containerd://1.2.3				
fargate-ip-192-0-2-1. <i>region-code</i> .compute.internal	v1.2.3-eks-1234567	192-0-2-1	<none>	Ready	<none>	7m30s	Amazon Linux 2
	1.23.456-789.012.amzn2.x86_64		containerd://1.2.3				

Managed nodes – Linux

NAME	INTERNAL-IP	EXTERNAL-IP	OS-IMAGE	STATUS	ROLES	AGE	VERSION
CONTAINER-RUNTIME							
ip-192-0-2-0. <i>region-code</i> .compute.internal	v1.2.3-eks-1234567	192.0.2.0	192.0.2.2	Ready	<none>	6m7s	Amazon Linux 2
	1.23.456-789.012.amzn2.x86_64		containerd://1.2.3				
ip-192-0-2-1. <i>region-code</i> .compute.internal	v1.2.3-eks-1234567	192.0.2.1	192.0.2.3	Ready	<none>	6m4s	Amazon Linux 2
	1.23.456-789.012.amzn2.x86_64		containerd://1.2.3				

For more information about what you see in the output, see [View Kubernetes resources \(p. 529\)](#).

2. View the workloads running on your cluster.

```
kubectl get pods -A -o wide
```

An example output is as follows.

Fargate – Linux

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE	IP
NODE				NOMINATED NODE		READINESS
GATES						
kube-system	coredns-1234567890-abcd	1/1	Running	0	18m	
	192.0.2.0	fargate-ip-192-0-2-0. <i>region-code</i> .compute.internal		<none>		
	<none>					

kube-system	coredns-1234567890-12345	1/1	Running	0	18m
	192.0.2.1		fargate-ip-192-0-2-1.region-code.compute.internal		<none>

Managed nodes – Linux

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE	IP
			NOMINATED	NODE	READINESS	GATES
kube-system	aws-node-12345	1/1	Running	0	7m43s	<none>
	192.0.2.1		ip-192-0-2-1.region-code.compute.internal	<none>		
kube-system	aws-node-67890	1/1	Running	0	7m46s	<none>
	192.0.2.0		ip-192-0-2-0.region-code.compute.internal	<none>		
kube-system	coredns-1234567890-abcd	1/1	Running	0	14m	<none>
	192.0.2.3		ip-192-0-2-3.region-code.compute.internal	<none>		
kube-system	coredns-1234567890-12345	1/1	Running	0	14m	<none>
	192.0.2.4		ip-192-0-2-4.region-code.compute.internal	<none>		
kube-system	kube-proxy-12345	1/1	Running	0	7m46s	<none>
	192.0.2.0		ip-192-0-2-0.region-code.compute.internal	<none>		
kube-system	kube-proxy-67890	1/1	Running	0	7m43s	<none>
	192.0.2.1		ip-192-0-2-1.region-code.compute.internal	<none>		

For more information about what you see in the output, see [View Kubernetes resources \(p. 529\)](#).

Step 3: Delete your cluster and nodes

After you've finished with the cluster and nodes that you created for this tutorial, you should clean up by deleting the cluster and nodes with the following command. If you want to do more with this cluster before you clean up, see [Next steps \(p. 16\)](#).

```
eksctl delete cluster --name my-cluster --region region-code
```

Next steps

The following documentation topics help you to extend the functionality of your cluster.

- Deploy a [sample application \(p. 356\)](#) to your cluster.
- The [IAM principal](#) that created the cluster is the only principal that can make calls to the Kubernetes API server with `kubectl` or the AWS Management Console. If you want other IAM principals to have access to your cluster, then you need to add them. For more information, see [Enabling IAM principal access to your cluster \(p. 420\)](#) and [Required permissions \(p. 529\)](#).
- Before deploying a cluster for production use, we recommend familiarizing yourself with all of the settings for [clusters \(p. 25\)](#) and [nodes \(p. 77\)](#). Some settings (such as enabling SSH access to Amazon EC2 nodes) must be made when the cluster is created.
- To increase security for your cluster, [configure the Amazon VPC Container Networking Interface plugin to use IAM roles for service accounts \(p. 272\)](#).

Getting started with Amazon EKS – AWS Management Console and AWS CLI

This guide helps you to create all of the required resources to get started with Amazon Elastic Kubernetes Service (Amazon EKS) using the AWS Management Console and the AWS CLI. In this guide,

you manually create each resource. At the end of this tutorial, you will have a running Amazon EKS cluster that you can deploy applications to.

The procedures in this guide give you complete visibility into how each resource is created and how the resources interact with each other. If you'd rather have most of the resources created for you automatically, use the `eksctl` CLI to create your cluster and nodes. For more information, see [Getting started with Amazon EKS – eksctl \(p. 13\)](#).

Prerequisites

Before starting this tutorial, you must install and configure the following tools and resources that you need to create and manage an Amazon EKS cluster.

- **AWS CLI** – A command line tool for working with AWS services, including Amazon EKS. For more information, see [Installing, updating, and uninstalling the AWS CLI](#) in the AWS Command Line Interface User Guide. After installing the AWS CLI, we recommend that you also configure it. For more information, see [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide.
- **kubectl** – A command line tool for working with Kubernetes clusters. For more information, see [Installing or updating kubectl \(p. 6\)](#).
- **Required IAM permissions** – The IAM security principal that you're using must have permissions to work with Amazon EKS IAM roles, service linked roles, AWS CloudFormation, a VPC, and related resources. For more information, see [Actions, resources, and condition keys for Amazon Elastic Kubernetes Service](#) and [Using service-linked roles](#) in the IAM User Guide. You must complete all steps in this guide as the same user. To check the current user, run the following command:

```
aws sts get-caller-identity
```

- We recommend that you complete the steps in this topic in a Bash shell. If you aren't using a Bash shell, some script commands such as line continuation characters and the way variables are set and used require adjustment for your shell. Additionally, the quoting and escaping rules for your shell might be different. For more information, see [Using quotation marks with strings in the AWS CLI](#) in the AWS Command Line Interface User Guide.

Step 1: Create your Amazon EKS cluster

Important

To get started as simply and quickly as possible, this topic includes steps to create a cluster with default settings. Before creating a cluster for production use, we recommend that you familiarize yourself with all settings and deploy a cluster with the settings that meet your requirements. For more information, see [Creating an Amazon EKS cluster \(p. 25\)](#). Some settings can only be enabled when creating your cluster.

To create your cluster

1. Create an Amazon VPC with public and private subnets that meets Amazon EKS requirements. Replace `region-code` with any AWS Region that is supported by Amazon EKS. For a list of AWS Regions, see [Amazon EKS endpoints and quotas](#) in the AWS General Reference guide. You can replace `my-eks-vpc-stack` with any name you choose.

```
aws cloudformation create-stack \
  --region region-code \
  --stack-name my-eks-vpc-stack \
  --template-url https://s3.us-west-2.amazonaws.com/amazon-
eks/cloudformation/2020-10-29/amazon-eks-vpc-private-subnets.yaml
```

Tip

For a list of all the resources the previous command creates, open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>. Choose the *my-eks-vpc-stack* stack and then choose the **Resources** tab.

2. Create a cluster IAM role and attach the required Amazon EKS IAM managed policy to it. Kubernetes clusters managed by Amazon EKS make calls to other AWS services on your behalf to manage the resources that you use with the service.
 - a. Copy the following contents to a file named *eks-cluster-role-trust-policy.json*.

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

- b. Create the role.

```
aws iam create-role \  
    --role-name myAmazonEKSClusterRole \  
    --assume-role-policy-document file://"eks-cluster-role-trust-policy.json"
```

- c. Attach the required Amazon EKS managed IAM policy to the role.

```
aws iam attach-role-policy \  
    --policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy \  
    --role-name myAmazonEKSClusterRole
```

3. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.

Make sure that the AWS Region shown in the upper right of your console is the AWS Region that you want to create your cluster in. If it's not, choose the dropdown next to the AWS Region name and choose the AWS Region that you want to use.

4. Choose **Add cluster**, and then choose **Create**. If you don't see this option, then choose **Clusters** in the left navigation pane first.
5. On the **Configure cluster** page, do the following:
 - a. Enter a **Name** for your cluster, such as *my-cluster*. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters.
 - b. For **Cluster Service Role**, choose *myAmazonEKSClusterRole*.
 - c. Leave the remaining settings at their default values and choose **Next**.
6. On the **Specify networking** page, do the following:
 - a. Choose the ID of the VPC that you created in a previous step from the **VPC** dropdown list. It is something like *vpc-00x000x000x0x000* | *my-eks-vpc-stack-VPC*.
 - b. Leave the remaining settings at their default values and choose **Next**.
7. On the **Configure logging** page, choose **Next**.
8. On the **Select add-ons** page, choose **Next**.

For more information on add-ons, see [Amazon EKS add-ons \(p. 385\)](#).

9. On the **Configure selected add-ons** settings page, choose **Next**.
10. On the **Review and create** page, choose **Create**.

To the right of the cluster's name, the cluster status is **Creating** for several minutes until the cluster provisioning process completes. Don't continue to the next step until the status is **Active**.

Note

You might receive an error that one of the Availability Zones in your request doesn't have sufficient capacity to create an Amazon EKS cluster. If this happens, the error output contains the Availability Zones that can support a new cluster. Retry creating your cluster with at least two subnets that are located in the supported Availability Zones for your account. For more information, see [Insufficient capacity \(p. 562\)](#).

Step 2: Configure your computer to communicate with your cluster

In this section, you create a kubeconfig file for your cluster. The settings in this file enable the `kubectl` CLI to communicate with your cluster.

To configure your computer to communicate with your cluster

1. Create or update a kubeconfig file for your cluster. Replace `region-code` with the AWS Region that you created your cluster in. Replace `my-cluster` with the name of your cluster.

```
aws eks update-kubeconfig --region region-code --name my-cluster
```

By default, the config file is created in `~/.kube` or the new cluster's configuration is added to an existing config file in `~/.kube`.

2. Test your configuration.

```
kubectl get svc
```

Note

If you receive any authorization or resource type errors, see [Unauthorized or access denied \(kubectl\) \(p. 563\)](#) in the troubleshooting topic.

An example output is as follows.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
svc/kubernetes	ClusterIP	10.100.0.1	<none>	443/TCP	1m

Step 3: Create nodes

Important

To get started as simply and quickly as possible, this topic includes steps to create nodes with default settings. Before creating nodes for production use, we recommend that you familiarize yourself with all settings and deploy nodes with the settings that meet your requirements. For more information, see [Amazon EKS nodes \(p. 77\)](#). Some settings can only be enabled when creating your nodes.

You can create a cluster with one of the following node types. To learn more about each type, see [Amazon EKS nodes \(p. 77\)](#). After your cluster is deployed, you can add other node types.

- **Fargate – Linux** – Choose this type of node if you want to run Linux applications on [AWS Fargate \(p. 131\)](#). Fargate is a serverless compute engine that lets you deploy Kubernetes Pods without managing Amazon EC2 instances.
- **Managed nodes – Linux** – Choose this type of node if you want to run Amazon Linux applications on Amazon EC2 instances. Though not covered in this guide, you can also add [Windows self-managed \(p. 117\)](#) and [Bottlerocket \(p. 114\)](#) nodes to your cluster.

Fargate – Linux

Create a Fargate profile. When Kubernetes Pods are deployed with criteria that matches the criteria defined in the profile, the Pods are deployed to Fargate.

To create a Fargate profile

1. Create an IAM role and attach the required Amazon EKS IAM managed policy to it. When your cluster creates Pods on Fargate infrastructure, the components running on the Fargate infrastructure must make calls to AWS APIs on your behalf. This is so that they can do actions such as pull container images from Amazon ECR or route logs to other AWS services. The Amazon EKS Pod execution role provides the IAM permissions to do this.
 - a. Copy the following contents to a file named *pod-execution-role-trust-policy.json*. Replace *region-code* with the AWS Region that your cluster is in. If you want to use the same role in all AWS Regions in your account, replace *region-code* with *. Replace *111122223333* with your account ID and *my-cluster* with the name of your cluster. If you want to use the same role for all clusters in your account, replace *my-cluster* with *.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Condition": {  
                "ArnLike": {  
                    "aws:SourceArn": "arn:aws:eks:region-code:111122223333:fargateprofile/my-cluster/*"  
                }  
            },  
            "Principal": {  
                "Service": "eks-fargate-pods.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

- b. Create a Pod execution IAM role.

```
aws iam create-role \  
  --role-name AmazonEKSFargatePodExecutionRole \  
  --assume-role-policy-document file:///"pod-execution-role-trust-policy.json"
```

- c. Attach the required Amazon EKS managed IAM policy to the role.

```
aws iam attach-role-policy \  
  --policy-arn arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy \  
  --role-name AmazonEKSFargatePodExecutionRole
```

```
--role-name AmazonEKSFargatePodExecutionRole
```

2. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
3. On the **Clusters** page, choose the *my-cluster* cluster.
4. On the *my-cluster* page, do the following:
 - a. Choose the **Compute** tab.
 - b. Under **Fargate Profiles**, choose **Add Fargate Profile**.
5. On the **Configure Fargate Profile** page, do the following:
 - a. For **Name**, enter a unique name for your Fargate profile, such as *my-profile*.
 - b. For **Pod execution role**, choose the **AmazonEKSFargatePodExecutionRole** that you created in a previous step.
 - c. Choose the **Subnets** dropdown and deselect any subnet with Public in its name. Only private subnets are supported for Pods that are running on Fargate.
 - d. Choose **Next**.
6. On the **Configure Pod selection** page, do the following:
 - a. For **Namespace**, enter **default**.
 - b. Choose **Next**.
7. On the **Review and create** page, review the information for your Fargate profile and choose **Create**.
8. After a few minutes, the **Status** in the **Fargate Profile configuration** section will change from **Creating** to **Active**. Don't continue to the next step until the status is **Active**.
9. If you plan to deploy all Pods to Fargate (none to Amazon EC2 nodes), do the following to create another Fargate profile and run the default name resolver (CoreDNS) on Fargate.

Note

If you don't do this, you won't have any nodes at this time.

- a. On the **Fargate Profile** page, choose *my-profile*.
- b. Under **Fargate profiles**, choose **Add Fargate Profile**.
- c. For **Name**, enter **CoreDNS**.
- d. For **Pod execution role**, choose the **AmazonEKSFargatePodExecutionRole** that you created in a previous step.
- e. Choose the **Subnets** dropdown and deselect any subnet with Public in its name. Only private subnets are supported for Pods running on Fargate.
- f. Choose **Next**.
- g. For **Namespace**, enter **kube-system**.
- h. Choose **Match labels**, and then choose **Add label**.
- i. Enter **k8s-app** for **Key** and **kube-dns** for value. This is necessary for the default name resolver (CoreDNS) to deploy to Fargate.
- j. Choose **Next**.
- k. On the **Review and create** page, review the information for your Fargate profile and choose **Create**.
- l. Run the following command to remove the default eks.amazonaws.com/compute-type : ec2 annotation from the CoreDNS Pods.

```
kubectl patch deployment coredns \
-n kube-system \
--type json \
```

```
-p='[{"op": "remove", "path": "/spec/template/metadata/annotations/eks.amazonaws.com~1compute-type"}]'
```

Note

The system creates and deploys two nodes based on the Fargate profile label you added. You won't see anything listed in **Node groups** because they aren't applicable for Fargate nodes, but you will see the new nodes listed in the **Overview** tab.

Managed nodes – Linux

Create a managed node group, specifying the subnets and node IAM role that you created in previous steps.

To create your Amazon EC2 Linux managed node group

1. Create a node IAM role and attach the required Amazon EKS IAM managed policy to it. The Amazon EKS node kubelet daemon makes calls to AWS APIs on your behalf. Nodes receive permissions for these API calls through an IAM instance profile and associated policies.
 - a. Copy the following contents to a file named *node-role-trust-policy.json*.

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

- b. Create the node IAM role.

```
aws iam create-role \  
  --role-name myAmazonEKSNodeRole \  
  --assume-role-policy-document file:///node-role-trust-policy.json"
```

- c. Attach the required managed IAM policies to the role.

```
aws iam attach-role-policy \  
  --policy-arn arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy \  
  --role-name myAmazonEKSNodeRole  
aws iam attach-role-policy \  
  --policy-arn arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly \  
  --role-name myAmazonEKSNodeRole  
aws iam attach-role-policy \  
  --policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy \  
  --role-name myAmazonEKSNodeRole
```

2. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
3. Choose the name of the cluster that you created in [Step 1: Create your Amazon EKS cluster \(p. 17\)](#), such as *my-cluster*.
4. On the *my-cluster* page, do the following:
 - a. Choose the **Compute** tab.

- b. Choose **Add Node Group**.
5. On the **Configure Node Group** page, do the following:
 - a. For **Name**, enter a unique name for your managed node group, such as **my-nodegroup**. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters.
 - b. For **Node IAM role name**, choose **myAmazonEKSNodeRole** role that you created in a previous step. We recommend that each node group use its own unique IAM role.
 - c. Choose **Next**.
6. On the **Set compute and scaling configuration** page, accept the default values and choose **Next**.
7. On the **Specify networking** page, accept the default values and choose **Next**.
8. On the **Review and create** page, review your managed node group configuration and choose **Create**.
9. After several minutes, the **Status** in the **Node Group configuration** section will change from **Creating** to **Active**. Don't continue to the next step until the status is **Active**.

Step 4: View resources

You can view your nodes and Kubernetes workloads.

To view your nodes and workloads

1. In the left navigation pane, choose **Clusters**. In the list of **Clusters**, choose the name of the cluster that you created, such as **my-cluster**.
2. On the **my-cluster** page, choose the following:
 - a. **Compute tab** – You see the list of **Nodes** that were deployed for the cluster. You can choose the name of a node to see more information about it.
 - b. **Resources tab** – You see all of the Kubernetes resources that are deployed by default to an Amazon EKS cluster. Select any resource type in the console to learn more about it.

Step 5: Delete resources

After you've finished with the cluster and nodes that you created for this tutorial, you should delete the resources that you created. If you want to do more with this cluster before you delete the resources, see [Next steps \(p. 24\)](#).

To delete the resources that you created in this guide

1. Delete any node groups or Fargate profiles that you created.
 - a. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
 - b. In the left navigation pane, choose **Clusters**. In the list of clusters, choose **my-cluster**.
 - c. Choose the **Compute** tab.
 - d. If you created a node group, choose the **my-nodegroup** node group and then choose **Delete**. Enter **my-nodegroup**, and then choose **Delete**.
 - e. For each Fargate profile that you created, choose it and then choose **Delete**. Enter the name of the profile, and then choose **Delete**.

Note

When deleting a second Fargate profile, you may need to wait for the first one to finish deleting.

- f. Don't continue until the node group or Fargate profiles are deleted.
2. Delete the cluster.
 - a. In the left navigation pane, choose **Clusters**. In the list of clusters, choose *my-cluster*.
 - b. Choose **Delete cluster**.
 - c. Enter *my-cluster* and then choose **Delete**. Don't continue until the cluster is deleted.
3. Delete the VPC AWS CloudFormation stack that you created.
 - a. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
 - b. Choose the *my-eks-vpc-stack* stack, and then choose **Delete**.
 - c. In the **Delete my-eks-vpc-stack** confirmation dialog box, choose **Delete stack**.
4. Delete the IAM roles that you created.
 - a. Open the IAM console at <https://console.aws.amazon.com/iam/>.
 - b. In the left navigation pane, choose **Roles**.
 - c. Select each role you created from the list (*myAmazonEKSClusterRole*, as well as **AmazonEKSFargatePodExecutionRole** or *myAmazonEKSNodeRole*). Choose **Delete**, enter the requested confirmation text, then choose **Delete**.

Next steps

The following documentation topics help you to extend the functionality of your cluster.

- The [IAM principal](#) that created the cluster is the only principal that can make calls to the Kubernetes API server with `kubectl` or the AWS Management Console. If you want other IAM principals to have access to your cluster, then you need to add them. For more information, see [Enabling IAM principal access to your cluster \(p. 420\)](#) and [Required permissions \(p. 529\)](#).
- Deploy a [sample application \(p. 356\)](#) to your cluster.
- Before deploying a cluster for production use, we recommend familiarizing yourself with all of the settings for [clusters \(p. 25\)](#) and [nodes \(p. 77\)](#). Some settings (such as enabling SSH access to Amazon EC2 nodes) must be made when the cluster is created.
- To increase security for your cluster, [configure the Amazon VPC Container Networking Interface plugin to use IAM roles for service accounts \(p. 272\)](#).

Amazon EKS clusters

An Amazon EKS cluster consists of two primary components:

- The Amazon EKS control plane
- Amazon EKS nodes that are registered with the control plane

The Amazon EKS control plane consists of control plane nodes that run the Kubernetes software, such as etcd and the Kubernetes API server. The control plane runs in an account managed by AWS, and the Kubernetes API is exposed via the Amazon EKS endpoint associated with your cluster. Each Amazon EKS cluster control plane is single-tenant and unique, and runs on its own set of Amazon EC2 instances.

All of the data stored by the etcd nodes and associated Amazon EBS volumes is encrypted using AWS KMS. The cluster control plane is provisioned across multiple Availability Zones and fronted by an Elastic Load Balancing Network Load Balancer. Amazon EKS also provisions elastic network interfaces in your VPC subnets to provide connectivity from the control plane instances to the nodes (for example, to support `kubectl exec` logs proxy data flows).

Important

In the Amazon EKS environment, etcd storage is limited to 8GB as per [upstream](#) guidance. You can monitor the `etcd_db_total_size_in_bytes` metric for the current database size.

Amazon EKS nodes run in your AWS account and connect to your cluster's control plane via the API server endpoint and a certificate file that is created for your cluster.

Note

- You can find out how the different components of Amazon EKS work in [Amazon EKS networking \(p. 256\)](#).
- For connected clusters, see [Amazon EKS Connector \(p. 574\)](#).

Topics

- [Creating an Amazon EKS cluster \(p. 25\)](#)
- [Updating an Amazon EKS cluster Kubernetes version \(p. 34\)](#)
- [Deleting an Amazon EKS cluster \(p. 38\)](#)
- [Amazon EKS cluster endpoint access control \(p. 41\)](#)
- [Enabling secret encryption on an existing cluster \(p. 46\)](#)
- [Enabling Windows support for your Amazon EKS cluster \(p. 49\)](#)
- [Private cluster requirements \(p. 58\)](#)
- [Amazon EKS Kubernetes versions \(p. 60\)](#)
- [Amazon EKS platform versions \(p. 71\)](#)
- [Autoscaling \(p. 75\)](#)

Creating an Amazon EKS cluster

This topic provides an overview of the available options and describes what to consider when you create an Amazon EKS cluster. If you need to create a cluster on an AWS Outpost, see [the section called "Local clusters" \(p. 590\)](#). If this is your first time creating an Amazon EKS cluster, we recommend that you follow one of our [Getting started with Amazon EKS \(p. 6\)](#) guides. These guides help you to create a simple, default cluster without expanding into all of the available options.

Prerequisites

- An existing VPC and subnets that meet [Amazon EKS requirements \(p. 256\)](#). Before you deploy a cluster for production use, we recommend that you have a thorough understanding of the VPC and subnet requirements. If you don't have a VPC and subnets, you can create them using an [Amazon EKS provided AWS CloudFormation template \(p. 259\)](#).
- The kubectl command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use kubectl version 1.26, 1.27, or 1.28 with it. To install or upgrade kubectl, see [Installing or updating kubectl \(p. 6\)](#).
- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with aws --version | cut -d / -f2 | cut -d ' ' -f1. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.
- An [IAM principal](#) with permissions to create and describe an Amazon EKS cluster. For more information, see [the section called "Create a local Kubernetes cluster on an Outpost" \(p. 489\)](#) and [the section called "List or describe all clusters" \(p. 490\)](#).

When an Amazon EKS cluster is created, the [IAM principal](#) that creates the cluster is permanently added to the Kubernetes RBAC authorization table as the administrator. This principal has system:masters permissions. This principal isn't visible in your cluster configuration. So, it's important to note the principal that created the cluster and make sure that you never delete it. Initially, only the [IAM principal](#) that created the server can make calls to the Kubernetes API server using kubectl. If you use the console to create the cluster, you must ensure that the same IAM credentials are in the AWS SDK credential chain when you run kubectl commands on your cluster. After your cluster is created, you can grant other [IAM principals](#) access to your cluster.

To create an Amazon EKS cluster

1. If you already have a cluster IAM role, or you're going to create your cluster with eksctl, then you can skip this step. By default, eksctl creates a role for you.

To create an Amazon EKS cluster IAM role

1. Run the following command to create an IAM trust policy JSON file.

```
cat >eks-cluster-role-trust-policy.json <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "eks.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
```

2. Create the Amazon EKS cluster IAM role. If necessary, preface `eks-cluster-role-trust-policy.json` with the path on your computer that you wrote the file to in the previous step. The

command associates the trust policy that you created in the previous step to the role. To create an IAM role, the [IAM principal](#) that is creating the role must be assigned the `iam:CreateRole` action (permission).

```
aws iam create-role --role-name myAmazonEKSClusterRole --assume-role-policy-document file://"eks-cluster-role-trust-policy.json"
```

3. Attach the Amazon EKS managed policy named [AmazonEKSClusterPolicy](#) to the role. To attach an IAM policy to an [IAM principal](#), the principal that is attaching the policy must be assigned one of the following IAM actions (permissions): `iam:AttachUserPolicy` or `iam:AttachRolePolicy`.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/  
AmazonEKSClusterPolicy --role-name myAmazonEKSClusterRole
```

2. Create an Amazon EKS cluster.

You can create a cluster by using `eksctl`, the AWS Management Console, or the AWS CLI.

`eksctl`

Prerequisite

Version `0.160.0` or later of the `eksctl` command line tool installed on your device or AWS CloudShell. To install or update `eksctl`, see [Installing or updating eksctl \(p. 13\)](#).

To create your cluster

Create an Amazon EKS IPv4 cluster with the Amazon EKS default Kubernetes version in your default AWS Region. Before running command, make the following replacements:

- Replace `region-code` with the AWS Region that you want to create your cluster in.
- Replace `my-cluster` with a name for your cluster. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters. The name must be unique within the AWS Region and AWS account that you're creating the cluster in.
- Replace `1.27` with any [Amazon EKS supported version \(p. 60\)](#).
- Change the values for `vpc-private-subnets` to meet your requirements. You can also add additional IDs. You must specify at least two subnet IDs. If you'd rather specify public subnets, you can change `--vpc-private-subnets` to `--vpc-public-subnets`. Public subnets have an associated route table with a route to an internet gateway, but private subnets don't have an associated route table. We recommend using private subnets whenever possible.

The subnets that you choose must meet the [Amazon EKS subnet requirements \(p. 257\)](#). Before selecting subnets, we recommend that you're familiar with all of the [Amazon EKS VPC and subnet requirements and considerations \(p. 256\)](#). You can't change which subnets you want to use after cluster creation.

```
eksctl create cluster --name my-cluster --region region-code --version 1.27 --vpc-private-subnets subnet-ExampleID1,subnet-ExampleID2 --without-nodegroup
```

Cluster provisioning takes several minutes. While the cluster is being created, several lines of output appear. The last line of output is similar to the following example line.

```
[#] EKS cluster "my-cluster" in "region-code" region is ready
```

Tip

To see the most options that you can specify when creating a cluster with `eksctl`, use the `eksctl create cluster --help` command. To see all the available options, you can use a config file. For more information, see [Using config files](#) and the [config file schema](#) in the `eksctl` documentation. You can find [config file examples](#) on GitHub.

Optional settings

The following are optional settings that, if required, must be added to the previous command. You can only enable these options when you create the cluster, not after. If you need to specify these options, you must create the cluster with an [eksctl config file](#) and specify the settings, rather than using the previous command.

- If you want to specify one or more security groups that Amazon EKS assigns to the network interfaces that it creates, specify the [securityGroup](#) option.

Whether you choose any security groups or not, Amazon EKS creates a security group that enables communication between your cluster and your VPC. Amazon EKS associates this security group, and any that you choose, to the network interfaces that it creates. For more information about the cluster security group that Amazon EKS creates, see [the section called "Security group requirements" \(p. 263\)](#). You can modify the rules in the cluster security group that Amazon EKS creates. If you choose to add your own security groups, you can't change the ones that you choose after cluster creation.

- If you want to specify which IPv4 Classless Inter-domain Routing (CIDR) block Kubernetes assigns service IP addresses from, specify the [serviceIPv4CIDR](#) option.

Specifying your own range can help prevent conflicts between Kubernetes services and other networks peered or connected to your VPC. Enter a range in CIDR notation. For example: `10.2.0.0/16`.

The CIDR block must meet the following requirements:

- Be within one of the following ranges: `10.0.0.0/8`, `172.16.0.0/12`, or `192.168.0.0/16`.
- Have a minimum size of `/24` and a maximum size of `/12`.
- Not overlap with the range of the VPC for your Amazon EKS resources.

You can only specify this option when using the IPv4 address family and only at cluster creation. If you don't specify this, then Kubernetes assigns service IP addresses from either the `10.100.0.0/16` or `172.20.0.0/16` CIDR blocks.

- If you're creating cluster and want the cluster to assign IPv6 addresses to Pods and services instead of IPv4 addresses, specify the [ipFamily](#) option.

Kubernetes assigns IPv4 addresses to Pods and services, by default. Before deciding to use the IPv6 family, make sure that you're familiar with all of the considerations and requirements in the [the section called "VPC requirements and considerations" \(p. 256\)](#), [the section called "Subnet requirements and considerations" \(p. 257\)](#), [the section called "Security group requirements" \(p. 263\)](#), and [the section called "IPv6" \(p. 278\)](#) topics. If you choose the IPv6 family, you can't specify an address range for Kubernetes to assign IPv6 service addresses from like you can for the IPv4 family. Kubernetes assigns service addresses from the unique local address range (`fc00::/7`).

AWS Management Console

To create your cluster

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose **Add cluster** and then choose **Create**.
3. On the **Configure cluster** page, enter the following fields:
 - **Name** – A name for your cluster. It must be unique in your AWS account. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters. The name must be unique within the AWS Region and AWS account that you're creating the cluster in.
 - **Kubernetes version** – The version of Kubernetes to use for your cluster. We recommend selecting the latest version, unless you need an earlier version.
 - **Cluster service role** – Choose the Amazon EKS cluster IAM role that you created to allow the Kubernetes control plane to manage AWS resources on your behalf.
 - **Secrets encryption** – (Optional) Choose to enable secrets encryption of Kubernetes secrets using a KMS key. You can also enable this after you create your cluster. Before you enable this capability, make sure that you're familiar with the information in [the section called "Enabling secret encryption" \(p. 46\)](#).
 - **Tags** – (Optional) Add any tags to your cluster. For more information, see [Tagging your Amazon EKS resources \(p. 451\)](#).
4. Choose **Next**.
5. On the **Specify networking** page, select values for the following fields:
 - **VPC** – Choose an existing VPC that meets [Amazon EKS VPC requirements \(p. 256\)](#) to create your cluster in. Before choosing a VPC, we recommend that you're familiar with all of the requirements and considerations in [the section called "VPC and subnet requirements" \(p. 256\)](#). You can't change which VPC you want to use after cluster creation. If no VPCs are listed, then you need to create one first. For more information, see [the section called "Creating a VPC" \(p. 259\)](#).
 - **Subnets** – By default, all available subnets in the VPC specified in the previous field are preselected. You must select at least two.

The subnets that you choose must meet the [Amazon EKS subnet requirements \(p. 257\)](#). Before selecting subnets, we recommend that you're familiar with all of the [Amazon EKS VPC and subnet requirements and considerations \(p. 256\)](#). You can't change which subnets you want to use after cluster creation.

Security groups – (Optional) Specify one or more security groups that you want Amazon EKS to associate to the network interfaces that it creates.

Whether you choose any security groups or not, Amazon EKS creates a security group that enables communication between your cluster and your VPC. Amazon EKS associates this security group, and any that you choose, to the network interfaces that it creates. For more information about the cluster security group that Amazon EKS creates, see [the section called "Security group requirements" \(p. 263\)](#). You can modify the rules in the cluster security group that Amazon EKS creates. If you choose to add your own security groups, you can't change the ones that you choose after cluster creation.

- **Choose cluster IP address family** – You can choose either **IPv4** and **IPv6**.

Kubernetes assigns IPv4 addresses to Pods and services, by default. Before deciding to use the IPv6 family, make sure that you're familiar with all of the considerations and requirements in the [the section called "VPC requirements and considerations" \(p. 256\)](#), [the section called "Subnet requirements and considerations" \(p. 257\)](#), [the section called](#)

"[Security group requirements](#)" (p. 263), and [the section called "IPv6" \(p. 278\)](#) topics. If you choose the IPv6 family, you can't specify an address range for Kubernetes to assign IPv6 service addresses from like you can for the IPv4 family. Kubernetes assigns service addresses from the unique local address range (fc00::/7).

- (Optional) Choose **Configure Kubernetes Service IP address range** and specify a **Service IPv4 range**.

Specifying your own range can help prevent conflicts between Kubernetes services and other networks peered or connected to your VPC. Enter a range in CIDR notation. For example: 10.2.0.0/16.

The CIDR block must meet the following requirements:

- Be within one of the following ranges: 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16.
- Have a minimum size of /24 and a maximum size of /12.
- Not overlap with the range of the VPC for your Amazon EKS resources.

You can only specify this option when using the IPv4 address family and only at cluster creation. If you don't specify this, then Kubernetes assigns service IP addresses from either the 10.100.0.0/16 or 172.20.0.0/16 CIDR blocks.

- For **Cluster endpoint access**, select an option. After your cluster is created, you can change this option. Before selecting a non-default option, make sure to familiarize yourself with the options and their implications. For more information, see [the section called "Configuring endpoint access" \(p. 41\)](#).
6. On the **Configure logging** page, you can optionally choose which log types that you want to enable. By default, each log type is **Disabled**. Before selecting a different option, familiarize yourself with the information in [Amazon EKS control plane logging \(p. 536\)](#). After you create the cluster, you can change this option.
 7. Select **Next**.
 8. On the **Select add-ons** page, choose the add-ons that you want to add to your cluster. You can choose as many **Amazon EKS add-ons** and **AWS Marketplace add-ons** as you require. If the **AWS Marketplace add-ons** that you want to install isn't listed, you can search for available **AWS Marketplace add-ons** by entering text in the search box. You can also search by **category**, **vendor**, or **pricing model** and then choose the add-ons from the search results. Once you've selected the add-ons that you want to install, choose **Next**.
 9. On the **Configure selected add-ons settings** page, select the version that you want to install and then choose **Next**. You can always update to a later version after cluster creation. You can update the configuration of each add-on after cluster creation. For more information about configuring add-ons, see [the section called "Updating an add-on" \(p. 400\)](#).

10On the **Review and create** page, review the information that you entered or selected on the previous pages. If you need to make changes, choose **Edit**. When you're satisfied, choose **Create**. The **Status** field shows **CREATING** while the cluster is provisioned.

Note

You might receive an error that one of the Availability Zones in your request doesn't have sufficient capacity to create an Amazon EKS cluster. If this happens, the error output contains the Availability Zones that can support a new cluster. Retry creating your cluster with at least two subnets that are located in the supported Availability Zones for your account. For more information, see [Insufficient capacity \(p. 562\)](#).

Cluster provisioning takes several minutes.

AWS CLI

To create your cluster

1. Create your cluster with the command that follows. Before running the command, make the following replacements:
 - Replace *region-code* with the AWS Region that you want to create your cluster in.
 - Replace *my-cluster* with a name for your cluster. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters. The name must be unique within the AWS Region and AWS account that you're creating the cluster in.
 - Replace *1.28* with any [Amazon EKS supported version \(p. 60\)](#).
 - Replace *111122223333* with your account ID and *myAmazonEKSClusterRole* with the name of your cluster IAM role.
 - Replace the values for subnet IDs with your own. You can also add additional IDs. You must specify at least two subnet IDs.

The subnets that you choose must meet the [Amazon EKS subnet requirements \(p. 257\)](#).

Before selecting subnets, we recommend that you're familiar with all of the [Amazon EKS VPC and subnet requirements and considerations \(p. 256\)](#). You can't change which subnets you want to use after cluster creation.

- If you don't want to specify a security group ID, remove `, securityGroupIds=sg-ExampleID1` from the command. If you want to specify one or more security group IDs, replace the values for securityGroupIds with your own. You can also add additional IDs.

Whether you choose any security groups or not, Amazon EKS creates a security group that enables communication between your cluster and your VPC. Amazon EKS associates this security group, and any that you choose, to the network interfaces that it creates. For more information about the cluster security group that Amazon EKS creates, see [the section called "Security group requirements" \(p. 263\)](#). You can modify the rules in the cluster security group that Amazon EKS creates. If you choose to add your own security groups, you can't change the ones that you choose after cluster creation.

```
aws eks create-cluster --region region-code --name my-cluster --kubernetes-version 1.28 \
--role-arn arn:aws:iam::111122223333:role/myAmazonEKSClusterRole \
--resources-vpc-config
subnetIds=subnet-ExampleID1,subnet-ExampleID2,securityGroupIds=sg-ExampleID1
```

Note

You might receive an error that one of the Availability Zones in your request doesn't have sufficient capacity to create an Amazon EKS cluster. If this happens, the error output contains the Availability Zones that can support a new cluster. Retry creating your cluster with at least two subnets that are located in the supported Availability Zones for your account. For more information, see [Insufficient capacity \(p. 562\)](#).

Optional settings

The following are optional settings that, if required, must be added to the previous command. You can only enable these options when you create the cluster, not after.

- If you want to specify which IPv4 Classless Inter-domain Routing (CIDR) block Kubernetes assigns service IP addresses from, you must specify it by adding the `--kubernetes-network-config serviceIpv4Cidr=CIDR block` to the following command.

Specifying your own range can help prevent conflicts between Kubernetes services and other networks peered or connected to your VPC. Enter a range in CIDR notation. For example: 10.2.0.0/16.

The CIDR block must meet the following requirements:

- Be within one of the following ranges: 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16.
- Have a minimum size of /24 and a maximum size of /12.
- Not overlap with the range of the VPC for your Amazon EKS resources.

You can only specify this option when using the IPv4 address family and only at cluster creation. If you don't specify this, then Kubernetes assigns service IP addresses from either the 10.100.0.0/16 or 172.20.0.0/16 CIDR blocks.

- If you're creating a cluster and want the cluster to assign IPv6 addresses to Pods and services instead of IPv4 addresses, add **--kubernetes-network-config ipFamily=ipv6** to the following command.

Kubernetes assigns IPv4 addresses to Pods and services, by default. Before deciding to use the IPv6 family, make sure that you're familiar with all of the considerations and requirements in the [the section called "VPC requirements and considerations" \(p. 256\)](#), [the section called "Subnet requirements and considerations" \(p. 257\)](#), [the section called "Security group requirements" \(p. 263\)](#), and [the section called "IPv6" \(p. 278\)](#) topics. If you choose the IPv6 family, you can't specify an address range for Kubernetes to assign IPv6 service addresses from like you can for the IPv4 family. Kubernetes assigns service addresses from the unique local address range (fc00::/7).

2. It takes several minutes to provision the cluster. You can query the status of your cluster with the following command.

```
aws eks describe-cluster --region region-code --name my-cluster --query "cluster.status"
```

Don't proceed to the next step until the output returned is ACTIVE.

3. If you created your cluster using eksctl, then you can skip this step. This is because eksctl already completed this step for you. Enable kubectl to communicate with your cluster by adding a new context to the kubectl config file. For more information about how to create and update the file, see [the section called "Creating kubeconfig file" \(p. 431\)](#).

```
aws eks update-kubeconfig --region region-code --name my-cluster
```

An example output is as follows.

```
Added new context arn:aws:eks:region-code:111122223333:cluster/my-cluster to /home/username/.kube/config
```

4. Confirm communication with your cluster by running the following command.

```
kubectl get svc
```

An example output is as follows.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
kubernetes	ClusterIP	10.100.0.1	<none>	443/TCP	28h

5. (Recommended) To use some Amazon EKS add-ons, or to enable individual Kubernetes workloads to have specific AWS Identity and Access Management (IAM) permissions, [create an IAM OpenID Connect \(OIDC\) provider \(p. 465\)](#) for your cluster. You only need to create an IAM OIDC provider for your cluster once. To learn more about Amazon EKS add-ons, see [Amazon EKS add-ons \(p. 385\)](#). To learn more about assigning specific IAM permissions to your workloads, see [the section called "IAM roles for service accounts" \(p. 464\)](#).
6. (Recommended) Configure your cluster for the Amazon VPC CNI plugin for Kubernetes plugin before deploying Amazon EC2 nodes to your cluster. By default, the plugin was installed with your cluster. When you add Amazon EC2 nodes to your cluster, the plugin is automatically deployed to each Amazon EC2 node that you add. The plugin requires you to attach one of the following IAM policies to an IAM role:

[AmazonEKS_CNI_Policy](#) managed IAM policy

If your cluster uses the IPv4 family

An [IAM policy that you create \(p. 276\)](#)

If your cluster uses the IPv6 family

The IAM role that you attach the policy to can be the node IAM role, or a dedicated role used only for the plugin. We recommend attaching the policy to this role. For more information about creating the role, see [the section called "Configure plugin for IAM account" \(p. 272\)](#) or [the section called "Node IAM role" \(p. 501\)](#).

7. If you deployed your cluster using the AWS Management Console, you can skip this step. The AWS Management Console deploys the Amazon VPC CNI plugin for Kubernetes, CoreDNS, and kube-proxy Amazon EKS add-ons, by default.

If you deploy your cluster using either eksctl or the AWS CLI, then the Amazon VPC CNI plugin for Kubernetes, CoreDNS, and kube-proxy self-managed add-ons are deployed. You can migrate the Amazon VPC CNI plugin for Kubernetes, CoreDNS, and kube-proxy self-managed add-ons that are deployed with your cluster to Amazon EKS add-ons. For more information, see [Amazon EKS add-ons \(p. 385\)](#).

8. If you plan to deploy workloads to your cluster that use Amazon EBS volumes , and you created a 1.23 or later cluster, then you must install the [the section called "Amazon EBS CSI driver" \(p. 228\)](#) to your cluster before deploying the workloads.

Recommended next steps:

- The [IAM principal](#) that created the cluster is the only principal that has access to the cluster. [Grant permissions to other IAM principals \(p. 420\)](#) so they can access your cluster.
- If the IAM principal that created the cluster only has the minimum IAM permissions referenced in the [prerequisites \(p. 26\)](#), then you might want to add additional Amazon EKS permissions for that principal. For more information about granting Amazon EKS permissions to IAM principals, see [the section called "Identity and access management" \(p. 478\)](#).
- If you want the IAM principal that created the cluster, or any other principals to view Kubernetes resources in the Amazon EKS console, grant the [the section called "Required permissions" \(p. 529\)](#) to the entities.
- If you want nodes and IAM principals to access your cluster from within your VPC, enable the private endpoint for your cluster. The public endpoint is enabled by default. You can disable the public endpoint once you've enabled the private endpoint, if desired. For more information, see [the section called "Configuring endpoint access" \(p. 41\)](#).
- [Enable secrets encryption for your cluster \(p. 46\)](#).
- [Configure logging for your cluster \(p. 536\)](#).
- [Add nodes to your cluster \(p. 77\)](#).

Updating an Amazon EKS cluster Kubernetes version

When a new Kubernetes version is available in Amazon EKS, you can update your Amazon EKS cluster to the latest version.

Important

Once you upgrade a cluster, you can't downgrade to a previous version. We recommend that, before you update to a new Kubernetes version, you review the information in [Amazon EKS Kubernetes versions \(p. 60\)](#) and also review in the update steps in this topic.

New Kubernetes versions sometimes introduce significant changes. Therefore, we recommend that you test the behavior of your applications against a new Kubernetes version before you update your production clusters. You can do this by building a continuous integration workflow to test your application behavior before moving to a new Kubernetes version.

The update process consists of Amazon EKS launching new API server nodes with the updated Kubernetes version to replace the existing ones. Amazon EKS performs standard infrastructure and readiness health checks for network traffic on these new nodes to verify that they're working as expected. However, once you've started the cluster upgrade, you can't pause or stop it. If any of these checks fail, Amazon EKS reverts the infrastructure deployment, and your cluster remains on the prior Kubernetes version. Running applications aren't affected, and your cluster is never left in a non-deterministic or unrecoverable state. Amazon EKS regularly backs up all managed clusters, and mechanisms exist to recover clusters if necessary. We're constantly evaluating and improving our Kubernetes infrastructure management processes.

To update the cluster, Amazon EKS requires up to five available IP addresses from the subnets that you specified when you created your cluster. Amazon EKS creates new cluster elastic network interfaces (network interfaces) in any of the subnets that you specified. The network interfaces may be created in different subnets than your existing network interfaces are in, so make sure that your security group rules allow [required cluster communication \(p. 263\)](#) for any of the subnets that you specified when you created your cluster. If any of the subnets that you specified when you created the cluster don't exist, don't have enough available IP addresses, or don't have security group rules that allows necessary cluster communication, then the update can fail.

Note

To ensure that the API server endpoint for your cluster is always accessible, Amazon EKS provides a highly available Kubernetes control plane and performs rolling updates of API server instances during update operations. In order to account for changing IP addresses of API server instances supporting your Kubernetes API server endpoint, you must ensure that your API server clients manage reconnects effectively. Recent versions of `kubectl` and the Kubernetes client [libraries](#) that are officially supported, perform this reconnect process transparently.

Update the Kubernetes version for your Amazon EKS cluster

To update the Kubernetes version for your cluster

1. Compare the Kubernetes version of your cluster control plane to the Kubernetes version of your nodes.
 - Get the Kubernetes version of your cluster control plane.

```
kubectl version --short
```

- Get the Kubernetes version of your nodes. This command returns all self-managed and managed Amazon EC2 and Fargate nodes. Each Fargate Pod is listed as its own node.

```
kubectl get nodes
```

Before updating your control plane to a new Kubernetes version, make sure that the Kubernetes minor version of both the managed nodes and Fargate nodes in your cluster are the same as your control plane's version. For example, if your control plane is running version 1.27 and one of your nodes is running version 1.26, then you must update your nodes to version 1.27 before updating your control plane to 1.28. We also recommend that you update your self-managed nodes to the same version as your control plane before updating the control plane. For more information, see [Updating a managed node group \(p. 91\)](#) and [Self-managed node updates \(p. 122\)](#). If you have Fargate nodes with a minor version lower than the control plane version, first delete the Pod that's represented by the node. Then update your control plane. Any remaining Pods will update to the new version after you redeploy them.

2. By default, the Pod security policy admission controller is enabled on Amazon EKS clusters. Before updating your cluster, ensure that the proper Pod security policies are in place. This is to avoid potential security issues. You can check for the default policy with the `kubectl get psp eks.privileged` command.

```
kubectl get psp eks.privileged
```

If you receive the following error, see [Amazon EKS default Pod security policy \(p. 522\)](#) before proceeding.

```
Error from server (NotFound): podsecuritypolicies.extensions "eks.privileged" not found
```

3. If the Kubernetes version that you originally deployed your cluster with was Kubernetes 1.18 or later, skip this step.

You might need to remove a discontinued term from your CoreDNS manifest.

- a. Check to see if your CoreDNS manifest has a line that only has the word upstream.

```
kubectl get configmap coredns -n kube-system -o jsonpath='{$.data.Corefile}' | grep upstream
```

If no output is returned, this means that your manifest doesn't have the line. If this is the case, skip to the next step. If the word upstream is returned, remove the line.

- b. Remove the line near the top of the file that only has the word upstream in the configmap file. Don't change anything else in the file. After the line is removed, save the changes.

```
kubectl edit configmap coredns -n kube-system -o yaml
```

4. Update your cluster using `eksctl`, the AWS Management Console, or the AWS CLI.

Important

- If you're updating to version 1.23 and use Amazon EBS volumes in your cluster, then you must install the Amazon EBS CSI driver in your cluster before updating your cluster to version 1.23 to avoid workload disruptions. For more information, see [the section called "Kubernetes 1.23" \(p. 70\)](#) and [the section called "Amazon EBS CSI driver" \(p. 228\)](#).
- Kubernetes 1.24 and later use `containerd` as the default container runtime. If you're switching to the `containerd` runtime and already have Fluentd configured for Container

Insights, then you must migrate Fluentd to Fluent Bit before updating your cluster. The Fluentd parsers are configured to only parse log messages in JSON format. Unlike dockererd, the containererd container runtime has log messages that aren't in JSON format. If you don't migrate to Fluent Bit, some of the configured Fluentd's parsers will generate a massive amount of errors inside the Fluentd container. For more information on migrating, see [Set up Fluent Bit as a DaemonSet to send logs to CloudWatch Logs](#).

- Because Amazon EKS runs a highly available control plane, you can update only one minor version at a time. For more information about this requirement, see [Kubernetes Version and Version Skew Support Policy](#). Assume that your current cluster version is version 1.26 and you want to update it to version 1.28. You must first update your version 1.26 cluster to version 1.27 and then update your version 1.27 cluster to version 1.28.
- Make sure that the kubelet on your managed and Fargate nodes are at the same Kubernetes version as your control plane before you update. We recommend that your self-managed nodes are at the same version as the control plane. They can be only up to one version behind the current version of the control plane.
- If your cluster is configured with a version of the Amazon VPC CNI plugin for Kubernetes that is earlier than 1.8.0, then we recommend that you update the plugin to the latest version before updating your cluster. To update the plugin, see [the section called "Amazon VPC CNI plugin for Kubernetes" \(p. 266\)](#).
- If you're updating your cluster to version 1.25 or later and have the AWS Load Balancer Controller deployed in your cluster, then update the controller to version 2.4.7 or later *before* updating your cluster version to 1.25. For more information, see the [the section called "Kubernetes 1.25" \(p. 66\)](#) release notes.

eksctl

This procedure requires eksctl version 0.160.0 or later. You can check your version with the following command:

```
eksctl version
```

For instructions on how to install and update eksctl, see [Installing or updating eksctl \(p. 13\)](#).

Update the Kubernetes version of your Amazon EKS control plane. Replace *my-cluster* with your cluster name. Replace **1.28** with the Amazon EKS supported version number that you want to update your cluster to. For a list of supported version numbers, see [the section called "Kubernetes versions" \(p. 60\)](#).

```
eksctl upgrade cluster --name my-cluster --version 1.28 --approve
```

The update takes several minutes to complete.

AWS Management Console

- a. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
- b. Choose the name of the Amazon EKS cluster to update and choose **Update cluster version**.
- c. For **Kubernetes version**, select the version to update your cluster to and choose **Update**.
- d. For **Cluster name**, enter the name of your cluster and choose **Confirm**.

The update takes several minutes to complete.

AWS CLI

- a. Update your Amazon EKS cluster with the following AWS CLI command. Replace the *example values* with your own. Replace **1.28** with the Amazon EKS supported version number that you want to update your cluster to. For a list of supported version numbers, see [the section called "Kubernetes versions" \(p. 60\)](#).

```
aws eks update-cluster-version --region region-code --name my-cluster --  
kubernetes-version 1.28
```

An example output is as follows.

```
{  
    "update": {  
        "id": "b5f0ba18-9a87-4450-b5a0-825e6e84496f",  
        "status": "InProgress",  
        "type": "VersionUpdate",  
        "params": [  
            {  
                "type": "Version",  
                "value": "1.28"  
            },  
            {  
                "type": "PlatformVersion",  
                "value": "eks.1"  
            }  
        ],  
        [...]  
        "errors": []  
    }  
}
```

- b. Monitor the status of your cluster update with the following command. Use the cluster name and update ID that the previous command returned. When a Successful status is displayed, the update is complete. The update takes several minutes to complete.

```
aws eks describe-update --region region-code --name my-cluster --update-  
id b5f0ba18-9a87-4450-b5a0-825e6e84496f
```

An example output is as follows.

```
{  
    "update": {  
        "id": "b5f0ba18-9a87-4450-b5a0-825e6e84496f",  
        "status": "Successful",  
        "type": "VersionUpdate",  
        "params": [  
            {  
                "type": "Version",  
                "value": "1.28"  
            },  
            {  
                "type": "PlatformVersion",  
                "value": "eks.1"  
            }  
        ],  
        [...]  
        "errors": []  
    }  
}
```

{}

5. After your cluster update is complete, update your nodes to the same Kubernetes minor version as your updated cluster. For more information, see [Self-managed node updates \(p. 122\)](#) and [Updating a managed node group \(p. 91\)](#). Any new Pods that are launched on Fargate have a kubelet version that matches your cluster version. Existing Fargate Pods aren't changed.
6. (Optional) If you deployed the Kubernetes Cluster Autoscaler to your cluster before updating the cluster, update the Cluster Autoscaler to the latest version that matches the Kubernetes major and minor version that you updated to.
 - a. Open the Cluster Autoscaler [releases](#) page in a web browser and find the latest Cluster Autoscaler version that matches your cluster's Kubernetes major and minor version. For example, if your cluster's Kubernetes version is 1.28 find the latest Cluster Autoscaler release that begins with 1.28. Record the semantic version number (1.28.n, for example) for that release to use in the next step.
 - b. Set the Cluster Autoscaler image tag to the version that you recorded in the previous step with the following command. If necessary, replace **1.28.n** with your own value.

```
kubectl -n kube-system set image deployment.apps/cluster-autoscaler cluster-autoscaler=registry.k8s.io/autoscaling/cluster-autoscaler:v1.28.n
```

7. (Clusters with GPU nodes only) If your cluster has node groups with GPU support (for example, p3.2xlarge), you must update the [NVIDIA device plugin for Kubernetes](#) DaemonSet on your cluster. Replace **vX.X.X** with your desired [NVIDIA/k8s-device-plugin](#) version before running the following command.

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/vX.X.X/nvidia-device-plugin.yml
```

8. Update the Amazon VPC CNI plugin for Kubernetes, CoreDNS, and kube-proxy add-ons. We recommend updating the add-ons to the minimum versions listed in [Service account tokens \(p. 463\)](#).
 - If you are using Amazon EKS add-ons, select **Clusters** in the Amazon EKS console, then select the name of the cluster that you updated in the left navigation pane. Notifications appear in the console. They inform you that a new version is available for each add-on that has an available update. To update an add-on, select the **Add-ons** tab. In one of the boxes for an add-on that has an update available, select **Update now**, select an available version, and then select **Update**.
 - Alternately, you can use the AWS CLI or eksctl to update add-ons. For more information, see [the section called "Updating an add-on" \(p. 400\)](#).
9. If necessary, update your version of kubectl. You must use a kubectl version that is within one minor version difference of your Amazon EKS cluster control plane. For example, a 1.27 kubectl client works with Kubernetes 1.26, 1.27, and 1.28 clusters. You can check your currently installed version with the following command.

```
kubectl version --short --client
```

Deleting an Amazon EKS cluster

When you're done using an Amazon EKS cluster, you should delete the resources associated with it so that you don't incur any unnecessary costs.

To remove a connected cluster, see [Deregistering a cluster \(p. 580\)](#)

Important

- If you have active services in your cluster that are associated with a load balancer, you must delete those services before deleting the cluster so that the load balancers are deleted properly. Otherwise, you can have orphaned resources in your VPC that prevent you from being able to delete the VPC.
- If you receive an error because the cluster creator has been removed, see [this article](#) to resolve.

You can delete a cluster with `eksctl`, the AWS Management Console, or the AWS CLI.

`eksctl`

To delete an Amazon EKS cluster and nodes with `eksctl`

This procedure requires `eksctl` version `0.160.0` or later. You can check your version with the following command:

```
eksctl version
```

For instructions on how to install or upgrade `eksctl`, see [Installing or updating eksctl \(p. 13\)](#).

1. List all services running in your cluster.

```
kubectl get svc --all-namespaces
```

2. Delete any services that have an associated EXTERNAL-IP value. These services are fronted by an Elastic Load Balancing load balancer, and you must delete them in Kubernetes to allow the load balancer and associated resources to be properly released.

```
kubectl delete svc service-name
```

3. Delete the cluster and its associated nodes with the following command, replacing `prod` with your cluster name.

```
eksctl delete cluster --name prod
```

Output:

```
[#] using region region-code
[#] deleting EKS cluster "prod"
[#] will delete stack "eksctl-prod-nodegroup-standard-nodes"
[#] waiting for stack "eksctl-prod-nodegroup-standard-nodes" to get deleted
[#] will delete stack "eksctl-prod-cluster"
[#] the following EKS cluster resource(s) for "prod" will be deleted: cluster. If
    in doubt, check CloudFormation console
```

AWS Management Console

To delete an Amazon EKS cluster with the AWS Management Console

1. List all services running in your cluster.

```
kubectl get svc --all-namespaces
```

2. Delete any services that have an associated EXTERNAL-IP value. These services are fronted by an Elastic Load Balancing load balancer, and you must delete them in Kubernetes to allow the load balancer and associated resources to be properly released.

```
kubectl delete svc service-name
```

3. Delete all node groups and Fargate profiles.
 - a. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
 - b. In the left navigation pane, choose Amazon EKS **Clusters**, and then in the tabbed list of clusters, choose the name of the cluster that you want to delete.
 - c. Choose the **Compute** tab and choose a node group to delete. Choose **Delete**, enter the name of the node group, and then choose **Delete**. Delete all node groups in the cluster.
- Note**
The node groups listed are [managed node groups \(p. 81\)](#) only.

 - d. Choose a **Fargate Profile** to delete, select **Delete**, enter the name of the profile, and then choose **Delete**. Delete all Fargate profiles in the cluster.
4. Delete all self-managed node AWS CloudFormation stacks.
 - a. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
 - b. Choose the node stack to delete, and then choose **Delete**.
 - c. In the **Delete stack** confirmation dialog box, choose **Delete stack**. Delete all self-managed node stacks in the cluster.
5. Delete the cluster.
 - a. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
 - b. choose the cluster to delete and choose **Delete**.
 - c. On the delete cluster confirmation screen, choose **Delete**.
6. (Optional) Delete the VPC AWS CloudFormation stack.
 - a. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
 - b. Select the VPC stack to delete, and then choose **Delete**.
 - c. In the **Delete stack** confirmation dialog box, choose **Delete stack**.

AWS CLI

To delete an Amazon EKS cluster with the AWS CLI

1. List all services running in your cluster.

```
kubectl get svc --all-namespaces
```

2. Delete any services that have an associated EXTERNAL-IP value. These services are fronted by an Elastic Load Balancing load balancer, and you must delete them in Kubernetes to allow the load balancer and associated resources to be properly released.

```
kubectl delete svc service-name
```

3. Delete all node groups and Fargate profiles.

- a. List the node groups in your cluster with the following command.

```
aws eks list-nodegroups --cluster-name my-cluster
```

Note

The node groups listed are [managed node groups \(p. 81\)](#) only.

- b. Delete each node group with the following command. Delete all node groups in the cluster.

```
aws eks delete-nodegroup --nodegroup-name my-nodegroup --cluster-name my-cluster
```

- c. List the Fargate profiles in your cluster with the following command.

```
aws eks list-fargate-profiles --cluster-name my-cluster
```

- d. Delete each Fargate profile with the following command. Delete all Fargate profiles in the cluster.

```
aws eks delete-fargate-profile --fargate-profile-name my-fargate-profile --cluster-name my-cluster
```

4. Delete all self-managed node AWS CloudFormation stacks.

- a. List your available AWS CloudFormation stacks with the following command. Find the node template name in the resulting output.

```
aws cloudformation list-stacks --query "StackSummaries[].StackName"
```

- b. Delete each node stack with the following command, replacing *node-stack* with your node stack name. Delete all self-managed node stacks in the cluster.

```
aws cloudformation delete-stack --stack-name node-stack
```

5. Delete the cluster with the following command, replacing *my-cluster* with your cluster name.

```
aws eks delete-cluster --name my-cluster
```

6. (Optional) Delete the VPC AWS CloudFormation stack.

- a. List your available AWS CloudFormation stacks with the following command. Find the VPC template name in the resulting output.

```
aws cloudformation list-stacks --query "StackSummaries[].StackName"
```

- b. Delete the VPC stack with the following command, replacing *my-vpc-stack* with your VPC stack name.

```
aws cloudformation delete-stack --stack-name my-vpc-stack
```

Amazon EKS cluster endpoint access control

This topic helps you to enable private access for your Amazon EKS cluster's Kubernetes API server endpoint and limit, or completely disable, public access from the internet.

When you create a new cluster, Amazon EKS creates an endpoint for the managed Kubernetes API server that you use to communicate with your cluster (using Kubernetes management tools such as `kubectl`).

By default, this API server endpoint is public to the internet, and access to the API server is secured using a combination of AWS Identity and Access Management (IAM) and native Kubernetes [Role Based Access Control \(RBAC\)](#).

You can enable private access to the Kubernetes API server so that all communication between your nodes and the API server stays within your VPC. You can limit the IP addresses that can access your API server from the internet, or completely disable internet access to the API server.

Note

Because this endpoint is for the Kubernetes API server and not a traditional AWS PrivateLink endpoint for communicating with an AWS API, it doesn't appear as an endpoint in the Amazon VPC console.

When you enable endpoint private access for your cluster, Amazon EKS creates a Route 53 private hosted zone on your behalf and associates it with your cluster's VPC. This private hosted zone is managed by Amazon EKS, and it doesn't appear in your account's Route 53 resources. In order for the private hosted zone to properly route traffic to your API server, your VPC must have `enableDnsHostnames` and `enableDnsSupport` set to `true`, and the DHCP options set for your VPC must include `AmazonProvidedDNS` in its domain name servers list. For more information, see [Updating DNS support for your VPC](#) in the *Amazon VPC User Guide*.

You can define your API server endpoint access requirements when you create a new cluster, and you can update the API server endpoint access for a cluster at any time.

Modifying cluster endpoint access

Use the procedures in this section to modify the endpoint access for an existing cluster. The following table shows the supported API server endpoint access combinations and their associated behavior.

API server endpoint access options

Endpoint public access	Endpoint private access	Behavior
Enabled	Disabled	<ul style="list-style-type: none">This is the default behavior for new Amazon EKS clusters.Kubernetes API requests that originate from within your cluster's VPC (such as node to control plane communication) leave the VPC but not Amazon's network.Your cluster API server is accessible from the internet. You can, optionally, limit the CIDR blocks that can access the public endpoint. If you limit access to specific CIDR blocks, then it is recommended that you also enable the private endpoint, or ensure that the CIDR blocks that you specify include the addresses that nodes and Fargate Pods (if you use them) access the public endpoint from.
Enabled	Enabled	<ul style="list-style-type: none">Kubernetes API requests within your cluster's VPC

Endpoint public access	Endpoint private access	Behavior
		<p>(such as node to control plane communication) use the private VPC endpoint.</p> <ul style="list-style-type: none"> Your cluster API server is accessible from the internet. You can, optionally, limit the CIDR blocks that can access the public endpoint.
Disabled	Enabled	<ul style="list-style-type: none"> All traffic to your cluster API server must come from within your cluster's VPC or a connected network. There is no public access to your API server from the internet. Any <code>kubectl</code> commands must come from within the VPC or a connected network. For connectivity options, see Accessing a private only API server (p. 46). The cluster's API server endpoint is resolved by public DNS servers to a private IP address from the VPC. In the past, the endpoint could only be resolved from within the VPC. <p>If your endpoint does not resolve to a private IP address within the VPC for an existing cluster, you can:</p> <ul style="list-style-type: none"> Enable public access and then disable it again. You only need to do so once for a cluster and the endpoint will resolve to a private IP address from that point forward. Update (p. 34) your cluster.

You can modify your cluster API server endpoint access using the AWS Management Console or AWS CLI.

AWS Management Console

To modify your cluster API server endpoint access using the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose the name of the cluster to display your cluster information.
3. Choose the **Networking** tab and choose **Update**.

4. For **Private access**, choose whether to enable or disable private access for your cluster's Kubernetes API server endpoint. If you enable private access, Kubernetes API requests that originate from within your cluster's VPC use the private VPC endpoint. You must enable private access to disable public access.
5. For **Public access**, choose whether to enable or disable public access for your cluster's Kubernetes API server endpoint. If you disable public access, your cluster's Kubernetes API server can only receive requests from within the cluster VPC.
6. (Optional) If you've enabled **Public access**, you can specify which addresses from the internet can communicate to the public endpoint. Select **Advanced Settings**. Enter a CIDR block, such as **203.0.113.5/32**. The block cannot include [reserved addresses](#). You can enter additional blocks by selecting **Add Source**. There is a maximum number of CIDR blocks that you can specify. For more information, see [Amazon EKS service quotas \(p. 455\)](#). If you specify no blocks, then the public API server endpoint receives requests from all (0.0.0.0/0) IP addresses. If you restrict access to your public endpoint using CIDR blocks, it is recommended that you also enable private endpoint access so that nodes and Fargate Pods (if you use them) can communicate with the cluster. Without the private endpoint enabled, your public access endpoint CIDR sources must include the egress sources from your VPC. For example, if you have a node in a private subnet that communicates to the internet through a NAT Gateway, you will need to add the outbound IP address of the NAT gateway as part of an allowed CIDR block on your public endpoint.
7. Choose **Update** to finish.

AWS CLI

To modify your cluster API server endpoint access using the AWS CLI

Complete the following steps using the AWS CLI version 1.27.160 or later. You can check your current version with `aws --version`. To install or upgrade the AWS CLI, see [Installing the AWS CLI](#).

1. Update your cluster API server endpoint access with the following AWS CLI command. Substitute your cluster name and desired endpoint access values. If you set `endpointPublicAccess=true`, then you can (optionally) enter single CIDR block, or a comma-separated list of CIDR blocks for `publicAccessCidrs`. The blocks cannot include [reserved addresses](#). If you specify CIDR blocks, then the public API server endpoint will only receive requests from the listed blocks. There is a maximum number of CIDR blocks that you can specify. For more information, see [Amazon EKS service quotas \(p. 455\)](#). If you restrict access to your public endpoint using CIDR blocks, it is recommended that you also enable private endpoint access so that nodes and Fargate Pods (if you use them) can communicate with the cluster. Without the private endpoint enabled, your public access endpoint CIDR sources must include the egress sources from your VPC. For example, if you have a node in a private subnet that communicates to the internet through a NAT Gateway, you will need to add the outbound IP address of the NAT gateway as part of an allowed CIDR block on your public endpoint. If you specify no CIDR blocks, then the public API server endpoint receives requests from all (0.0.0.0/0) IP addresses.

Note

The following command enables private access and public access from a single IP address for the API server endpoint. Replace **203.0.113.5/32** with a single CIDR block, or a comma-separated list of CIDR blocks that you want to restrict network access to.

```
aws eks update-cluster-config \
--region region-code \
--name my-cluster \
--resources-vpc-config
endpointPublicAccess=true,publicAccessCidrs="203.0.113.5/32",endpointPrivateAccess=true
```

An example output is as follows.

```
{
  "update": {
    "id": "e6f0905f-a5d4-4a2a-8c49-EXAMPLE00000",
    "status": "InProgress",
    "type": "EndpointAccessUpdate",
    "params": [
      {
        "type": "EndpointPublicAccess",
        "value": "true"
      },
      {
        "type": "EndpointPrivateAccess",
        "value": "true"
      },
      {
        "type": "publicAccessCidrs",
        "value": "[\203.0.113.5/32\""
      }
    ],
    "createdAt": 1576874258.137,
    "errors": []
  }
}
```

2. Monitor the status of your endpoint access update with the following command, using the cluster name and update ID that was returned by the previous command. Your update is complete when the status is shown as Successful.

```
aws eks describe-update \
  --region region-code \
  --name my-cluster \
  --update-id e6f0905f-a5d4-4a2a-8c49-EXAMPLE00000
```

An example output is as follows.

```
{
  "update": {
    "id": "e6f0905f-a5d4-4a2a-8c49-EXAMPLE00000",
    "status": "Successful",
    "type": "EndpointAccessUpdate",
    "params": [
      {
        "type": "EndpointPublicAccess",
        "value": "true"
      },
      {
        "type": "EndpointPrivateAccess",
        "value": "true"
      },
      {
        "type": "publicAccessCidrs",
        "value": "[\203.0.113.5/32\""
      }
    ],
    "createdAt": 1576874258.137,
    "errors": []
  }
}
```

Accessing a private only API server

If you have disabled public access for your cluster's Kubernetes API server endpoint, you can only access the API server from within your VPC or a [connected network](#). Here are a few possible ways to access the Kubernetes API server endpoint:

Connected network

Connect your network to the VPC with an [AWS transit gateway](#) or other [connectivity](#) option and then use a computer in the connected network. You must ensure that your Amazon EKS control plane security group contains rules to allow ingress traffic on port 443 from your connected network.

Amazon EC2 bastion host

You can launch an Amazon EC2 instance into a public subnet in your cluster's VPC and then log in via SSH into that instance to run `kubectl` commands. For more information, see [Linux bastion hosts on AWS](#). You must ensure that your Amazon EKS control plane security group contains rules to allow ingress traffic on port 443 from your bastion host. For more information, see [Amazon EKS security group requirements and considerations \(p. 263\)](#).

When you configure `kubectl` for your bastion host, be sure to use AWS credentials that are already mapped to your cluster's RBAC configuration, or add the [IAM principal](#) that your bastion will use to the RBAC configuration before you remove endpoint public access. For more information, see [Enabling IAM principal access to your cluster \(p. 420\)](#) and [Unauthorized or access denied \(kubectl\) \(p. 563\)](#).

AWS Cloud9 IDE

AWS Cloud9 is a cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser. You can create an AWS Cloud9 IDE in your cluster's VPC and use the IDE to communicate with your cluster. For more information, see [Creating an environment in AWS Cloud9](#). You must ensure that your Amazon EKS control plane security group contains rules to allow ingress traffic on port 443 from your IDE security group. For more information, see [Amazon EKS security group requirements and considerations \(p. 263\)](#).

When you configure `kubectl` for your AWS Cloud9 IDE, be sure to use AWS credentials that are already mapped to your cluster's RBAC configuration, or add the IAM principal that your IDE will use to the RBAC configuration before you remove endpoint public access. For more information, see [Enabling IAM principal access to your cluster \(p. 420\)](#) and [Unauthorized or access denied \(kubectl\) \(p. 563\)](#).

Enabling secret encryption on an existing cluster

If you enable [secrets encryption](#), the Kubernetes secrets are encrypted using the AWS KMS key that you select. The KMS key must meet the following conditions:

- Symmetric
- Can encrypt and decrypt data
- Created in the same AWS Region as the cluster
- If the KMS key was created in a different account, the [IAM principal](#) must have access to the KMS key.

For more information, see [Allowing IAM principals in other accounts to use a KMS key](#) in the [AWS Key Management Service Developer Guide](#).

Warning

You can't disable secrets encryption after enabling it. This action is irreversible.

eksctl

You can enable encryption in two ways:

- Add encryption to your cluster with a single command.

To automatically re-encrypt your secrets, run the following command.

```
eksctl utils enable-secrets-encryption \
--cluster my-cluster \
--key-arn arn:aws:kms:region-code:account:key/key
```

To opt-out of automatically re-encrypting your secrets, run the following command.

```
eksctl utils enable-secrets-encryption
--cluster my-cluster \
--key-arn arn:aws:kms:region-code:account:key/key \
--encrypt-existing-secrets=false
```

- Add encryption to your cluster with a `kms-cluster.yaml` file.

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-cluster
  region: region-code

secretsEncryption:
  keyARN: arn:aws:kms:region-code:account:key/key
```

To have your secrets re-encrypt automatically, run the following command.

```
eksctl utils enable-secrets-encryption -f kms-cluster.yaml
```

To opt out of automatically re-encrypting your secrets, run the following command.

```
eksctl utils enable-secrets-encryption -f kms-cluster.yaml --encrypt-existing-
secrets=false
```

AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose the cluster that you want to add KMS encryption to.
3. Choose the **Overview** tab (this is selected by default).
4. Scroll down to the **Secrets encryption** section and choose **Enable**.
5. Select a key from the dropdown list and choose the **Enable** button. If no keys are listed, you must create one first. For more information, see [Creating keys](#).
6. Choose the **Confirm** button to use the chosen key.

AWS CLI

1. Associate the **secrets encryption** configuration with your cluster using the following AWS CLI command. Replace the *example values* with your own.

```
aws eks associate-encryption-config \
--cluster-name my-cluster \
--encryption-config '[{"resources":["secrets"],"provider": {"keyArn":"arn:aws:kms:region-code:account:key/key"}}]'
```

An example output is as follows.

```
{  
  "update": {  
    "id": "3141b835-8103-423a-8e68-12c2521ffa4d",  
    "status": "InProgress",  
    "type": "AssociateEncryptionConfig",  
    "params": [  
      {  
        "type": "EncryptionConfig",  
        "value": "[{\\"resources\\": [\"secrets\"], \\"provider\\": {\\\"keyArn\\": \"arn:aws:kms:region-code:account:key/key\"}}]\"  
      }  
    ],  
    "createdAt": 1613754188.734,  
    "errors": []  
  }  
}
```

2. You can monitor the status of your encryption update with the following command. Use the specific cluster name and update ID that was returned in the previous output. When a Successful status is displayed, the update is complete.

```
aws eks describe-update \
--region region-code \
--name my-cluster \
--update-id 3141b835-8103-423a-8e68-12c2521ffa4d
```

An example output is as follows.

```
{  
  "update": {  
    "id": "3141b835-8103-423a-8e68-12c2521ffa4d",  
    "status": "Successful",  
    "type": "AssociateEncryptionConfig",  
    "params": [  
      {  
        "type": "EncryptionConfig",  
        "value": "[{\\"resources\\": [\"secrets\"], \\"provider\\": {\\\"keyArn\\": \"arn:aws:kms:region-code:account:key/key\"}}]\"  
      }  
    ],  
    "createdAt": 1613754188.734,  
    "errors": []  
  }  
}
```

3. To verify that encryption is enabled in your cluster, run the `describe-cluster` command. The response contains an `EncryptionConfig` string.

```
aws eks describe-cluster --region region-code --name my-cluster
```

After you enabled encryption on your cluster, you must encrypt all existing secrets with the new key:

Note

If you use `eksctl`, running the following command is necessary only if you opt out of re-encrypting your secrets automatically.

```
kubectl get secrets --all-namespaces -o json | kubectl annotate --overwrite -f - kms-  
encryption-timestamp="time value"
```

Warning

If you enable [secrets encryption](#) for an existing cluster and the KMS key that you use is ever deleted, then there's no way to recover the cluster. If you delete the KMS key, you permanently put the cluster in a degraded state. For more information, see [Deleting AWS KMS keys](#).

Note

By default, the `create-key` command creates a [symmetric encryption KMS key](#) with a key policy that gives the account root admin access on AWS KMS actions and resources. If you want to scope down the permissions, make sure that the `kms:DescribeKey` and `kms:CreateGrant` actions are permitted on the policy for the principal that calls the `create-cluster` API. For clusters using KMS Envelope Encryption, `kms:CreateGrant` permissions are required. The condition `kms:GrantIsForAWSResource` is not supported for the `CreateCluster` action, and should not be used in KMS policies to control `kms:CreateGrant` permissions for users performing `CreateCluster`.

Enabling Windows support for your Amazon EKS cluster

Before deploying Windows nodes, be aware of the following considerations.

Considerations

- You can use host networking on Windows nodes using HostProcess Pods. For more information, see [Create a Windows HostProcessPod](#) in the Kubernetes documentation.
- Amazon EKS clusters must contain one or more Linux or Fargate nodes to run core system Pods that only run on Linux, such as CoreDNS.
- The `kubelet` and `kube-proxy` event logs are redirected to the EKS Windows Event Log and are set to a 200 MB limit.
- You can't use [Tutorial: Security groups for Pods \(p. 324\)](#) with Pods running on Windows nodes.
- You can't use [custom networking \(p. 306\)](#) with Windows nodes.
- You can't use IPv6 with Windows nodes.
- Windows nodes support one elastic network interface per node. By default, the number of Pods that you can run per Windows node is equal to the number of IP addresses available per elastic network interface for the node's instance type, minus one. For more information, see [IP addresses per network interface per instance type](#) in the *Amazon EC2 User Guide for Windows Instances*.
- In an Amazon EKS cluster, a single service with a load balancer can support up to 1024 back-end Pods. Each Pod has its own unique IP address. The previous limit of 64 Pods is no longer the case, after [Windows Server update](#) starting with [OS Build 17763.2746](#).
- Windows containers aren't supported for Amazon EKS Pods on Fargate.
- You can't retrieve logs from the `vpc-resource-controller` Pod. You previously could when you deployed the controller to the data plane.
- There is a cool down period before an IPv4 address is assigned to a new Pod. This prevents traffic from flowing to an older Pod with the same IPv4 address due to stale `kube-proxy` rules.
- The source for the controller is managed on GitHub. To contribute to, or file issues against the controller, visit the [project](#) on GitHub.

- When specifying a custom AMI ID for Windows managed node groups, add eks:kube-proxy-windows to your AWS IAM Authenticator configuration map. For more information, see [Limits and conditions when specifying an AMI ID \(p. 106\)](#).

Prerequisites

- An existing cluster. The cluster must be running one of the Kubernetes versions and platform versions listed in the following table. Any Kubernetes and platform versions later than those listed are also supported. If your cluster or platform version is earlier than one of the following versions, you need to [enable legacy Windows support \(p. 53\)](#) on your cluster's data plane. Once your cluster is at one of the following Kubernetes and platform versions, or later, you can [remove legacy Windows support \(p. 51\)](#) and [enable Windows support \(p. 50\)](#) on your control plane.

Kubernetes version	Platform version
1.28	eks.1
1.27	eks.1
1.26	eks.1
1.25	eks.1
1.24	eks.2
1.23	eks.1

- Your cluster must have at least one (we recommend at least two) Linux node or Fargate Pod to run CoreDNS. If you enable legacy Windows support, you must use a Linux node (you can't use a Fargate Pod) to run CoreDNS.
- An existing [Amazon EKS cluster IAM role \(p. 499\)](#).

Enabling Windows support

If your cluster isn't at, or later, than one of the Kubernetes and platform versions listed in the [Prerequisites \(p. 50\)](#), you must enable legacy Windows support instead. For more information, see [Enabling legacy Windows support \(p. 53\)](#).

If you've never enabled Windows support on your cluster, skip to the next step.

If you enabled Windows support on a cluster that is earlier than a Kubernetes or platform version listed in the [Prerequisites \(p. 50\)](#), then you must first [remove the vpc-resource-controller and vpc-admission-webhook from your data plane \(p. 51\)](#). They're deprecated and no longer needed.

To enable Windows support for your cluster

- If you don't have Amazon Linux nodes in your cluster and use security groups for Pods, skip to the next step. Otherwise, confirm that the AmazonEKSVPCCResourceController managed policy is attached to your [cluster role \(p. 499\)](#). Replace `eksClusterRole` with your cluster role name.

```
aws iam list-attached-role-policies --role-name eksClusterRole
```

An example output is as follows.

```
{
```

```

    "AttachedPolicies": [
      {
        "PolicyName": "AmazonEKSClusterPolicy",
        "PolicyArn": "arn:aws:iam::aws:policy/AmazonEKSClusterPolicy"
      },
      {
        "PolicyName": "AmazonEKSVPCCResourceController",
        "PolicyArn": "arn:aws:iam::aws:policy/AmazonEKSVPCCResourceController"
      }
    ]
}

```

If the policy is attached, as it is in the previous output, skip the next step.

2. Attach the [AmazonEKSVPCCResourceController](#) managed policy to your [Amazon EKS cluster IAM role \(p. 499\)](#). Replace `eksClusterRole` with your cluster role name.

```

aws iam attach-role-policy \
--role-name eksClusterRole \
--policy-arn arn:aws:iam::aws:policy/AmazonEKSVPCCResourceController

```

3. Create a file named `vpc-resource-controller-configmap.yaml` with the following contents.

```

apiVersion: v1
kind: ConfigMap
metadata:
  name: amazon-vpc-cni
  namespace: kube-system
data:
  enable-windows-ipam: "true"

```

4. Apply the ConfigMap to your cluster.

```

kubectl apply -f vpc-resource-controller-configmap.yaml

```

Removing legacy Windows support from your data plane

If you enabled Windows support on a cluster that is earlier than a Kubernetes or platform version listed in the [Prerequisites \(p. 50\)](#), then you must first remove the `vpc-resource-controller` and `vpc-admission-webhook` from your data plane. They're deprecated and no longer needed because the functionality that they provided is now enabled on the control plane.

1. Uninstall the `vpc-resource-controller` with the following command. Use this command regardless of which tool you originally installed it with. Replace `region-code` (only the instance of that text after `/manifests/`) with the AWS Region that your cluster is in.

```

kubectl delete -f https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-resource-controller/latest/vpc-resource-controller.yaml

```

2. Uninstall the `vpc-admission-webhook` using the instructions for the tool that you installed it with.

`eksctl`

Run the following commands.

```
kubectl delete deployment -n kube-system vpc-admission-webhook
kubectl delete service -n kube-system vpc-admission-webhook
kubectl delete mutatingwebhookconfigurations.admissionregistration.k8s.io vpc-
admission-webhook-cfg
```

kubectl on macOS or Windows

Run the following command. Replace *region-code* (only the instance of that text after / manifests/) with the AWS Region that your cluster is in.

```
kubectl delete -f https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-
code/vpc-admission-webhook/latest/vpc-admission-webhook-deployment.yaml
```

3. [Enable Windows support \(p. 50\)](#) for your cluster on the control plane.

Disabling Windows support

To disable Windows support on your cluster

1. If your cluster contains Amazon Linux nodes and you use [security groups for Pods \(p. 324\)](#) with them, then skip this step.

Remove the AmazonVPCResourceController managed IAM policy from your [cluster role \(p. 499\)](#). Replace *eksClusterRole* with the name of your cluster role and *111122223333* with your account ID.

```
aws iam detach-role-policy \
--role-name eksClusterRole \
--policy-arn arn:aws:iam::aws:policy/AmazonEKSVPCCResourceController
```

2. Disable Windows IPAM in the amazon-vpc-cni ConfigMap.

```
kubectl patch configmap/amazon-vpc-cni \
-n kube-system \
--type merge \
-p '{"data":{"enable-windows-ipam":"false"}}'
```

Deploying Pods

When you deploy Pods to your cluster, you need to specify the operating system that they use if you're running a mixture of node types.

For Linux Pods, use the following node selector text in your manifests.

```
nodeSelector:
  kubernetes.io/os: linux
  kubernetes.io/arch: amd64
```

For Windows Pods, use the following node selector text in your manifests.

```
nodeSelector:
  kubernetes.io/os: windows
  kubernetes.io/arch: amd64
```

You can deploy a [sample application \(p. 356\)](#) to see the node selectors in use.

Enabling legacy Windows support

If your cluster is at, or later, than one of the Kubernetes and platform versions listed in the [Prerequisites \(p. 50\)](#), then we recommend that you enable Windows support on your control plane instead. For more information, see [Enabling Windows support \(p. 50\)](#).

The following steps help you to enable legacy Windows support for your Amazon EKS cluster's data plane if your cluster or platform version are earlier than the versions listed in the [Prerequisites \(p. 50\)](#). Once your cluster and platform version are at, or later than a version listed in the [Prerequisites \(p. 50\)](#), we recommend that you [remove legacy Windows support \(p. 51\)](#) and [enable it for your control plane \(p. 50\)](#).

You can use eksctl, a Windows client, or a macOS or Linux client to enable legacy Windows support for your cluster.

eksctl

To enable legacy Windows support for your cluster with eksctl

Prerequisite

This procedure requires eksctl version 0.160.0 or later. You can check your version with the following command.

```
eksctl version
```

For more information about installing or upgrading eksctl, see [Installing or updating eksctl \(p. 13\)](#).

1. Enable Windows support for your Amazon EKS cluster with the following eksctl command. Replace *my-cluster* with the name of your cluster. This command deploys the VPC resource controller and VPC admission controller webhook that are required on Amazon EKS clusters to run Windows workloads.

```
eksctl utils install-vpc-controllers --cluster my-cluster --approve
```

Important

The VPC admission controller webhook is signed with a certificate that expires one year after the date of issue. To avoid down time, make sure to renew the certificate before it expires. For more information, see [Renewing the VPC admission webhook certificate \(p. 56\)](#).

2. After you have enabled Windows support, you can launch a Windows node group into your cluster. For more information, see [Launching self-managed Windows nodes \(p. 117\)](#).

Windows

To enable legacy Windows support for your cluster with a Windows client

In the following steps, replace *region-code* with the AWS Region that your cluster resides in.

1. Deploy the VPC resource controller to your cluster.

```
kubectl apply -f https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-resource-controller/latest/vpc-resource-controller.yaml
```

2. Deploy the VPC admission controller webhook to your cluster.

- a. Download the required scripts and deployment files.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-admission-webhook/latest/vpc-admission-webhook-deployment.yaml;
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-admission-webhook/latest/Setup-VPCAdmissionWebhook.ps1;
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-admission-webhook/latest/webhook-create-signed-cert.ps1;
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-admission-webhook/latest/webhook-patch-ca-bundle.ps1;
```

- b. Install [OpenSSL](#) and [jq](#).
- c. Set up and deploy the VPC admission webhook.

```
./Setup-VPCAdmissionWebhook.ps1 -DeploymentTemplate ".\vpc-admission-webhook-deployment.yaml"
```

Important

The VPC admission controller webhook is signed with a certificate that expires one year after the date of issue. To avoid down time, make sure to renew the certificate before it expires. For more information, see [Renewing the VPC admission webhook certificate \(p. 56\)](#).

3. Determine if your cluster has the required cluster role binding.

```
kubectl get clusterrolebinding eks:kube-proxy-windows
```

If output similar to the following example output is returned, then the cluster has the necessary role binding.

NAME	AGE
eks:kube-proxy-windows	10d

If the output includes `Error from server (NotFound)`, then the cluster does not have the necessary cluster role binding. Add the binding by creating a file named [*eks-kube-proxy-windows-crb.yaml*](#) with the following content.

```
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: eks:kube-proxy-windows
  labels:
    k8s-app: kube-proxy
    eks.amazonaws.com/component: kube-proxy
subjects:
  - kind: Group
    name: "eks:kube-proxy-windows"
roleRef:
  kind: ClusterRole
  name: system:node-proxier
  apiGroup: rbac.authorization.k8s.io
```

Apply the configuration to the cluster.

```
kubectl apply -f eks-kube-proxy-windows-crb.yaml
```

4. After you have enabled Windows support, you can launch a Windows node group into your cluster. For more information, see [Launching self-managed Windows nodes \(p. 117\)](#).

macOS and Linux

To enable legacy Windows support for your cluster with a macOS or Linux client

This procedure requires that the `openssl` library and `jq` JSON processor are installed on your client system.

In the following steps, replace `region-code` with the AWS Region that your cluster resides in.

1. Deploy the VPC resource controller to your cluster.

```
kubectl apply -f https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-resource-controller/latest/vpc-resource-controller.yaml
```

2. Create the VPC admission controller webhook manifest for your cluster.

- a. Download the required scripts and deployment files.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-admission-webhook/latest/webhook-create-signed-cert.sh  
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-admission-webhook/latest/webhook-patch-ca-bundle.sh  
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-admission-webhook/latest/vpc-admission-webhook-deployment.yaml
```

- b. Add permissions to the shell scripts so that they can be run.

```
chmod +x webhook-create-signed-cert.sh webhook-patch-ca-bundle.sh
```

- c. Create a secret for secure communication.

```
./webhook-create-signed-cert.sh
```

- d. Verify the secret.

```
kubectl get secret -n kube-system vpc-admission-webhook-certs
```

- e. Configure the webhook and create a deployment file.

```
cat ./vpc-admission-webhook-deployment.yaml | ./webhook-patch-ca-bundle.sh > vpc-admission-webhook.yaml
```

3. Deploy the VPC admission webhook.

```
kubectl apply -f vpc-admission-webhook.yaml
```

Important

The VPC admission controller webhook is signed with a certificate that expires one year after the date of issue. To avoid down time, make sure to renew the certificate before it expires. For more information, see [Renewing the VPC admission webhook certificate \(p. 56\)](#).

4. Determine if your cluster has the required cluster role binding.

```
kubectl get clusterrolebinding eks:kube-proxy-windows
```

If output similar to the following example output is returned, then the cluster has the necessary role binding.

NAME	ROLE	AGE
eks:kube-proxy-windows	ClusterRole/system:node-proxier	19h

If the output includes `Error from server (NotFound)`, then the cluster does not have the necessary cluster role binding. Add the binding by creating a file named `eks-kube-proxy-windows-crb.yaml` with the following content.

```
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: eks:kube-proxy-windows
  labels:
    k8s-app: kube-proxy
    eks.amazonaws.com/component: kube-proxy
subjects:
  - kind: Group
    name: "eks:kube-proxy-windows"
roleRef:
  kind: ClusterRole
  name: system:node-proxier
  apiGroup: rbac.authorization.k8s.io
```

Apply the configuration to the cluster.

```
kubectl apply -f eks-kube-proxy-windows-crb.yaml
```

- After you have enabled Windows support, you can launch a Windows node group into your cluster. For more information, see [Launching self-managed Windows nodes \(p. 117\)](#).

Renewing the VPC admission webhook certificate

The certificate used by the VPC admission webhook expires one year after issue. To avoid down time, it's important that you renew the certificate before it expires. You can check the expiration date of your current certificate with the following command.

```
kubectl get secret \
-n kube-system \
vpc-admission-webhook-certs -o json | \
jq -r '.data."cert.pem"' | \
base64 -decode | \
openssl x509 \
-noout \
-enddate | \
cut -d= -f2
```

An example output is as follows.

```
May 28 14:23:00 2022 GMT
```

You can renew the certificate using `eksctl` or a Windows or Linux/macOS computer. Follow the instructions for the tool you originally used to install the VPC admission webhook. For example, if you originally installed the VPC admission webhook using `eksctl`, then you should renew the certificate using the instructions on the `eksctl` tab.

eksctl

1. Reinstall the certificate. Replace *my-cluster* with the name of your cluster.

```
eksctl utils install-vpc-controllers -cluster my-cluster -approve
```

2. Verify that you receive the following output.

```
2021/05/28 05:24:59 [INFO] generate received request
2021/05/28 05:24:59 [INFO] received CSR
2021/05/28 05:24:59 [INFO] generating key: rsa-2048
2021/05/28 05:24:59 [INFO] encoded CSR
```

3. Restart the webhook deployment.

```
kubectl rollout restart deployment -n kube-system vpc-admission-webhook
```

4. If the certificate that you renewed was expired, and you have Windows Pods stuck in the Container creating state, then you must delete and redeploy those Pods.

Windows

1. Get the script to generate new certificate.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-admission-webhook/latest/webhook-create-signed-cert.ps1;
```

2. Prepare parameter for the script.

```
./webhook-create-signed-cert.ps1 -ServiceName vpc-admission-webhook-svc -SecretName vpc-admission-webhook-certs -Namespace kube-system
```

3. Restart the webhook deployment.

```
kubectl rollout restart deployment -n kube-system vpc-admission-webhook-deployment
```

4. If the certificate that you renewed was expired, and you have Windows Pods stuck in the Container creating state, then you must delete and redeploy those Pods.

Linux and macOS

Prerequisite

You must have OpenSSL and jq installed on your computer.

1. Get the script to generate new certificate.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/manifests/region-code/vpc-admission-webhook/latest/webhook-create-signed-cert.sh
```

2. Change the permissions.

```
chmod +x webhook-create-signed-cert.sh
```

3. Run the script.

```
./webhook-create-signed-cert.sh
```

4. Restart the webhook.

```
kubectl rollout restart deployment -n kube-system vpc-admission-webhook-deployment
```

5. If the certificate that you renewed was expired, and you have Windows Pods stuck in the Container creating state, then you must delete and redeploy those Pods.

Supporting higher Pod density on Windows nodes

In Amazon EKS, each Pod is allocated an IPv4 address from your VPC. Due to this, the number of Pods that you can deploy to a node is constrained by the available IP addresses, even if there are sufficient resources to run more Pods on the node. Since only one elastic network interface is supported by a Windows node, by default, the maximum number of available IP addresses on a Windows node is equal to:

```
Number of private IPv4 addresses for each interface on the node - 1
```

One IP address is used as the primary IP address of the network interface, so it can't be allocated to Pods.

You can enable higher Pod density on Windows nodes by enabling IP prefix delegation. This feature enables you to assign a /28 IPv4 prefix to the primary network interface, instead of assigning secondary IPv4 addresses. Assigning an IP prefix increases the maximum available IPv4 addresses on the node to:

```
(Number of private IPv4 addresses assigned to the interface attached to the node - 1) * 16
```

With this significantly larger number of available IP addresses, available IP addresses shouldn't limit your ability to scale the number of Pods on your nodes. For more information, see [the section called "Increase available IP addresses" \(p. 318\)](#).

Private cluster requirements

This topic describes how to deploy an Amazon EKS cluster that is deployed on the AWS Cloud, but doesn't have outbound internet access. If you have a local cluster on AWS Outposts, see [the section called "Launching nodes" \(p. 614\)](#), instead of this topic.

If you're not familiar with Amazon EKS networking, see [De-mystifying cluster networking for Amazon EKS worker nodes](#). If your cluster doesn't have outbound internet access, then it must meet the following requirements:

- Your cluster must pull images from a container registry that's in your VPC. You can create an Amazon Elastic Container Registry in your VPC and copy container images to it for your nodes to pull from. For more information, see [the section called "Copy an image to a repository" \(p. 381\)](#).
- Your cluster must have endpoint private access enabled. This is required for nodes to register with the cluster endpoint. Endpoint public access is optional. For more information, see [Amazon EKS cluster endpoint access control \(p. 41\)](#).
- Self-managed Linux and Windows nodes must include the following bootstrap arguments before they're launched. These arguments bypass Amazon EKS introspection and don't require access to the Amazon EKS API from within the VPC.
 1. Determine the value of your cluster's endpoint with the following command. Replace `my-cluster` with the name of your cluster.

```
aws eks describe-cluster --name my-cluster --query cluster.endpoint --output text
```

An example output is as follows.

```
https://EXAMPLE108C897D9B2F1B21D5EXAMPLE.sk1.region-code.eks.amazonaws.com
```

2. Determine the value of your cluster's certificate authority with the following command. Replace *my-cluster* with the name of your cluster.

```
aws eks describe-cluster --name my-cluster --query cluster.certificateAuthority --output text
```

The returned output is a long string.

3. Replace *cluster-endpoint* and *certificate-authority* in the following commands with the values returned in the output from the previous commands. For more information about specifying bootstrap arguments when launching self-managed nodes, see [the section called "Amazon Linux" \(p. 108\)](#) and [the section called "Windows" \(p. 117\)](#).
- For Linux nodes:

```
--apiserver-endpoint cluster-endpoint --b64-cluster-ca certificate-authority
```

For additional arguments, see the [bootstrap script](#) on GitHub.

- For Windows nodes:

Note

If you're using custom service CIDR, then you need to specify it using the `-ServiceCIDR` parameter. Otherwise, the DNS resolution for Pods in the cluster will fail.

```
-APIServerEndpoint cluster-endpoint -Base64ClusterCA certificate-authority
```

For additional arguments, see [Bootstrap script configuration parameters \(p. 186\)](#).

- Your cluster's aws-auth ConfigMap must be created from within your VPC. For more information about creating the aws-auth ConfigMap, see [Enabling IAM principal access to your cluster \(p. 420\)](#).
- Pods configured with [IAM roles for service accounts \(p. 464\)](#) acquire credentials from an AWS Security Token Service (AWS STS) API call. If there is no outbound internet access, you must create and use an AWS STS VPC endpoint in your VPC. Most AWS v1 SDKs use the global AWS STS endpoint by default (`sts.amazonaws.com`), which doesn't use the AWS STS VPC endpoint. To use the AWS STS VPC endpoint, you might need to configure your SDK to use the regional AWS STS endpoint (`sts.region-code.amazonaws.com`). For more information, see [the section called "Configuring AWS STS endpoint" \(p. 474\)](#).
- Your cluster's VPC subnets must have a VPC interface endpoint for any AWS services that your Pods need access to. For more information, see [Access an AWS service using an interface VPC endpoint](#). Some commonly-used services and endpoints are listed in the following table. For a complete list of endpoints, see [AWS services that integrate with AWS PrivateLink](#) in the [AWS PrivateLink Guide](#).

Service	Endpoint
Amazon EC2	com.amazonaws. <i>region-code</i> .ec2

Service	Endpoint
Amazon Elastic Container Registry (for pulling container images)	com.amazonaws. <i>region-code</i> .ecr.api, com.amazonaws. <i>region-code</i> .ecr.dkr, and com.amazonaws. <i>region-code</i> .s3
Application Load Balancers and Network Load Balancers	com.amazonaws. <i>region-code</i> .elasticloadbalancing
AWS X-Ray	com.amazonaws. <i>region-code</i> .xray
Amazon CloudWatch Logs	com.amazonaws. <i>region-code</i> .logs
AWS Security Token Service (required when using IAM roles for service accounts)	com.amazonaws. <i>region-code</i> .sts

Considerations

- Any self-managed nodes must be deployed to subnets that have the VPC interface endpoints that you require. If you create a managed node group, the VPC interface endpoint security group must allow the CIDR for the subnets, or you must add the created node security group to the VPC interface endpoint security group.
- If your Pods use Amazon EFS volumes, then before deploying the [Amazon EFS CSI driver \(p. 244\)](#), the driver's [kustomization.yaml](#) file must be changed to set the container images to use the same AWS Region as the Amazon EKS cluster.
- You can use the [AWS Load Balancer Controller \(p. 333\)](#) to deploy AWS Application Load Balancers (ALB) and Network Load Balancers to your private cluster. When deploying it, you should use [command line flags](#) to set enable-shield, enable-waf, and enable-wafv2 to false. [Certificate discovery](#) with hostnames from Ingress objects isn't supported. This is because the controller needs to reach AWS Certificate Manager, which doesn't have a VPC interface endpoint.

The controller supports network load balancers with IP targets, which are required for use with Fargate. For more information, see [Application load balancing on Amazon EKS \(p. 375\)](#) and [Create a network load balancer \(p. 371\)](#).

- The [Amazon FSx for Lustre CSI driver \(p. 249\)](#) isn't supported.
- [Cluster Autoscaler \(p. 75\)](#) is supported. When deploying Cluster Autoscaler Pods, make sure that the command line includes --aws-use-static-instance-list=true. For more information, see [Use Static Instance List](#) on GitHub. The worker node VPC must also include the AWS STS VPC endpoint and autoscaling VPC endpoint.
- Some container software products use API calls that access the AWS Marketplace Metering Service to monitor usage. Private clusters do not allow these calls, so you can't use these container types in private clusters.

Amazon EKS Kubernetes versions

Amazon EKS Extended Support for Kubernetes Versions is in preview release and is subject to change. There is no additional cost for extended versions during the preview period.

Kubernetes rapidly evolves with new features, design updates, and bug fixes. The community releases new Kubernetes minor versions (such as 1.28) on average once every four months. Amazon EKS follows

the upstream release and deprecation cycle for minor versions. As new Kubernetes versions become available in Amazon EKS, we recommend that you proactively update your clusters to use the latest available version.

A minor version is under standard support in Amazon EKS for the first 14 months after it's released. Once a version is past the end of standard support date, it automatically enters extended support for the next 12 months. Extended support allows you to stay at a specific Kubernetes version for longer at an additional cost per cluster hour. **Extended support for Kubernetes versions is currently in preview, and there is no additional charge during the preview period.** If you haven't updated your cluster before the extended support period ends, your cluster is auto-upgraded to the oldest currently supported extended version.

We recommend that you create your cluster with the latest available Kubernetes version supported by Amazon EKS. If your application requires a specific version of Kubernetes, you can select older versions. You can create new Amazon EKS clusters on any version offered in standard or extended support.

Available versions on standard support

The following Kubernetes versions are currently available in Amazon EKS standard support:

- 1.28
- 1.27
- 1.26
- 1.25
- 1.24
- 1.23

For important changes to be aware of for each version in standard support, see [Release notes for standard support versions \(p. 64\)](#).

Available versions on extended support

There are currently no versions on extended support. Kubernetes 1.23 will be the first version to enter extended support on October 11, 2023.

Amazon EKS Kubernetes release calendar

The following table shows important release and support dates to consider for each Kubernetes version.

Note

Dates with only a month and a year are approximate and are updated with an exact date when it's known.

Kubernetes version	Upstream release	Amazon EKS release	End of standard support	End of extended support
1.28	August 15, 2023	September 26, 2023	November 2024	November 2025
1.27	April 11, 2023	May 24, 2023	July 2024	July 2025
1.26	December 9, 2022	April 11, 2023	June 2024	June 2025

Kubernetes version	Upstream release	Amazon EKS release	End of standard support	End of extended support
1.25	August 23, 2022	February 22, 2023	May 2024	May 2025
1.24	May 3, 2022	November 15, 2022	January 31, 2024	January 2025
1.23	December 7, 2021	August 11, 2022	October 11, 2023	October 11, 2024

Amazon EKS version FAQs

How many Kubernetes versions are available in standard support?

In line with the Kubernetes community support for Kubernetes versions, Amazon EKS is committed to offering standard support for at least four production-ready versions of Kubernetes at any given time. We will announce the end of standard support date of a given Kubernetes minor version at least 60 days in advance. Because of the Amazon EKS qualification and release process for new Kubernetes versions, the end of standard support date of a Kubernetes version on Amazon EKS will be on or after the date that the Kubernetes project stops supporting the version upstream.

How long does a Kubernetes receive standard support by Amazon EKS?

A Kubernetes version received standard support for 14 months after first being available on Amazon EKS. This is true even if upstream Kubernetes no longer support a version that's available on Amazon EKS. We backport security patches that are applicable to the Kubernetes versions that are supported on Amazon EKS.

Am I notified when standard support is ending for a Kubernetes version on Amazon EKS?

Yes. If any clusters in your account are running the version nearing the end of support, Amazon EKS sends out a notice through the AWS Health Dashboard approximately 12 months after the Kubernetes version was released on Amazon EKS. The notice includes the end of support date. This is at least 60 days from the date of the notice.

Which Kubernetes features are supported by Amazon EKS?

Amazon EKS supports all generally available (GA) features of the Kubernetes API. It also supports all beta features, which are enabled by default. Alpha features aren't supported.

Are Amazon EKS managed node groups automatically updated along with the cluster control plane version?

No. A managed node group creates Amazon EC2 instances in your account. These instances aren't automatically upgraded when you or Amazon EKS update your control plane. For more information, see [the section called "Updating a managed node group" \(p. 91\)](#). We recommend maintaining the same Kubernetes version on your control plane and nodes.

Are self-managed node groups automatically updated along with the cluster control plane version?

No. A self-managed node group includes Amazon EC2 instances in your account. These instances aren't automatically upgraded when you or Amazon EKS update the control plane version on your behalf. A self-managed node group doesn't have any indication in the console that it needs updating. You can view the kubelet version installed on a node by selecting the node in the **Nodes** list on the **Overview** tab of your cluster to determine which nodes need updating. You must manually update the nodes. For more information, see [the section called "Updates" \(p. 122\)](#).

The Kubernetes project tests compatibility between the control plane and nodes for up to three minor versions. For example, 1.25 nodes continue to operate when orchestrated by a 1.28 control plane. However, running a cluster with nodes that are persistently three minor versions behind the

control plane isn't recommended. For more information, see [Kubernetes version and version skew support policy](#) in the Kubernetes documentation. We recommend maintaining the same Kubernetes version on your control plane and nodes.

Are Pods running on Fargate automatically upgraded with an automatic cluster control plane version upgrade?

No. We strongly recommend running Fargate Pods as part of a replication controller, such as a Kubernetes deployment. Then do a rolling restart of all Fargate Pods. The new version of the Fargate Pod is deployed with a kubelet version that's the same version as your updated cluster control plane version. For more information, see [Deployments](#) in the Kubernetes documentation.

Important

If you update the control plane, you must still update the Fargate nodes yourself. To update Fargate nodes, delete the Fargate Pod represented by the node and redeploy the Pod. The new Pod is deployed with a kubelet version that's the same version as your cluster.

Amazon extended support FAQs

The standard support and extended support terminology is new to me. What do those terms mean?

Standard support for a Kubernetes version in Amazon EKS begins when a Kubernetes version is released on Amazon EKS, and will end 14 months after the release date. Extended support for a Kubernetes version will begin immediately after the end of standard support, and will end after the next 12 months. For example, standard support for version 1.23 in Amazon EKS ends on October 11, 2023. Extended support for version 1.23 will begin on October 12, 2023 and end on October 11, 2024.

What do I need to do to get extended support for Amazon EKS clusters?

You don't have to take any action to get extended support for your Amazon EKS clusters. Standard support will begin when a Kubernetes version is released on Amazon EKS, and will end 14 months after the release date. Extended support for a Kubernetes version will begin immediately after the end of standard support, and will end after the next 12 months. Clusters that are running on a Kubernetes version past the end of standard support will automatically be onboarded to extended support.

For which Kubernetes versions can I get extended support?

Extended support is available for Kubernetes versions 1.23 and higher. You can run clusters on any version for up to 12 months after the end of standard support for that version. This means that each version will be supported for 26 months in Amazon EKS (14 months of standard support plus 12 months of extended support).

What if I don't want to use extended support?

If you don't want to be automatically enrolled in extended support, you can upgrade your cluster to a Kubernetes version that's in standard Amazon EKS support. Clusters that aren't upgraded to a Kubernetes version in standard support will automatically enter extended support.

What will happen at the end of 12 months of extended support?

Clusters running on a Kubernetes version that has completed its 26-month lifecycle (14 months of standard support plus 12 months of extended support) will be auto-upgraded to the next version.

On the end of extended support date, you can no longer create new Amazon EKS clusters with the unsupported version. Existing control planes are automatically updated by Amazon EKS to the earliest supported version through a gradual deployment process after the end of support date. After the automatic control plane update, make sure to manually update cluster add-ons and Amazon EC2 nodes. For more information, see [the section called "Update the Kubernetes version for your Amazon EKS cluster" \(p. 34\)](#).

When exactly is my control plane automatically updated after the end of extended support date?

Amazon EKS can't provide specific time frames. Automatic updates can happen at any time after the end of extended support date. You won't receive any notification before the update. We recommend that you proactively update your control plane without relying on the Amazon EKS automatic update process. For more information, see [the section called "Updating Kubernetes version" \(p. 34\)](#).

Can I leave my control plane on a Kubernetes version indefinitely?

No. Cloud security at AWS is the highest priority. Past a certain point (usually one year), the Kubernetes community stops releasing common vulnerabilities and exposures (CVE) patches and discourages CVE submission for unsupported versions. This means that vulnerabilities specific to an older version of Kubernetes might not even be reported. This leaves clusters exposed with no notice and no remediation options in the event of a vulnerability. Given this, Amazon EKS doesn't allow control planes to stay on a version that reached end of extended support.

Is there additional cost to get extended support?

Yes, there will be additional cost for Amazon EKS clusters running in extended support. Pricing details will be announced before general availability of extended support in early 2024.

What is included in extended support?

Amazon EKS clusters in Extended Support receive ongoing security patches for the Kubernetes control plane. Additionally, Amazon EKS will release patches for the Amazon VPC CNI, kube-proxy, and CoreDNS add-ons for Extended Support versions. Amazon EKS will also release patches for AWS-published Amazon EKS optimized AMIs for Amazon Linux and Bottlerocket, as well as Amazon EKS Fargate nodes for those versions. All clusters in Extended Support will continue to get access to technical support from AWS.

Are there any limitations to patches for non-Kubernetes components in extended support?

While Extended Support covers all of the Kubernetes specific components from AWS, it will only provide support for AWS-published Amazon EKS optimized AMIs for Amazon Linux and Bottlerocket at all times. This means, you will potentially have newer components (such as OS or kernel) on your Amazon EKS optimized AMI while using Extended Support. For example, once Amazon Linux 2 reaches the [end of its lifecycle in 2025](#), the Amazon EKS optimized Amazon Linux AMIs will be built using a newer Amazon Linux OS. Amazon EKS will announce and document important support lifecycle discrepancies such as this for each Kubernetes version.

Release notes for standard support versions

This topic gives important changes to be aware of for each Kubernetes version in standard support. When upgrading, carefully review the changes that have occurred between the old and new versions for your cluster.

Note

For 1.24 and later clusters, officially published Amazon EKS AMIs include containerd as the only runtime. Kubernetes versions earlier than 1.24 use Docker as the default runtime. These versions have a bootstrap flag option that you can use to test out your workloads on any supported cluster with containerd. For more information, see [Amazon EKS ended support for Docker shim \(p. 155\)](#).

Kubernetes 1.28

Kubernetes 1.28 is now available in Amazon EKS. For more information about Kubernetes 1.28, see the [official release announcement](#).

Important

Starting with Kubernetes 1.28, you will no longer be able to use Amazon EC2 P2 instances with the Amazon EKS optimized accelerated Amazon Linux AMIs out of the box. These AMIs

for Kubernetes versions 1.28 or later will support NVIDIA 525 series or later drivers, which are incompatible with the P2 instances. However, NVIDIA 525 series or later drivers are compatible with the P3, P4, and P5 instances, so you can use those instances with the AMIs for Kubernetes version 1.28 or later. Before your Amazon EKS clusters are upgraded to version 1.28, migrate any P2 instances to P3, P4, and P5 instances. You should also proactively upgrade your applications to work with the NVIDIA 525 series or later.

- Kubernetes v1.28 expanded the supported skew between core node and control plane components by one minor version, from n-2 to n-3, so that node components (kubelet and kube-proxy) for the oldest supported minor version can work with control plane components (kube-apiserver, kube-scheduler, kube-controller-manager, cloud-controller-manager) for the newest supported minor version.
- Metrics `force_delete_pods_total` and `force_delete_pod_errors_total` in the Pod GC Controller are enhanced to account for all forceful pods deletion. A reason is added to the metric to indicate whether the pod is forcefully deleted because it's terminated, orphaned, terminating with the out-of-service taint, or terminating and unscheduled.
- The PersistentVolume (PV) controller has been modified to automatically assign a default StorageClass to any unbound PersistentVolumeClaim with the `storageClassName` not set. Additionally, the PersistentVolumeClaim admission validation mechanism within the API server has been adjusted to allow changing values from an unset state to an actual StorageClass name.

For the complete Kubernetes 1.28 changelog, see <https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.28.md>.

Kubernetes 1.27

Kubernetes 1.27 is now available in Amazon EKS. For more information about Kubernetes 1.27, see the [official release announcement](#).

Important

- The support for the alpha seccomp annotations `seccomp.security.alpha.kubernetes.io/pod` and `container.seccomp.security.alpha.kubernetes.io` annotations was removed. The alpha seccomp annotations was deprecated in 1.19, and with their removal in 1.27, seccomp fields will no longer auto-populate for Pods with seccomp annotations. Instead, use the `securityContext.seccompProfile` field for Pods or containers to configure seccomp profiles. To check whether you are using the deprecated alpha seccomp annotations in your cluster, run the following command:

```
kubectl get pods --all-namespaces -o json | grep
-E 'seccomp.security.alpha.kubernetes.io/pod|
container.seccomp.security.alpha.kubernetes.io'
```

- The `--container-runtime` command line argument for the kubelet was removed. The default container runtime for Amazon EKS has been containerd since 1.24, which eliminates the need to specify the container runtime. From 1.27 onwards, Amazon EKS will ignore the `--container-runtime` argument passed to any bootstrap scripts. It is important that you don't pass this argument to `--kubelet-extra-args` in order to prevent errors during the node bootstrap process. You must remove the `--container-runtime` argument from all of your node creation workflows and build scripts.
- The kubelet in Kubernetes 1.27 increased the default kubeAPIQPS to 50 and kubeAPIBurst to 100. These enhancements allow the kubelet to handle a higher volume of API queries, improving response times and performance. When the demands for Pods increase, due to scaling requirements,

the revised defaults ensure that the kubelet can efficiently manage the increased workload. As a result, Pod launches are quicker and cluster operations are more effective.

- You can use more fine grained Pod topology to spread policies such as `minDomain`. This parameter gives you the ability to specify the minimum number of domains your Pods should be spread across. `nodeAffinityPolicy` and `nodeTaintPolicy` allow for an extra level of granularity in governing Pod distribution. This is in accordance to node affinities, taints, and the `matchLabelKeys` field in the `topologySpreadConstraints` of your Pod's specification. This permits the selection of Pods for spreading calculations following a rolling upgrade.
- Kubernetes 1.27 promoted to beta a new policy mechanism for StatefulSets that controls the lifetime of their PersistentVolumeClaims(PVCs). The new PVC retention policy lets you specify if the PVCs generated from the StatefulSet spec template will be automatically deleted or retained when the StatefulSet is deleted or replicas in the StatefulSet are scaled down.
- The [goaway-chance](#) option in the Kubernetes API server helps prevent HTTP/2 client connections from being stuck on a single API server instance, by randomly closing a connection. When the connection is closed, the client will try to reconnect, and will likely land on a different API server as a result of load balancing. Amazon EKS version 1.27 has enabled goaway-chance flag. If your workload running on Amazon EKS cluster uses a client that is not compatible with [HTTP GOAWAY](#), we recommend that you update your client to handle GOAWAY by reconnecting on connection termination.

For the complete Kubernetes 1.27 changelog, see <https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.27.md>.

Kubernetes 1.26

Kubernetes 1.26 is now available in Amazon EKS. For more information about Kubernetes 1.26, see the [official release announcement](#).

Important

Kubernetes 1.26 no longer supports CRI v1alpha2. This results in the kubelet no longer registering the node if the container runtime doesn't support CRI v1. This also means that Kubernetes 1.26 doesn't support containerd minor version 1.5 and earlier. If you're using containerd, you need to upgrade to containerd version 1.6.0 or later before you upgrade any nodes to Kubernetes 1.26. You also need to upgrade any other container runtimes that only support the v1alpha2. For more information, defer to the container runtime vendor. By default, Amazon Linux and Bottlerocket AMIs include containerd version 1.6.6.

- Before you upgrade to Kubernetes 1.26, upgrade your Amazon VPC CNI plugin for Kubernetes to version 1.12 or later. If you don't upgrade to Amazon VPC CNI plugin for Kubernetes version 1.12 or later, the Amazon VPC CNI plugin for Kubernetes will crash. For more information, see [Working with the Amazon VPC CNI plugin for Kubernetes Amazon EKS add-on](#).
- The [goaway-chance](#) option in the Kubernetes API server helps prevent HTTP/2 client connections from being stuck on a single API server instance, by randomly closing a connection. When the connection is closed, the client will try to reconnect, and will likely land on a different API server as a result of load balancing. Amazon EKS version 1.26 has enabled goaway-chance flag. If your workload running on Amazon EKS cluster uses a client that is not compatible with [HTTP GOAWAY](#), we recommend that you update your client to handle GOAWAY by reconnecting on connection termination.

For the complete Kubernetes 1.26 changelog, see <https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.26.md>.

Kubernetes 1.25

Kubernetes 1.25 is now available in Amazon EKS. For more information about Kubernetes 1.25, see the [official release announcement](#).

Important

- PodSecurityPolicy (PSP) is removed in Kubernetes 1.25. PSPs are replaced with [Pod Security Admission \(PSA\)](#) and Pod Security Standards (PSS). PSA is a built-in admission controller that implements the security controls outlined in the [PSS](#). PSA and PSS are graduated to stable in Kubernetes 1.25 and are enabled in Amazon EKS by default. If you have PSPs in your cluster, make sure to migrate from PSP to the built-in Kubernetes PSS or to a policy-as-code solution before upgrading your cluster to version 1.25. If you don't migrate from PSP, you might encounter interruptions to your workloads. For more information, see the [the section called "1.25 Pod security policy removal FAQ" \(p. 525\)](#).
- Kubernetes version 1.25 contains changes that alter the behavior of an existing feature known as API Priority and Fairness (APF). APF serves to shield the API server from potential overload during periods of heightened request volumes. It does this by placing restrictions on the number of concurrent requests that can be processed at any given time. This is achieved through the application of distinct priority levels and limits to requests originating from various workloads or users. This approach ensures that critical applications or high-priority requests receive preferential treatment, while simultaneously preventing lower priority requests from overwhelming the API server. For more information, see [API Priority and Fairness](#) in the Kubernetes documentation or [API Priority and Fairness](#) in the EKS Best Practices Guide.

These updates were introduced in [PR #10352](#) and [PR #118601](#). Previously, APF treated all types of requests uniformly, with each request consuming a single unit of the concurrent request limit. The APF behavior change assigns higher units of concurrency to LIST requests due to the exceptionally heavy burden put on the API server by these requests. The API server estimates the number of objects that will be returned by a LIST request. It assigns a unit of concurrency that is proportional to the number of objects returned.

Upon upgrading to Amazon EKS version 1.25 or higher, this updated behavior might cause workloads with heavy LIST requests (that previously functioned without issue) to encounter rate limiting. This would be indicated by an HTTP 429 response code. To avoid potential workload disruption due to LIST requests being rate limited, we strongly encourage you to restructure your workloads to reduce the rate of these requests. Alternatively, you can address this issue by adjusting the APF settings to allocate more capacity for essential requests while reducing the capacity allocated to non-essential ones. For more information about these mitigation techniques, see [Preventing Dropped Requests](#) in the EKS Best Practices Guide.

- Amazon EKS 1.25 includes enhancements to cluster authentication that contain updated YAML libraries. If a YAML value in the aws-auth ConfigMap found in the kube-system namespace starts with a macro, where the first character is a curly brace, you should add quotation marks (" ") before and after the curly braces ({}). This is required to ensure that aws-iam-authenticator version v0.6.3 accurately parses the aws-auth ConfigMap in Amazon EKS 1.25.
- The beta API version (`discovery.k8s.io/v1beta1`) of EndpointSlice was deprecated in Kubernetes 1.21 and is no longer served as of Kubernetes 1.25. This API has been updated to `discovery.k8s.io/v1`. For more information, see [EndpointSlice](#) in the Kubernetes documentation. The AWS Load Balancer Controller v2.4.6 and earlier used the v1beta1 endpoint to communicate with EndpointSlices. If you're using the EndpointSlices configuration for the AWS Load Balancer Controller, you must upgrade to AWS Load Balancer Controller v2.4.7 *before* upgrading your Amazon EKS cluster to 1.25. If you upgrade to 1.25 while using the EndpointSlices configuration for the AWS Load Balancer Controller, the controller will crash and result in interruptions to your workloads. To upgrade the controller, see [the section called "AWS Load Balancer Controller" \(p. 333\)](#).
- SeccompDefault is promoted to beta in Kubernetes 1.25. By setting the `--seccomp-default` flag when you configure kubelet, the container runtime uses its `RuntimeDefaultseccomp` profile, rather than the unconfined (`seccomp disabled`) mode. The default profiles provide a strong set of

security defaults, while preserving the functionality of the workload. Although this flag is available, Amazon EKS doesn't enable this flag by default, so Amazon EKS behavior is effectively unchanged. If you want to, you can start enabling this on your nodes. For more details, see the tutorial [Restrict a Container's Syscalls with seccomp](#) in the Kubernetes documentation.

- Support for the Container Runtime Interface (CRI) for Docker (also known as Dockershim) was removed from Kubernetes 1.24 and later. The only container runtime in Amazon EKS official AMIs for Kubernetes 1.24 and later clusters is containerd. Before upgrading to Amazon EKS 1.24 or later, remove any reference to bootstrap script flags that aren't supported anymore. For more information, see [Amazon EKS ended support for Dockershim \(p. 155\)](#).
- The support for wildcard queries was deprecated in CoreDNS 1.8.7 and removed in CoreDNS 1.9. This was done as a security measure. Wildcard queries no longer work and return NXDOMAIN instead of an IP address.
- The [goaway-chance](#) option in the Kubernetes API server helps prevent HTTP/2 client connections from being stuck on a single API server instance, by randomly closing a connection. When the connection is closed, the client will try to reconnect, and will likely land on a different API server as a result of load balancing. Amazon EKS version 1.25 has enabled goaway-chance flag. If your workload running on Amazon EKS cluster uses a client that is not compatible with [HTTP GOAWAY](#), we recommend that you update your client to handle GOAWAY by reconnecting on connection termination.

For the complete Kubernetes 1.25 changelog, see <https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.25.md#changelog-since-v1240>.

Kubernetes 1.24

Kubernetes 1.24 is now available in Amazon EKS. For more information about Kubernetes 1.24, see the [official release announcement](#).

Important

- Starting with Kubernetes 1.24, new beta APIs aren't enabled in clusters by default. By default, existing beta APIs and new versions of existing beta APIs continue to be enabled. Amazon EKS follows the same behavior as upstream Kubernetes 1.24. The feature gates that control new features for both new and existing API operations are enabled by default. This is in alignment with upstream Kubernetes. For more information, see [KEP-3136: Beta APIs Are Off by Default](#) on GitHub.
- Support for Container Runtime Interface (CRI) for Docker (also known as Dockershim) is removed from Kubernetes 1.24. Amazon EKS official AMIs have containerd as the only runtime. Before moving to Amazon EKS 1.24 or higher, you must remove any reference to bootstrap script flags that aren't supported anymore. You must also make sure that IP forwarding is enabled for your worker nodes. For more information, see [Amazon EKS ended support for Dockershim \(p. 155\)](#).
- If you already have Fluentd configured for Container Insights, then you must migrate Fluentd to Fluent Bit before updating your cluster. The Fluentd parsers are configured to only parse log messages in JSON format. Unlike dockerfd, the containerd container runtime has log messages that aren't in JSON format. If you don't migrate to Fluent Bit, some of the configured Fluentd's parsers will generate a massive amount of errors inside the Fluentd container. For more information on migrating, see [Set up Fluent Bit as a DaemonSet to send logs to CloudWatch Logs](#).
- In Kubernetes 1.23 and earlier, kubelet serving certificates with unverifiable IP and DNS Subject Alternative Names (SANs) are automatically issued with unverifiable SANs. These unverifiable SANs are omitted from the provisioned certificate. In version 1.24 and later clusters, kubelet serving certificates aren't issued if any SAN can't be verified. This prevents kubectl exec and kubectl logs commands from working. For more information, see [Certificate signing considerations before upgrading your cluster to Kubernetes 1.24 \(p. 461\)](#).

- When upgrading an Amazon EKS 1.23 cluster that uses Fluent Bit, you must make sure that it's running k8s/1.3.12 or later. You can do this by reapplying the latest applicable Fluent Bit YAML file from GitHub. For more information, see [Setting up Fluent Bit](#) in the Amazon CloudWatch User Guide.
- You can use Topology Aware Hints to indicate your preference for keeping traffic in zone when cluster worker nodes are deployed across multiple availability zones. Routing traffic within a zone can help reduce costs and improve network performance. By default, Topology Aware Hints are enabled in Amazon EKS 1.24. For more information, see [Topology Aware Hints](#) in the Kubernetes documentation.
- The PodSecurityPolicy (PSP) is scheduled for removal in Kubernetes 1.25. PSPs are being replaced with [Pod Security Admission \(PSA\)](#). PSA is a built-in admission controller that uses the security controls that are outlined in the [Pod Security Standards \(PSS\)](#). PSA and PSS are both beta features and are enabled in Amazon EKS by default. To address the removal of PSP in version 1.25, we recommend that you implement PSS in Amazon EKS. For more information, see [Implementing Pod Security Standards in Amazon EKS](#) on the AWS blog.
- The `client.authentication.k8s.io/v1alpha1 ExecCredential` is removed in Kubernetes 1.24. The ExecCredential API was generally available in Kubernetes 1.22. If you use a client-go credential plugin that relies on the v1alpha1 API, contact the distributor of your plugin on how to migrate to the v1 API.
- For Kubernetes 1.24, we contributed a feature to the upstream Cluster Autoscaler project that simplifies scaling Amazon EKS managed node groups to and from zero nodes. Previously, for the Cluster Autoscaler to understand the resources, labels, and taints of a managed node group that was scaled to zero nodes, you needed to tag the underlying Amazon EC2 Auto Scaling group with the details of the nodes that it was responsible for. Now, when there are no running nodes in the managed node group, the Cluster Autoscaler calls the Amazon EKS `DescribeNodegroup` API operation. This API operation provides the information that the Cluster Autoscaler requires of the managed node group's resources, labels, and taints. This feature requires that you add the `eks:DescribeNodegroup` permission to the Cluster Autoscaler service account IAM policy. When the value of a Cluster Autoscaler tag on the Auto Scaling group powering an Amazon EKS managed node group conflicts with the node group itself, the Cluster Autoscaler prefers the value of the Auto Scaling group tag. This is so that you can override values as needed. For more information, see [Autoscaling \(p. 75\)](#).
- If you intend to use Inferentia or Trainium instance types with Amazon EKS 1.24, you must upgrade to the AWS Neuron device plugin version 1.9.3.0 or later. For more information, see [Neuron K8 release \[1.9.3.0\]](#) in the AWS Neuron Documentation.
- Containerd has IPv6 enabled for Pods, by default. It applies node kernel settings to Pod network namespaces. Because of this, containers in a Pod bind to both IPv4 (127.0.0.1) and IPv6 (:1) loopback addresses. IPv6 is the default protocol for communication. Before updating your cluster to version 1.24, we recommend that you test your multi-container Pods. Modify apps so that they can bind to all IP addresses on loopback interfaces. The majority of libraries enable IPv6 binding, which is backward compatible with IPv4. When it's not possible to modify your application code, you have two options:
 - Run an `init` container and set `disable_ipv6` to `true` (`sysctl -w net.ipv6.conf.all.disable_ipv6=1`).
 - Configure a [mutating admission webhook](#) to inject an `init` container alongside your application Pods.

If you need to block IPv6 for all Pods across all nodes, you might have to disable IPv6 on your instances.

- The [goaway-chance](#) option in the Kubernetes API server helps prevent HTTP/2 client connections from being stuck on a single API server instance, by randomly closing a connection. When the connection is closed, the client will try to reconnect, and will likely land on a different API server as a result of load balancing. Amazon EKS version 1.24 has enabled goaway-chance flag. If your workload running on Amazon EKS cluster uses a client that is not compatible with [HTTP GOAWAY](#), we recommend that you update your client to handle GOAWAY by reconnecting on connection termination.

For the complete Kubernetes 1.24 changelog, see <https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG-1.24.md#changelog-since-v1230>.

Kubernetes 1.23

Kubernetes 1.23 is now available in Amazon EKS. For more information about Kubernetes 1.23, see the [official release announcement](#).

Important

The Kubernetes in-tree to container storage interface (CSI) volume migration feature is enabled. This feature enables the replacement of existing Kubernetes in-tree storage plugins for Amazon EBS with a corresponding Amazon EBS CSI driver. For more information, see [Kubernetes 1.17 Feature: Kubernetes In-Tree to CSI Volume Migration Moves to Beta](#) on the Kubernetes blog.

The feature translates in-tree APIs to equivalent CSI APIs and delegates operations to a replacement CSI driver. With this feature, if you use existing StorageClass, PersistentVolume, and PersistentVolumeClaim objects that belong to these workloads, there likely won't be any noticeable change. The feature enables Kubernetes to delegate all storage management operations from the in-tree plugin to the CSI driver. If you use Amazon EBS volumes in an existing cluster, install the Amazon EBS CSI driver in your cluster before you update your cluster to version 1.23. If you don't install the driver before updating an existing cluster, interruptions to your workloads might occur. If you plan to deploy workloads that use Amazon EBS volumes in a new 1.23 cluster, install the Amazon EBS CSI driver in your cluster before deploying the workloads to your cluster. For instructions on how to install the Amazon EBS CSI driver on your cluster, see [Amazon EBS CSI driver \(p. 228\)](#). For frequently asked questions about the migration feature, see [Amazon EBS CSI migration frequently asked questions \(p. 241\)](#).

- Kubernetes stopped supporting dockershim in version 1.20 and removed dockershim in version 1.24. For more information, see [Kubernetes is Moving on From Dockershim: Commitments and Next Steps](#) in the Kubernetes blog. Amazon EKS will end support for dockershim starting in Amazon EKS version 1.24. Starting with Amazon EKS version 1.24, Amazon EKS official AMIs will have containerd as the only runtime.

Even though Amazon EKS version 1.23 continues to support dockershim, we recommend that you start testing your applications now to identify and remove any Docker dependencies. This way, you are prepared to update your cluster to version 1.24. For more information about dockershim removal, see [the section called "Dockershim deprecation" \(p. 155\)](#).

- Kubernetes graduated IPv4/IPv6 dual-stack networking for Pods, services, and nodes to general availability. However, Amazon EKS and the Amazon VPC CNI plugin for Kubernetes don't support dual-stack networking. Your clusters can assign IPv4 or IPv6 addresses to Pods and services, but can't assign both address types.
- Kubernetes graduated the Pod Security Admission (PSA) feature to beta. The feature is enabled by default. For more information, see [Pod Security Admission](#) in the Kubernetes documentation. PSA replaces the [Pod Security Policy](#) (PSP) admission controller. The PSP admission controller isn't supported and is scheduled for removal in Kubernetes version 1.25.

The PSP admission controller enforces Pod security standards on Pods in a namespace based on specific namespace labels that set the enforcement level. For more information, see [Pod Security Standards \(PSS\) and Pod Security Admission \(PSA\)](#) in the Amazon EKS best practices guide.

- The kube-proxy image deployed with clusters is now the [minimal base image](#) maintained by Amazon EKS Distro (EKS-D). The image contains minimal packages and doesn't have shells or package managers.
- Kubernetes graduated ephemeral containers to beta. Ephemeral containers are temporary containers that run in the same namespace as an existing Pod. You can use them to observe the state of Pods and containers for troubleshooting and debugging purposes. This is especially useful for interactive troubleshooting when kubectl exec is insufficient because either a container has crashed or

a container image doesn't include debugging utilities. An example of a container that includes a debugging utility is [distroless images](#). For more information, see [Debugging with an ephemeral debug container](#) in the Kubernetes documentation.

- Kubernetes graduated the HorizontalPodAutoscaler autoscaling/v2 stable API to general availability. The HorizontalPodAutoscaler autoscaling/v2beta2 API is deprecated. It will be unavailable in 1.26.
- The [goaway-chance](#) option in the Kubernetes API server helps prevent HTTP/2 client connections from being stuck on a single API server instance, by randomly closing a connection. When the connection is closed, the client will try to reconnect, and will likely land on a different API server as a result of load balancing. Amazon EKS version 1.23 has enabled goaway-chance flag. If your workload running on Amazon EKS cluster uses a client that is not compatible with [HTTP GOAWAY](#), we recommend that you update your client to handle GOAWAY by reconnecting on connection termination.

For the complete Kubernetes 1.23 changelog, see <https://github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.23.md#changelog-since-v1220>.

Amazon EKS platform versions

Amazon EKS platform versions represent the capabilities of the Amazon EKS cluster control plane, such as which Kubernetes API server flags are enabled, as well as the current Kubernetes patch version. Each Kubernetes minor version has one or more associated Amazon EKS platform versions. The platform versions for different Kubernetes minor versions are independent. If you have a local cluster on AWS Outposts, see [the section called "Platform versions" \(p. 597\)](#) instead of this topic.

When a new Kubernetes minor version is available in Amazon EKS, such as 1.28, the initial Amazon EKS platform version for that Kubernetes minor version starts at eks . 1. However, Amazon EKS releases new platform versions periodically to enable new Kubernetes control plane settings and to provide security fixes.

When new Amazon EKS platform versions become available for a minor version:

- The Amazon EKS platform version number is incremented (eks . *n+1*).
- Amazon EKS automatically upgrades all existing clusters to the latest Amazon EKS platform version for their corresponding Kubernetes minor version. Automatic upgrades of existing Amazon EKS platform versions are rolled out incrementally. The roll-out process might take some time. If you need the latest Amazon EKS platform version features immediately, you should create a new Amazon EKS cluster.

If your cluster is more than two platform versions behind the current platform version, then it's possible that Amazon EKS wasn't able to automatically update your cluster. For details of what may cause this, see [the section called "Old platform version" \(p. 571\)](#).

- Amazon EKS might publish a new node AMI with a corresponding patch version. However, all patch versions are compatible between the EKS control plane and node AMIs for a given Kubernetes minor version.

New Amazon EKS platform versions don't introduce breaking changes or cause service interruptions.

Clusters are always created with the latest available Amazon EKS platform version (eks . *n*) for the specified Kubernetes version. If you update your cluster to a new Kubernetes minor version, your cluster receives the current Amazon EKS platform version for the Kubernetes minor version that you updated to.

The current and recent Amazon EKS platform versions are described in the following tables.

Kubernetes version 1.28

The following admission controllers are enabled for all 1.28 platform versions: NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle, LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionPolicy, ValidatingAdmissionWebhook, ResourceQuota.

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.28.1	eks.1	Initial release of Kubernetes version 1.28 for Amazon EKS. For more information, see Kubernetes 1.28 (p. 64) .	September 26, 2023

Kubernetes version 1.27

The following admission controllers are enabled for all 1.27 platform versions: NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle, LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionPolicy, ValidatingAdmissionWebhook, ResourceQuota.

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.27.4	eks.5	New platform version with security fixes and enhancements.	August 30, 2023
1.27.4	eks.4	New platform version with security fixes and enhancements.	July 30, 2023
1.27.3	eks.3	New platform version with security fixes and enhancements.	June 30, 2023
1.27.2	eks.2	New platform version with security fixes and enhancements.	June 9, 2023
1.27.1	eks.1	Initial release of Kubernetes version 1.27 for Amazon EKS. For more information, see Kubernetes 1.27 (p. 65) .	May 24, 2023

Kubernetes version 1.26

The following admission controllers are enabled for all 1.26 platform versions: NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle,

`LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionPolicy, ValidatingAdmissionWebhook, ResourceQuota.`

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.26.7	eks.6	New platform version with security fixes and enhancements.	August 30, 2023
1.26.7	eks.5	New platform version with security fixes and enhancements.	July 30, 2023
1.26.6	eks.4	New platform version with security fixes and enhancements.	June 30, 2023
1.26.5	eks.3	New platform version with security fixes and enhancements.	June 9, 2023
1.26.4	eks.2	New platform version with security fixes and enhancements.	May 5, 2023
1.26.2	eks.1	Initial release of Kubernetes version 1.26 for Amazon EKS. For more information, see Kubernetes 1.26 (p. 66) .	April 11, 2023

Kubernetes version 1.25

The following admission controllers are enabled for all 1.25 platform versions:
`NodeRestriction, ExtendedResourceToleration, NamespaceLifecycle, LimitRanger, ServiceAccount, TaintNodesByCondition, PodSecurity, Priority, DefaultTolerationSeconds, DefaultStorageClass, StorageObjectInUseProtection, PersistentVolumeClaimResize, RuntimeClass, CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, MutatingAdmissionWebhook, ValidatingAdmissionPolicy, ValidatingAdmissionWebhook, ResourceQuota.`

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.25.12	eks.7	New platform version with security fixes and enhancements.	August 30, 2023
1.25.12	eks.6	New platform version with security fixes and enhancements.	July 30, 2023
1.25.11	eks.5	New platform version with security fixes and enhancements.	June 30, 2023
1.25.10	eks.4	New platform version with security fixes and enhancements.	June 9, 2023
1.25.9	eks.3	New platform version with security fixes and enhancements.	May 5, 2023

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.25.8	eks.2	New platform version with security fixes and enhancements.	March 24, 2023
1.25.6	eks.1	Initial release of Kubernetes version 1.25 for Amazon EKS. For more information, see Kubernetes 1.25 (p. 66) .	February 21, 2023

Kubernetes version 1.24

The following admission controllers are enabled for all 1.24 platform versions: CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, DefaultStorageClass, DefaultTolerationSeconds, ExtendedResourceToleration, LimitRanger, MutatingAdmissionWebhook, NamespaceLifecycle, NodeRestriction, PersistentVolumeClaimResize, Priority, PodSecurityPolicy, ResourceQuota, RuntimeClass, ServiceAccount, StorageObjectInUseProtection, TaintNodesByCondition, and ValidatingAdmissionWebhook.

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.24.16	eks.10	New platform version with security fixes and enhancements.	August 30, 2023
1.24.16	eks.9	New platform version with security fixes and enhancements.	July 30, 2023
1.24.15	eks.8	New platform version with security fixes and enhancements.	June 30, 2023
1.24.14	eks.7	New platform version with security fixes and enhancements.	June 9, 2023
1.24.13	eks.6	New platform version with security fixes and enhancements.	May 5, 2023
1.24.12	eks.5	New platform version with security fixes and enhancements.	March 24, 2023
1.24.8	eks.4	New platform version with security fixes and enhancements.	January 27, 2023
1.24.7	eks.3	New platform version with security fixes and enhancements.	December 5, 2022
1.24.7	eks.2	New platform version with security fixes and enhancements.	November 18, 2022
1.24.7	eks.1	Initial release of Kubernetes version 1.24 for Amazon EKS. For more information, see Kubernetes 1.24 (p. 68) .	November 15, 2022

Kubernetes version 1.23

The following admission controllers are enabled for all 1.23 platform versions: CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, DefaultStorageClass, DefaultTolerationSeconds, ExtendedResourceToleration, LimitRanger, MutatingAdmissionWebhook, NamespaceLifecycle, NodeRestriction, PersistentVolumeClaimResize, Priority, PodSecurityPolicy, ResourceQuota, RuntimeClass, ServiceAccount, StorageObjectInUseProtection, TaintNodesByCondition, and ValidatingAdmissionWebhook.

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.23.17	eks.12	New platform version with security fixes and enhancements.	August 30, 2023
1.23.17	eks.11	New platform version with security fixes and enhancements.	July 30, 2023
1.23.17	eks.10	New platform version with security fixes and enhancements.	June 30, 2023
1.23.17	eks.9	New platform version with security fixes and enhancements.	June 9, 2023
1.23.17	eks.8	New platform version with security fixes and enhancements.	May 5, 2023
1.23.17	eks.7	New platform version with security fixes and enhancements.	March 24, 2023
1.23.14	eks.6	New platform version with security fixes and enhancements.	January 27, 2023
1.23.13	eks.5	New platform version with security fixes and enhancements.	December 5, 2022
1.23.13	eks.4	New platform version with security fixes and enhancements.	November 18, 2022
1.23.12	eks.3	New platform version with security fixes and enhancements.	November 7, 2022
1.23.10	eks.2	New platform version with security fixes and enhancements.	September 21, 2022
1.23.7	eks.1	Initial release of Kubernetes version 1.23 for Amazon EKS. For more information, see Kubernetes 1.23 (p. 70) .	August 11, 2022

Autoscaling

Autoscaling is a function that automatically scales your resources out and in to meet changing demands. This is a major Kubernetes function that would otherwise require extensive human resources to perform manually.

Amazon EKS supports two autoscaling products:

Karpenter

Karpenter is a flexible, high-performance Kubernetes cluster autoscaler that helps improve application availability and cluster efficiency. Karpenter launches right-sized compute resources (for example, Amazon EC2 instances) in response to changing application load in under a minute. Through integrating Kubernetes with AWS, Karpenter can provision just-in-time compute resources that precisely meet the requirements of your workload. Karpenter automatically provisions new compute resources based on the specific requirements of cluster workloads. These include compute, storage, acceleration, and scheduling requirements. Amazon EKS supports clusters using Karpenter, although Karpenter works with any conformant Kubernetes cluster. For more information, see the [Karpenter](#) documentation.

Cluster Autoscaler

The Kubernetes Cluster Autoscaler automatically adjusts the number of nodes in your cluster when pods fail or are rescheduled onto other nodes. The Cluster Autoscaler uses Auto Scaling groups. For more information, see [Cluster Autoscaler on AWS](#).

Amazon EKS nodes

A Kubernetes node is a machine that runs containerized applications. Each node has the following components:

- [Container runtime](#) – Software that's responsible for running the containers.
- [kubelet](#) – Makes sure that containers are healthy and running within their associated Pod.
- [kube-proxy](#) – Maintains network rules that allow communication to your Pods.

For more information, see [Nodes](#) in the Kubernetes documentation.

Your Amazon EKS cluster can schedule Pods on any combination of [self-managed nodes \(p. 108\)](#), [Amazon EKS managed node groups \(p. 81\)](#), and [AWS Fargate \(p. 131\)](#). To learn more about nodes deployed in your cluster, see [View Kubernetes resources \(p. 529\)](#).

Note

Nodes must be in the same VPC as the subnets you selected when you created the cluster. However, the nodes don't have to be in the same subnets.

The following table provides several criteria to evaluate when deciding which options best meet your requirements. This table doesn't include [connected nodes \(p. 574\)](#) that were created outside of Amazon EKS, which can only be viewed.

Note

Bottlerocket has some specific differences from the general information in this table. For more information, see the Bottlerocket [documentation](#) on GitHub.

Criteria	EKS managed node groups	Self managed nodes	AWS Fargate
Can be deployed to AWS Outposts	No	Yes	No
Can be deployed to an AWS Local Zone	No	Yes – For more information, see Amazon EKS and AWS Local Zones (p. 560) .	No
Can run containers that require Windows	Yes	Yes (p. 49) – Your cluster still requires at least one (two recommended for availability) Linux node though.	No
Can run containers that require Linux	Yes	Yes	Yes
Can run workloads that require the Inferentia chip	Yes (p. 415) – Amazon Linux nodes only	Yes (p. 415) – Amazon Linux only	No
Can run workloads that require a GPU	Yes (p. 158) – Amazon Linux nodes only	Yes (p. 158) – Amazon Linux only	No

Criteria	EKS managed node groups	Self managed nodes	AWS Fargate
Can run workloads that require Arm processors	Yes (p. 160)	Yes (p. 160)	No
Can run AWS Bottlerocket	Yes	Yes (p. 114)	No
Pods share a kernel runtime environment with other Pods	Yes – All of your Pods on each of your nodes	Yes – All of your Pods on each of your nodes	No – Each Pod has a dedicated kernel
Pods share CPU, memory, storage, and network resources with other Pods.	Yes – Can result in unused resources on each node	Yes – Can result in unused resources on each node	No – Each Pod has dedicated resources and can be sized independently to maximize resource utilization.
Pods can use more hardware and memory than requested in Pod specs	Yes – If the Pod requires more resources than requested, and resources are available on the node, the Pod can use additional resources.	Yes – If the Pod requires more resources than requested, and resources are available on the node, the Pod can use additional resources.	No – The Pod can be re-deployed using a larger vCPU and memory configuration though.
Must deploy and manage Amazon EC2 instances	Yes (p. 85) – automated through Amazon EKS if you deployed an Amazon EKS optimized AMI. If you deployed a custom AMI, then you must update the instance manually.	Yes – Manual configuration or using Amazon EKS provided AWS CloudFormation templates to deploy Linux (x86) (p. 108) , Linux (Arm) (p. 160) , or Windows (p. 49) nodes.	No
Must secure, maintain, and patch the operating system of Amazon EC2 instances	Yes	Yes	No
Can provide bootstrap arguments at deployment of a node, such as extra kubelet arguments.	Yes – Using eksctl or a launch template (p. 98) with a custom AMI	Yes – For more information, see the bootstrap script usage information on GitHub.	No

Criteria	EKS managed node groups	Self managed nodes	AWS Fargate
Can assign IP addresses to Pods from a different CIDR block than the IP address assigned to the node.	Yes – Using a launch template with a custom AMI. For more information, see Customizing managed nodes with launch templates (p. 98) .	Yes – For more information, see Custom networking for pods (p. 306) .	No
Can SSH into node	Yes	Yes	No – There's no node host operating system to SSH to.
Can deploy your own custom AMI to nodes	Yes – Using a launch template (p. 98)	Yes	No
Can deploy your own custom CNI to nodes	Yes – Using a launch template (p. 98) with a custom AMI	Yes	No
Must update node AMI on your own	Yes (p. 91) – If you deployed an Amazon EKS optimized AMI, you're notified in the Amazon EKS console when updates are available. You can perform the update with one-click in the console. If you deployed a custom AMI, you're not notified in the Amazon EKS console when updates are available. You must perform the update on your own.	Yes (p. 128) – Using tools other than the Amazon EKS console. This is because self managed nodes can't be managed with the Amazon EKS console.	No

Criteria	EKS managed node groups	Self managed nodes	AWS Fargate
Must update node Kubernetes version on your own	Yes (p. 91) – If you deployed an Amazon EKS optimized AMI, you're notified in the Amazon EKS console when updates are available. You can perform the update with one-click in the console. If you deployed a custom AMI, you're not notified in the Amazon EKS console when updates are available. You must perform the update on your own.	Yes (p. 128) – Using tools other than the Amazon EKS console. This is because self managed nodes can't be managed with the Amazon EKS console.	No – You don't manage nodes.
Can use Amazon EBS storage with Pods	Yes (p. 228)	Yes (p. 228)	No
Can use Amazon EFS storage with Pods	Yes (p. 244)	Yes (p. 244)	Yes (p. 244)
Can use Amazon FSx for Lustre storage with Pods	Yes (p. 249)	Yes (p. 249)	No
Can use Network Load Balancer for services	Yes (p. 369)	Yes (p. 369)	Yes, when using the Create a network load balancer (p. 371)
Pods can run in a public subnet	Yes	Yes	No
Can assign different VPC security groups to individual Pods	Yes (p. 324) – Linux nodes only	Yes (p. 324) – Linux nodes only	Yes
Can run Kubernetes DaemonSets	Yes	Yes	No
Support HostPort and HostNetwork in the Pod manifest	Yes	Yes	No
AWS Region availability	All Amazon EKS supported regions	All Amazon EKS supported regions	Some Amazon EKS supported regions (p. 131)
Can run containers on Amazon EC2 dedicated hosts	Yes	Yes	No

Criteria	EKS managed node groups	Self managed nodes	AWS Fargate
Pricing	Cost of Amazon EC2 instance that runs multiple Pods. For more information, see Amazon EC2 pricing .	Cost of Amazon EC2 instance that runs multiple Pods. For more information, see Amazon EC2 pricing .	Cost of an individual Fargate memory and CPU configuration. Each Pod has its own cost. For more information, see AWS Fargate pricing .

Managed node groups

Amazon EKS managed node groups automate the provisioning and lifecycle management of nodes (Amazon EC2 instances) for Amazon EKS Kubernetes clusters.

With Amazon EKS managed node groups, you don't need to separately provision or register the Amazon EC2 instances that provide compute capacity to run your Kubernetes applications. You can create, automatically update, or terminate nodes for your cluster with a single operation. Node updates and terminations automatically drain nodes to ensure that your applications stay available.

Every managed node is provisioned as part of an Amazon EC2 Auto Scaling group that's managed for you by Amazon EKS. Every resource including the instances and Auto Scaling groups runs within your AWS account. Each node group runs across multiple Availability Zones that you define.

You can add a managed node group to new or existing clusters using the Amazon EKS console, `eksctl`, AWS CLI, AWS API, or infrastructure as code tools including AWS CloudFormation. Nodes launched as part of a managed node group are automatically tagged for auto-discovery by the Kubernetes cluster autoscaler. You can use the node group to apply Kubernetes labels to nodes and update them at any time.

There are no additional costs to use Amazon EKS managed node groups, you only pay for the AWS resources you provision. These include Amazon EC2 instances, Amazon EBS volumes, Amazon EKS cluster hours, and any other AWS infrastructure. There are no minimum fees and no upfront commitments.

To get started with a new Amazon EKS cluster and managed node group, see [Getting started with Amazon EKS – AWS Management Console and AWS CLI \(p. 16\)](#).

To add a managed node group to an existing cluster, see [Creating a managed node group \(p. 85\)](#).

Managed node groups concepts

- Amazon EKS managed node groups create and manage Amazon EC2 instances for you.
- Every managed node is provisioned as part of an Amazon EC2 Auto Scaling group that's managed for you by Amazon EKS. Moreover, every resource including Amazon EC2 instances and Auto Scaling groups run within your AWS account.
- The Auto Scaling group of a managed node group spans every subnet that you specify when you create the group.
- Amazon EKS tags managed node group resources so that they are configured to use the Kubernetes [Cluster Autoscaler \(p. 75\)](#).

Important

If you are running a stateful application across multiple Availability Zones that is backed by Amazon EBS volumes and using the Kubernetes [Autoscaling \(p. 75\)](#), you should configure

multiple node groups, each scoped to a single Availability Zone. In addition, you should enable the `--balance-similar-node-groups` feature.

- You can use a custom launch template for a greater level of flexibility and customization when deploying managed nodes. For example, you can specify extra kubelet arguments and use a custom AMI. For more information, see [Customizing managed nodes with launch templates \(p. 98\)](#). If you don't use a custom launch template when first creating a managed node group, there is an auto-generated launch template. Don't manually modify this auto-generated template or errors occur.
- Amazon EKS follows the shared responsibility model for CVEs and security patches on managed node groups. When managed nodes run an Amazon EKS optimized AMI, Amazon EKS is responsible for building patched versions of the AMI when bugs or issues are reported. We can publish a fix. However, you're responsible for deploying these patched AMI versions to your managed node groups. When managed nodes run a custom AMI, you're responsible for building patched versions of the AMI when bugs or issues are reported and then deploying the AMI. For more information, see [Updating a managed node group \(p. 91\)](#).
- Amazon EKS managed node groups can be launched in both public and private subnets. If you launch a managed node group in a public subnet on or after April 22, 2020, the subnet must have `MapPublicIpOnLaunch` set to true for the instances to successfully join a cluster. If the public subnet was created using `eksctl` or the [Amazon EKS vended AWS CloudFormation templates \(p. 259\)](#) on or after March 26, 2020, then this setting is already set to true. If the public subnets were created before March 26, 2020, you must change the setting manually. For more information, see [Modifying the public IPv4 addressing attribute for your subnet](#).
- When deploying a managed node group in private subnets, you must ensure that it can access Amazon ECR for pulling container images. You can do this by connecting a NAT gateway to the route table of the subnet or by adding the following [AWS PrivateLink VPC endpoints](#):
 - Amazon ECR API endpoint interface – `com.amazonaws.region-code.ecr.api`
 - Amazon ECR Docker registry API endpoint interface – `com.amazonaws.region-code.ecr.dkr`
 - Amazon S3 gateway endpoint – `com.amazonaws.region-code.ecr.s3`

For other commonly-used services and endpoints, see [Private cluster requirements \(p. 58\)](#).

- Managed node groups can't be deployed on [AWS Outposts \(p. 588\)](#) or in AWS Wavelength or AWS Local Zones.
- You can create multiple managed node groups within a single cluster. For example, you can create one node group with the standard Amazon EKS optimized Amazon Linux 2 AMI for some workloads and another with the GPU variant for workloads that require GPU support.
- If your managed node group encounters an [Amazon EC2 instance status check](#) failure, Amazon EKS returns an error code to help you to diagnose the issue. For more information, see [Managed node group error codes \(p. 564\)](#).
- Amazon EKS adds Kubernetes labels to managed node group instances. These Amazon EKS provided labels are prefixed with `eks.amazonaws.com`.
- Amazon EKS automatically drains nodes using the Kubernetes API during terminations or updates.
- Pod disruption budgets aren't respected when terminating a node with AZRebalance or reducing the desired node count. These actions try to evict Pods on the node. But if it takes more than 15 minutes, the node is terminated regardless of whether all Pods on the node are terminated. To extend the period until the node is terminated, add a lifecycle hook to the Auto Scaling group. For more information, see [Add lifecycle hooks](#) in the [Amazon EC2 Auto Scaling User Guide](#).
- In order to run the drain process correctly after receiving a Spot interruption notification or a capacity rebalance notification, `CapacityRebalance` must be set to `true`.
- Updating managed node groups respects the Pod disruption budgets that you set for your Pods. For more information, see [Managed node update behavior \(p. 94\)](#).
- There are no additional costs to use Amazon EKS managed node groups. You only pay for the AWS resources that you provision.
- If you want to encrypt Amazon EBS volumes for your nodes, you can deploy the nodes using a launch template. To deploy managed nodes with encrypted Amazon EBS volumes without using a launch

template, encrypt all new Amazon EBS volumes created in your account. For more information, see [Encryption by default](#) in the *Amazon EC2 User Guide for Linux Instances*.

Managed node group capacity types

When creating a managed node group, you can choose either the On-Demand or Spot capacity type. Amazon EKS deploys a managed node group with an Amazon EC2 Auto Scaling group that either contains only On-Demand or only Amazon EC2 Spot Instances. You can schedule Pods for fault tolerant applications to Spot managed node groups, and fault intolerant applications to On-Demand node groups within a single Kubernetes cluster. By default, a managed node group deploys On-Demand Amazon EC2 instances.

On-Demand

With On-Demand Instances, you pay for compute capacity by the second, with no long-term commitments.

How it works

By default, if you don't specify a **Capacity Type**, the managed node group is provisioned with On-Demand Instances. A managed node group configures an Amazon EC2 Auto Scaling group on your behalf with the following settings applied:

- The allocation strategy to provision On-Demand capacity is set to prioritized. Managed node groups use the order of instance types passed in the API to determine which instance type to use first when fulfilling On-Demand capacity. For example, you might specify three instance types in the following order: c5.large, c4.large, and c3.large. When your On-Demand Instances are launched, the managed node group fulfills On-Demand capacity by starting with c5.large, then c4.large, and then c3.large. For more information, see [Amazon EC2 Auto Scaling group](#) in the *Amazon EC2 Auto Scaling User Guide*.
- Amazon EKS adds the following Kubernetes label to all nodes in your managed node group that specifies the capacity type: eks.amazonaws.com/capacityType: ON_DEMAND. You can use this label to schedule stateful or fault intolerant applications on On-Demand nodes.

Spot

Amazon EC2 Spot Instances are spare Amazon EC2 capacity that offers steep discounts off of On-Demand prices. Amazon EC2 Spot Instances can be interrupted with a two-minute interruption notice when EC2 needs the capacity back. For more information, see [Spot Instances](#) in the *Amazon EC2 User Guide for Linux Instances*. You can configure a managed node group with Amazon EC2 Spot Instances to optimize costs for the compute nodes running in your Amazon EKS cluster.

How it works

To use Spot Instances inside a managed node group, create a managed node group by setting the capacity type as spot. A managed node group configures an Amazon EC2 Auto Scaling group on your behalf with the following Spot best practices applied:

- The allocation strategy to provision Spot capacity is set to capacity-optimized to ensure that your Spot nodes are provisioned in the optimal Spot capacity pools. To increase the number of Spot capacity pools available for allocating capacity from, configure a managed node group to use multiple instance types.
- Amazon EC2 Spot Capacity Rebalancing is enabled so that Amazon EKS can gracefully drain and rebalance your Spot nodes to minimize application disruption when a Spot node is at elevated risk of

interruption. For more information, see [Amazon EC2 Auto Scaling Capacity Rebalancing](#) in the *Amazon EC2 Auto Scaling User Guide*.

- When a Spot node receives a rebalance recommendation, Amazon EKS automatically attempts to launch a new replacement Spot node.
- If a Spot two-minute interruption notice arrives before the replacement Spot node is in a Ready state, Amazon EKS starts draining the Spot node that received the rebalance recommendation. Amazon EKS drains the node on a best-effort basis. As a result, there's no guarantee that Amazon EKS will wait for the replacement node to join the cluster before draining the existing node.
- When a replacement Spot node is bootstrapped and in the Ready state on Kubernetes, Amazon EKS cordons and drains the Spot node that received the rebalance recommendation. Cordonning the Spot node ensures that the service controller doesn't send any new requests to this Spot node. It also removes it from its list of healthy, active Spot nodes. Draining the Spot node ensures that running Pods are evicted gracefully.
- Amazon EKS adds the following Kubernetes label to all nodes in your managed node group that specifies the capacity type: `eks.amazonaws.com/capacityType: SPOT`. You can use this label to schedule fault tolerant applications on Spot nodes.

Considerations for selecting a capacity type

When deciding whether to deploy a node group with On-Demand or Spot capacity, you should consider the following conditions:

- Spot Instances are a good fit for stateless, fault-tolerant, flexible applications. These include batch and machine learning training workloads, big data ETLs such as Apache Spark, queue processing applications, and stateless API endpoints. Because Spot is spare Amazon EC2 capacity, which can change over time, we recommend that you use Spot capacity for interruption-tolerant workloads. More specifically, Spot capacity is suitable for workloads that can tolerate periods where the required capacity isn't available.
- We recommend that you use On-Demand for applications that are fault intolerant. This includes cluster management tools such as monitoring and operational tools, deployments that require StatefulSets, and stateful applications, such as databases.
- To maximize the availability of your applications while using Spot Instances, we recommend that you configure a Spot managed node group to use multiple instance types. We recommend applying the following rules when using multiple instance types:
 - Within a managed node group, if you're using the [Cluster Autoscaler \(p. 75\)](#), we recommend using a flexible set of instance types with the same amount of vCPU and memory resources. This is to ensure that the nodes in your cluster scale as expected. For example, if you need four vCPUs and eight GiB memory, use `c3.xlarge`, `c4.xlarge`, `c5.xlarge`, `c5d.xlarge`, `c5a.xlarge`, `c5n.xlarge`, or other similar instance types.
 - To enhance application availability, we recommend deploying multiple Spot managed node groups. For this, each group should use a flexible set of instance types that have the same vCPU and memory resources. For example, if you need 4 vCPUs and 8 GiB memory, we recommend that you create one managed node group with `c3.xlarge`, `c4.xlarge`, `c5.xlarge`, `c5d.xlarge`, `c5a.xlarge`, `c5n.xlarge`, or other similar instance types, and a second managed node group with `m3.xlarge`, `m4.xlarge`, `m5.xlarge`, `m5d.xlarge`, `m5a.xlarge`, `m5n.xlarge` or other similar instance types.
 - When deploying your node group with the Spot capacity type that's using a custom launch template, use the API to pass multiple instance types. Don't pass a single instance type through the launch template. For more information about deploying a node group using a launch template, see [Customizing managed nodes with launch templates \(p. 98\)](#).

Creating a managed node group

This topic describes how you can launch Amazon EKS managed node groups of nodes that register with your Amazon EKS cluster. After the nodes join the cluster, you can deploy Kubernetes applications to them.

If this is your first time launching an Amazon EKS managed node group, we recommend that you follow one of our [Getting started with Amazon EKS \(p. 6\)](#) guides instead. The guides provide walkthroughs for creating an Amazon EKS cluster with nodes.

Important

- Amazon EKS nodes are standard Amazon EC2 instances. You're billed based on the normal Amazon EC2 prices. For more information, see [Amazon EC2 Pricing](#).
- You can't create managed nodes in an AWS Region where you have AWS Outposts, AWS Wavelength, or AWS Local Zones enabled. You can create self-managed nodes in an AWS Region where you have AWS Outposts, AWS Wavelength, or AWS Local Zones enabled. For more information, see [Launching self-managed Amazon Linux nodes \(p. 108\)](#), [Launching self-managed Windows nodes \(p. 117\)](#), and [Launching self-managed Bottlerocket nodes \(p. 114\)](#). You can also create a self-managed Amazon Linux node group on an Outpost. For more information, see the section called "Launching nodes" (p. 614).
- If you don't [specify an AMI ID \(p. 102\)](#) for the bootstrap.sh file included with Amazon EKS optimized Linux or Bottlerocket, managed node groups enforce a maximum number on the value of maxPods. For instances with less than 30 vCPUs, the maximum number is 110. For instances with greater than 30 vCPUs, the maximum number jumps to 250. These numbers are based on [Kubernetes scalability thresholds](#) and recommended settings by internal Amazon EKS scalability team testing. For more information, see the [Amazon VPC CNI plugin increases pods per node limits](#) blog post.

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Creating an Amazon EKS cluster \(p. 25\)](#).
- (Optional, but recommended) The Amazon VPC CNI plugin for Kubernetes add-on configured with its own IAM role that has the necessary IAM policy attached to it. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).
- Familiarity with the considerations listed in [Choosing an Amazon EC2 instance type \(p. 152\)](#). Depending on the instance type you choose, there may be additional prerequisites for your cluster and VPC.
- To add a Windows managed node group, you must first enable Windows support for your cluster. For more information, see [Enabling Windows support for your Amazon EKS cluster \(p. 49\)](#).

You can create a managed node group with eksctl or the AWS Management Console.

eksctl

To create a managed node group with eksctl

This procedure requires eksctl version 0.160.0 or later. You can check your version with the following command:

```
eksctl version
```

For instructions on how to install or upgrade eksctl, see [Installing or updating eksctl \(p. 13\)](#).

1. (Optional) If the **AmazonEKS_CNI_Policy** managed IAM policy is attached to your [the section called "Node IAM role" \(p. 501\)](#), we recommend assigning it to an IAM role that you associate to the Kubernetes aws-node service account instead. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).
2. Create a managed node group with or without using a custom launch template. Manually specifying a launch template allows for greater customization of a node group. For example, it can allow deploying a custom AMI or providing arguments to the bootstrap.sh script in an Amazon EKS optimized AMI. For a complete list of every available option and default, enter the following command.

```
eksctl create nodegroup --help
```

In the following command, replace *my-cluster* with the name of your cluster and replace *my-mng* with the name of your node group. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters.

Important

If you don't use a custom launch template when first creating a managed node group, don't use one at a later time for the node group. If you didn't specify a custom launch template, the system auto-generates a launch template that we don't recommend that you modify manually. Manually modifying this auto-generated launch template might cause errors.

Without a launch template

eksctl creates a default Amazon EC2 launch template in your account and deploys the node group using a launch template that it creates based on options that you specify. Before specifying a value for --node-type, see [Choosing an Amazon EC2 instance type \(p. 152\)](#).

Replace *ami-family* with an allowed keyword. For more information, see [Setting the node AMI Family](#) in the eksctl documentation. Replace *my-key* with the name of your Amazon EC2 key pair or public key. This key is used to SSH into your nodes after they launch.

Note

For Windows, this command doesn't enable SSH. Instead, it associates your Amazon EC2 key pair with the instance and allows you to RDP into the instance.

If you don't already have an Amazon EC2 key pair, you can create one in the AWS Management Console. For Linux information, see [Amazon EC2 key pairs and Linux instances](#) in the *Amazon EC2 User Guide for Linux Instances*. For Windows information, see [Amazon EC2 key pairs and Windows instances](#) in the *Amazon EC2 User Guide for Windows Instances*.

We recommend blocking Pod access to IMDS if the following conditions are true:

- You plan to assign IAM roles to all of your Kubernetes service accounts so that Pods only have the minimum permissions that they need.
- No Pods in the cluster require access to the Amazon EC2 instance metadata service (IMDS) for other reasons, such as retrieving the current AWS Region.

For more information, see [Restrict access to the instance profile assigned to the worker node](#).

If you want to block Pod access to IMDS, then add the **--disable-pod-imds** option to the following command.

```
eksctl create nodegroup \  
  --cluster my-cluster \  
  ...
```

```
--region region-code \
--name my-mng \
--node-ami-family ami-family \
--node-type m5.large \
--nodes 3 \
--nodes-min 2 \
--nodes-max 4 \
--ssh-access \
--ssh-public-key my-key
```

Your instances can optionally assign a significantly higher number of IP addresses to Pods, assign IP addresses to Pods from a different CIDR block than the instance's, and be deployed to a cluster without internet access. For more information, see [Increase the amount of available IP addresses for your Amazon EC2 nodes \(p. 318\)](#), [Custom networking for pods \(p. 306\)](#), and [Private cluster requirements \(p. 58\)](#) for additional options to add to the previous command.

Managed node groups calculates and applies a single value for the maximum number of Pods that can run on each node of your node group, based on instance type. If you create a node group with different instance types, the smallest value calculated across all instance types is applied as the maximum number of Pods that can run on every instance type in the node group. Managed node groups calculates the value using the script referenced in [Amazon EKS recommended maximum Pods for each Amazon EC2 instance type \(p. 154\)](#).

With a launch template

The launch template must already exist and must meet the requirements specified in [Launch template configuration basics \(p. 98\)](#).

We recommend blocking Pod access to IMDS if the following conditions are true:

- You plan to assign IAM roles to all of your Kubernetes service accounts so that Pods only have the minimum permissions that they need.
- No Pods in the cluster require access to the Amazon EC2 instance metadata service (IMDS) for other reasons, such as retrieving the current AWS Region.

For more information, see [Restrict access to the instance profile assigned to the worker node](#).

If you want to block Pod access to IMDS, then specify the necessary settings in the launch template.

- a. Copy the following contents to your device. Replace the *example values* and then run the modified command to create the eks-nodegroup.yaml file. Several settings that you specify when deploying without a launch template are moved into the launch template. If you don't specify a version, the template's default version is used.

```
cat >eks-nodegroup.yaml <<EOF
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
  name: my-cluster
  region: region-code
managedNodeGroups:
- name: my-mng
  launchTemplate:
    id: lt-id
    version: "1"
EOF
```

For a complete list of eksctl config file settings, see [Config file schema](#) in the eksctl documentation. Your instances can optionally assign a significantly higher number of IP addresses to Pods, assign IP addresses to Pods from a different CIDR block than the instance's, use the containerd runtime, and be deployed to a cluster without outbound internet access. For more information, see [Increase the amount of available IP addresses for your Amazon EC2 nodes \(p. 318\)](#), [Custom networking for pods \(p. 306\)](#), [Enable the containerd runtime bootstrap flag \(p. 157\)](#), and [Private cluster requirements \(p. 58\)](#) for additional options to add to the config file.

If you didn't specify an AMI ID in your launch template, managed node groups calculates and applies a single value for the maximum number of Pods that can run on each node of your node group, based on instance type. If you create a node group with different instance types, the smallest value calculated across all instance types is applied as the maximum number of Pods that can run on every instance type in the node group. Managed node groups calculates the value using the script referenced in [Amazon EKS recommended maximum Pods for each Amazon EC2 instance type \(p. 154\)](#).

If you specified an AMI ID in your launch template, specify the maximum number of Pods that can run on each node of your node group if you're using [custom networking \(p. 306\)](#) or want to [increase the number of IP addresses assigned to your instance \(p. 318\)](#). For more information, see [Amazon EKS recommended maximum Pods for each Amazon EC2 instance type \(p. 154\)](#).

- b. Deploy the nodegroup with the following command.

```
eksctl create nodegroup --config-file eks-nodegroup.yaml
```

AWS Management Console

To create a managed node group using the AWS Management Console

1. Wait for your cluster status to show as ACTIVE. You can't create a managed node group for a cluster that isn't already ACTIVE.
2. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
3. Choose the name of the cluster that you want to create a managed node group in.
4. Select the **Compute** tab.
5. Choose **Add node group**.
6. On the **Configure node group** page, fill out the parameters accordingly, and then choose **Next**.
 - **Name** – Enter a unique name for your managed node group. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters.
 - **Node IAM role** – Choose the node instance role to use with your node group. For more information, see [Amazon EKS node IAM role \(p. 501\)](#).

Important

- You can't use the same role that is used to create any clusters.
- We recommend using a role that's not currently in use by any self-managed node group. Otherwise, you plan to use with a new self-managed node group. For more information, see [Deleting a managed node group \(p. 107\)](#).
- **Use launch template** – (Optional) Choose if you want to use an existing launch template. Select a **Launch Template Name**. Then, select a **Launch template version**. If you don't select a version, then Amazon EKS uses the template's default version. Launch templates allow for more customization of your node group, such as allowing you to deploy a custom AMI, assign

a significantly higher number of IP addresses to Pods, assign IP addresses to Pods from a different CIDR block than the instance's, enable the `containerd` runtime for your instances, and deploying nodes to a cluster without outbound internet access. For more information, see [Increase the amount of available IP addresses for your Amazon EC2 nodes \(p. 318\)](#), [Custom networking for pods \(p. 306\)](#), [Enable the `containerd` runtime bootstrap flag \(p. 157\)](#), and [Private cluster requirements \(p. 58\)](#).

The launch template must meet the requirements in [Customizing managed nodes with launch templates \(p. 98\)](#). If you don't use your own launch template, the Amazon EKS API creates a default Amazon EC2 launch template in your account and deploys the node group using the default launch template.

If you implement [IAM roles for service accounts \(p. 464\)](#), assign necessary permissions directly to every Pod that requires access to AWS services, and no Pods in your cluster require access to IMDS for other reasons, such as retrieving the current AWS Region, then you can also disable access to IMDS for Pods that don't use host networking in a launch template. For more information, see [Restrict access to the instance profile assigned to the worker node](#).

- **Kubernetes labels** – (Optional) You can choose to apply Kubernetes labels to the nodes in your managed node group.
 - **Kubernetes taints** – (Optional) You can choose to apply Kubernetes taints to the nodes in your managed node group. The available options in the **Effect** menu are **NoSchedule**, **NoExecute**, and **PreferNoSchedule**. For more information, see [Node taints on managed node groups \(p. 97\)](#).
 - **Tags** – (Optional) You can choose to tag your Amazon EKS managed node group. These tags don't propagate to other resources in the node group, such as Auto Scaling groups or instances. For more information, see [Tagging your Amazon EKS resources \(p. 451\)](#).
7. On the **Set compute and scaling configuration** page, fill out the parameters accordingly, and then choose **Next**.
- **AMI type** – Select an AMI type. If you are deploying Arm instances, be sure to review the considerations in [Amazon EKS optimized Arm Amazon Linux AMIs \(p. 160\)](#) before deploying.

If you specified a launch template on the previous page, and specified an AMI in the launch template, then you can't select a value. The value from the template is displayed. The AMI specified in the template must meet the requirements in [Specifying an AMI \(p. 102\)](#).

- **Capacity type** – Select a capacity type. For more information about choosing a capacity type, see [Managed node group capacity types \(p. 83\)](#). You can't mix different capacity types within the same node group. If you want to use both capacity types, create separate node groups, each with their own capacity and instance types.
- **Instance types** – By default, one or more instance type is specified. To remove a default instance type, select the X on the right side of the instance type. Choose the instance types to use in your managed node group. For more information, see [Choosing an Amazon EC2 instance type \(p. 152\)](#).

The console displays a set of commonly used instance types. If you need to create a managed node group with an instance type that's not displayed, then use `eksctl`, the AWS CLI, AWS CloudFormation, or an SDK to create the node group. If you specified a launch template on the previous page, then you can't select a value because the instance type must be specified in the launch template. The value from the launch template is displayed. If you selected **Spot for Capacity type**, then we recommend specifying multiple instance types to enhance availability.

- **Disk size** – Enter the disk size (in GiB) to use for your node's root volume.

If you specified a launch template on the previous page, then you can't select a value because it must be specified in the launch template.

- **Desired size** – Specify the current number of nodes that the managed node group should maintain at launch.

Note

Amazon EKS doesn't automatically scale your node group in or out. However, you can configure the Kubernetes [Cluster Autoscaler \(p. 75\)](#) to do this for you.

- **Minimum size** – Specify the minimum number of nodes that the managed node group can scale in to.
- **Maximum size** – Specify the maximum number of nodes that the managed node group can scale out to.
- **Node group update configuration** – (Optional) You can select the number or percentage of nodes to be updated in parallel. These nodes will be unavailable during the update. For **Maximum unavailable**, select one of the following options and specify a **Value**:
 - **Number** – Select and specify the number of nodes in your node group that can be updated in parallel.
 - **Percentage** – Select and specify the percentage of nodes in your node group that can be updated in parallel. This is useful if you have a large number of nodes in your node group.

8. On the **Specify networking** page, fill out the parameters accordingly, and then choose **Next**.

- **Subnets** – Choose the subnets to launch your managed nodes into.

Important

If you are running a stateful application across multiple Availability Zones that is backed by Amazon EBS volumes and using the Kubernetes [Autoscaling \(p. 75\)](#), you should configure multiple node groups, each scoped to a single Availability Zone. In addition, you should enable the `--balance-similar-node-groups` feature.

Important

- If you choose a public subnet, and your cluster has only the public API server endpoint enabled, then the subnet must have `MapPublicIPOnLaunch` set to `true` for the instances to successfully join a cluster. If the subnet was created using `eksctl` or the [Amazon EKS vended AWS CloudFormation templates \(p. 259\)](#) on or after March 26, 2020, then this setting is already set to `true`. If the subnets were created with `eksctl` or the AWS CloudFormation templates before March 26, 2020, then you need to change the setting manually. For more information, see [Modifying the public IPv4 addressing attribute for your subnet](#).
- If you use a launch template and specify multiple network interfaces, Amazon EC2 won't auto-assign a public IPv4 address, even if `MapPublicIpOnLaunch` is set to `true`. For nodes to join the cluster in this scenario, you must either enable the cluster's private API server endpoint, or launch nodes in a private subnet with outbound internet access provided through an alternative method, such as a NAT Gateway. For more information, see [Amazon EC2 instance IP addressing](#) in the [Amazon EC2 User Guide for Linux Instances](#).
- **Configure SSH access to nodes** (Optional). Enabling SSH allows you to connect to your instances and gather diagnostic information if there are issues. We highly recommend enabling remote access when you create a node group. You can't enable remote access after the node group is created.

If you chose to use a launch template, then this option isn't shown. To enable remote access to your nodes, specify a key pair in the launch template and ensure that the proper port is open to the nodes in the security groups that you specify in the launch template. For more information, see [Using custom security groups \(p. 100\)](#).

Note

For Windows, this command doesn't enable SSH. Instead, it associates your Amazon EC2 key pair with the instance and allows you to RDP into the instance.

- For **SSH key pair** (Optional), choose an Amazon EC2 SSH key to use. For Linux information, see [Amazon EC2 key pairs and Linux instances](#) in the *Amazon EC2 User Guide for Linux Instances*. For Windows information, see [Amazon EC2 key pairs and Windows instances](#) in the *Amazon EC2 User Guide for Windows Instances*. If you chose to use a launch template, then you can't select one. When an Amazon EC2 SSH key is provided for node groups using Bottlerocket AMIs, the administrative container is also enabled. For more information, see [Admin container](#) on GitHub.
 - For **Allow SSH remote access from**, if you want to limit access to specific instances, then select the security groups that are associated to those instances. If you don't select specific security groups, then SSH access is allowed from anywhere on the internet ($0.0.0.0/0$).
9. On the **Review and create** page, review your managed node group configuration and choose **Create**.

If nodes fail to join the cluster, then see [Nodes fail to join cluster \(p. 562\)](#) in the Troubleshooting guide.

10. Watch the status of your nodes and wait for them to reach the Ready status.

```
kubectl get nodes --watch
```

11. (GPU nodes only) If you chose a GPU instance type and the Amazon EKS optimized accelerated AMI, then you must apply the [NVIDIA device plugin for Kubernetes](#) as a DaemonSet on your cluster. Replace `vX.X.X` with your desired [NVIDIA/k8s-device-plugin](#) version before running the following command.

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/vX.X.X/nvidia-device-plugin.yaml
```

Now that you have a working Amazon EKS cluster with nodes, you're ready to start installing Kubernetes add-ons and deploying applications to your cluster. The following documentation topics help you to extend the functionality of your cluster.

- The [IAM principal](#) that created the cluster is the only principal that can make calls to the Kubernetes API server with `kubectl` or the AWS Management Console. If you want other IAM principals to have access to your cluster, then you need to add them. For more information, see [Enabling IAM principal access to your cluster \(p. 420\)](#) and [Required permissions \(p. 529\)](#).
- We recommend blocking Pod access to IMDS if the following conditions are true:
 - You plan to assign IAM roles to all of your Kubernetes service accounts so that Pods only have the minimum permissions that they need.
 - No Pods in the cluster require access to the Amazon EC2 instance metadata service (IMDS) for other reasons, such as retrieving the current AWS Region.

For more information, see [Restrict access to the instance profile assigned to the worker node](#).

- [Autoscaling \(p. 75\)](#) – Configure the Kubernetes Cluster Autoscaler to automatically adjust the number of nodes in your node groups.
- [Deploy a sample application \(p. 356\)](#) to your cluster.
- [Cluster management \(p. 444\)](#) – Learn how to use important tools for managing your cluster.

Updating a managed node group

When you initiate a managed node group update, Amazon EKS automatically updates your nodes for you, completing the steps listed in [Managed node update behavior \(p. 94\)](#). If you're using an Amazon

EKS optimized AMI, Amazon EKS automatically applies the latest security patches and operating system updates to your nodes as part of the latest AMI release version.

There are several scenarios where it's useful to update your Amazon EKS managed node group's version or configuration:

- You have updated the Kubernetes version for your Amazon EKS cluster and want to update your nodes to use the same Kubernetes version.
- A new AMI release version is available for your managed node group. For more information about AMI versions, see these sections:
 - [Amazon EKS optimized Amazon Linux AMI versions \(p. 160\)](#)
 - [Amazon EKS optimized Bottlerocket AMIs \(p. 174\)](#)
 - [Amazon EKS optimized Windows AMI versions \(p. 189\)](#)
- You want to adjust the minimum, maximum, or desired count of the instances in your managed node group.
- You want to add or remove Kubernetes labels from the instances in your managed node group.
- You want to add or remove AWS tags from your managed node group.
- You need to deploy a new version of a launch template with configuration changes, such as an updated custom AMI.
- You have deployed version 1.9.0 or later of the Amazon VPC CNI add-on, enabled the add-on for prefix delegation, and want new AWS Nitro System instances in a node group to support a significantly increased number of Pods. For more information, see [Increase the amount of available IP addresses for your Amazon EC2 nodes \(p. 318\)](#).
- You have enabled IP prefix delegation for Windows nodes and want new AWS Nitro System instances in a node group to support a significantly increased number of Pods. For more information, see [the section called "Increase available IP addresses" \(p. 318\)](#).

If there's a newer AMI release version for your managed node group's Kubernetes version, you can update your node group's version to use the newer AMI version. Similarly, if your cluster is running a Kubernetes version that's newer than your node group, you can update the node group to use the latest AMI release version to match your cluster's Kubernetes version.

When a node in a managed node group is terminated due to a scaling operation or update, the Pods in that node are drained first. For more information, see [Managed node update behavior \(p. 94\)](#).

Update a node group version

You can update a node group version with `eksctl` or the AWS Management Console. The version that you update to can't be greater than the control plane's version.

`eksctl`

To update a node group version with `eksctl`

- Update a managed node group to the latest AMI release of the same Kubernetes version that's currently deployed on the nodes with the following command. Replace every `example value` with your own values.

```
eksctl upgrade nodegroup \
--name=node-group-name \
--cluster=my-cluster \
--region=region-code
```

Note

If you're upgrading a node group that's deployed with a launch template to a new launch template version, add `--launch-template-version` *version-number* to the preceding command. The launch template must meet the requirements described in [Customizing managed nodes with launch templates \(p. 98\)](#). If the launch template includes a custom AMI, the AMI must meet the requirements in [Specifying an AMI \(p. 102\)](#). When you upgrade your node group to a newer version of your launch template, every node is recycled to match the new configuration of the launch template version that's specified.

You can't directly upgrade a node group that's deployed without a launch template to a new launch template version. Instead, you must deploy a new node group using the launch template to update the node group to a new launch template version.

You can upgrade a node group to the same version as the control plane's Kubernetes version. For example, if you have a cluster running Kubernetes 1.27, you can upgrade nodes currently running Kubernetes 1.26 to version 1.27 with the following command.

```
eksctl upgrade nodegroup \
--name=node-group-name \
--cluster=my-cluster \
--region=region-code \
--kubernetes-version=1.27
```

AWS Management Console

To update a node group version with the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose the cluster that contains the node group to update.
3. If at least one node group has an available update, a box appears at the top of the page notifying you of the available update. If you select the **Compute** tab, you'll see **Update now** in the **AMI release version** column in the **Node groups** table for the node group that has an available update. To update the node group, choose **Update now**.

You won't see a notification for node groups that were deployed with a custom AMI. If your nodes are deployed with a custom AMI, complete the following steps to deploy a new updated custom AMI.

 - a. Create a new version of your AMI.
 - b. Create a new launch template version with the new AMI ID.
 - c. Upgrade the nodes to the new version of the launch template.
4. On the **Update node group version** dialog box, activate or deactivate the following options:
 - **Update node group version** – This option is unavailable if you deployed a custom AMI or your Amazon EKS optimized AMI is currently on the latest version for your cluster.
 - **Change launch template version** – This option is unavailable if the node group is deployed without a custom launch template. You can only update the launch template version for a node group that has been deployed with a custom launch template. Select the **Launch template version** that you want to update the node group to. If your node group is configured with a custom AMI, then the version that you select must also specify an AMI. When you upgrade to a newer version of your launch template, every node is recycled to match the new configuration of the launch template version specified.
5. For **Update strategy**, select one of the following options:

- **Rolling update** – This option respects the Pod disruption budgets for your cluster. Updates fail if there's a Pod disruption budget issue that causes Amazon EKS to be unable to gracefully drain the Pods that are running on this node group.
- **Force update** – This option doesn't respect Pod disruption budgets. Updates occur regardless of Pod disruption budget issues by forcing node restarts to occur.

6. Choose **Update**.

Edit a node group configuration

You can modify some of the configurations of a managed node group.

To edit a node group configuration

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose the cluster that contains the node group to edit.
3. Select the **Compute** tab.
4. Select the node group to edit, and then choose **Edit**.
5. (Optional) On the **Edit node group** page, do the following:
 - a. Edit the **Node group scaling configuration**.
 - **Desired size** – Specify the current number of nodes that the managed node group should maintain.
 - **Minimum size** – Specify the minimum number of nodes that the managed node group can scale in to.
 - **Maximum size** – Specify the maximum number of nodes that the managed node group can scale out to. For the maximum number of nodes supported in a node group, see [Amazon EKS service quotas \(p. 455\)](#).
 - b. (Optional) Add or remove **Kubernetes labels** to the nodes in your node group. The labels shown here are only the labels that you have applied with Amazon EKS. Other labels may exist on your nodes that aren't shown here.
 - c. (Optional) Add or remove **Kubernetes taints** to the nodes in your node group. Added taints can have the effect of either **NoSchedule**, **NoExecute**, or **PreferNoSchedule**. For more information, see [Node taints on managed node groups \(p. 97\)](#).
 - d. (Optional) Add or remove **Tags** from your node group resource. These tags are only applied to the Amazon EKS node group. They don't propagate to other resources, such as subnets or Amazon EC2 instances in the node group.
 - e. (Optional) Edit the **Node Group update configuration**. Select either **Number** or **Percentage**.
 - **Number** – Select and specify the number of nodes in your node group that can be updated in parallel. These nodes will be unavailable during update.
 - **Percentage** – Select and specify the percentage of nodes in your node group that can be updated in parallel. These nodes will be unavailable during update. This is useful if you have many nodes in your node group.
 - f. When you're finished editing, choose **Save changes**.

Managed node update behavior

The Amazon EKS managed worker node upgrade strategy has four different phases described in the following sections.

Setup phase

The setup phase has these steps:

1. It creates a new Amazon EC2 launch template version for the Auto Scaling group that's associated with your node group. The new launch template version uses the target AMI or a custom launch template version for the update.
2. It updates the Auto Scaling group to use the latest launch template version.
3. It determines the maximum quantity of nodes to upgrade in parallel using the `updateConfig` property for the node group. The maximum unavailable has a quota of 100 nodes. The default value is one node. For more information, see the [updateConfig](#) property in the *Amazon EKS API Reference*.

Scale up phase

When upgrading the nodes in a managed node group, the upgraded nodes are launched in the same Availability Zone as those that are being upgraded. To guarantee this placement, we use Amazon EC2's Availability Zone Rebalancing. For more information, see [Availability Zone Rebalancing](#) in the *Amazon EC2 Auto Scaling User Guide*. To meet this requirement, it's possible that we'd launch up to two instances per Availability Zone in your managed node group.

The scale up phase has these steps:

1. It increments the Auto Scaling Group's maximum size and desired size by the larger of either:
 - Up to twice the number of Availability Zones that the Auto Scaling group is deployed in.
 - The maximum unavailable of upgrade.

For example, if your node group has five Availability Zones and `maxUnavailable` as one, the upgrade process can launch a maximum of 10 nodes. However when `maxUnavailable` is 20 (or anything higher than 10, the process would launch 20 new nodes).

2. After scaling the Auto Scaling group, it checks if the nodes using the latest configuration are present in the node group. This step succeeds only when it meets these criteria:
 - At least one new node is launched in every Availability Zone where the node exists.
 - Every new node should be in Ready state.
 - New nodes should have Amazon EKS applied labels.

These are the Amazon EKS applied labels on the worker nodes in a regular node group:

- `eks.amazonaws.com/nodegroup-image=$amiName`
- `eks.amazonaws.com/nodegroup=$nodeGroupName`

These are the Amazon EKS applied labels on the worker nodes in a custom launch template or AMI node group:

- `eks.amazonaws.com/nodegroup-image=$amiName`
- `eks.amazonaws.com/nodegroup=$nodeGroupName`
- `eks.amazonaws.com/sourceLaunchTemplateId=$launchTemplateId`
- `eks.amazonaws.com/sourceLaunchTemplateVersion=$launchTemplateVersion`

3. It marks nodes as unschedulable to avoid scheduling new Pods. It also labels nodes with `node.kubernetes.io/exclude-from-external-load-balancers=true` to remove the nodes from load balancers before terminating the nodes.

The following are known reasons which lead to a `NodeCreationFailure` error in this phase:

Insufficient capacity in the Availability Zone

There is a possibility that the Availability Zone might not have capacity of requested instance types. It's recommended to configure multiple instance types while creating a managed node group.

EC2 instance limits in your account

You may need to increase the number of Amazon EC2 instances your account can run simultaneously using Service Quotas. For more information, see [EC2 Service Quotas](#) in the *Amazon Elastic Compute Cloud User Guide for Linux Instances*.

Custom user data

Custom user data can sometimes break the bootstrap process. This scenario can lead to the kubelet not starting on the node or nodes not getting expected Amazon EKS labels on them. For more information on handling custom LT/AMI, see [Specifying an AMI \(p. 102\)](#).

Any changes which make a node unhealthy or not ready

Node disk pressure, memory pressure, and similar conditions can lead to a node not going to Ready state.

Upgrade phase

The upgrade phase has these steps:

1. It randomly selects a node that needs to be upgraded, up to the maximum unavailable configured for the node group.
2. It drains the Pods from the node. If the Pods don't leave the node within 15 minutes and there's no force flag, the upgrade phase fails with a PodEvictionFailure error. For this scenario, you can apply the force flag with the update-nodegroup-version request to delete the Pods.
3. It cordons the node after every Pod is evicted and waits for 60 seconds. This is done so that the service controller doesn't send any new requests to this node and removes this node from its list of active nodes.
4. It sends a termination request to the Auto Scaling Group for the cordoned node.
5. It repeats the previous upgrade steps until there are no nodes in the node group that are deployed with the earlier version of the launch template.

The following are known reasons which lead to a PodEvictionFailure error in this phase:

Aggressive PDB

Aggressive PDB is defined on the Pod or there are multiple PDBs pointing to the same Pod.

Deployment tolerating all the taints

Once every Pod is evicted, it's expected for the node to be empty because the node is [tainted](#) in the earlier steps. However, if the deployment tolerates every taint, then the node is more likely to be non-empty, leading to Pod eviction failure.

Scale down phase

The scale down phase decrements the Auto Scaling group maximum size and desired size by one to return to values before the update started.

If the Upgrade workflow determines that the Cluster Autoscaler is scaling up the node group during the scale down phase of the workflow, it exits immediately without bringing the node group back to its original size.

Node taints on managed node groups

Amazon EKS supports configuring Kubernetes taints through managed node groups. Taints and tolerations work together to ensure that Pods aren't scheduled onto inappropriate nodes. One or more taints can be applied to a node. This marks that the node shouldn't accept any Pods that don't tolerate the taints. Tolerations are applied to Pods and allow, but don't require, the Pods to schedule onto nodes with matching taints. For more information, see [Taints and Toleration](#)s in the Kubernetes documentation.

Kubernetes node taints can be applied to new and existing managed node groups using the AWS Management Console or through the Amazon EKS API.

- For information on creating a node group with a taint using the AWS Management Console, see [Creating a managed node group \(p. 85\)](#).
- The following is an example of creating a node group with a taint using the AWS CLI:

```
aws eks create-nodegroup \
  --cli-input-json '
{
  "clusterName": "my-cluster",
  "nodegroupName": "node-taints-example",
  "subnets": [
    "subnet-1234567890abcdef0",
    "subnet-abcdef01234567890",
    "subnet-021345abcdef67890"
  ],
  "nodeRole": "arn:aws:iam::111122223333:role/AmazonEKSNodeRole",
  "taints": [
    {
      "key": "dedicated",
      "value": "gpuGroup",
      "effect": "NO_SCHEDULE"
    }
  ]
}'
```

For more information and examples of usage, see [taint](#) in the Kubernetes reference documentation.

Note

- Taints can be updated after you create the node group using the `UpdateNodegroupConfig` API.
- The taint key must begin with a letter or number. It can contain letters, numbers, hyphens (-), periods (.), and underscores (_). It can be up to 63 characters long.
- Optionally, the taint key can begin with a DNS subdomain prefix and a single /. If it begins with a DNS subdomain prefix, it can be 253 characters long.
- The value is optional and must begin with a letter or number. It can contain letters, numbers, hyphens (-), periods (.), and underscores (_). It can be up to 63 characters long.
- When using Kubernetes directly or the AWS Management Console, the taint effect must be `NoSchedule`, `PrefeNoSchedule`, or `NoExecute`. However, when using the AWS CLI or API, the taint effect must be `NO_SCHEDULE`, `PREFER_NO_SCHEDULE`, or `NO_EXECUTE`.
- A maximum of 50 taints are allowed per node group.
- If taints that were created using a managed node group are removed manually from a node, then Amazon EKS doesn't add the taints back to the node. This is true even if the taints are specified in the managed node group configuration.

You can use the [aws_eks_update-nodegroup-config](#) AWS CLI command to add, remove, or replace taints for managed node groups. For more information, see [Configuring taints for Managed Node Groups](#) in the Amazon EKS Workshop.

Customizing managed nodes with launch templates

For the highest level of customization, you can deploy managed nodes using your own launch template. Using a launch template allows capabilities such as the following:

- Provide bootstrap arguments at deployment of a node, such as extra [kubelet](#) arguments.
- Assign IP addresses to Pods from a different CIDR block than the IP address assigned to the node.
- Deploy your own custom AMI to nodes.
- Deploy your own custom CNI to nodes.

When you give your own launch template upon first creating a managed node group, you will also have greater flexibility later. As long as you deploy a managed node group with your own launch template, you can iteratively update it with a different version of the same launch template. When you update your node group to a different version of your launch template, all nodes in the group are recycled to match the new configuration of the specified launch template version.

Managed node groups are always deployed with a launch template to be used with the Amazon EC2 Auto Scaling group. When you don't provide a launch template, the Amazon EKS API creates one automatically with default values in your account. However, we don't recommend that you modify auto-generated launch templates. Furthermore, existing node groups that don't use a custom launch template can't be updated directly. Instead, you must create a new node group with a custom launch template to do so.

Launch template configuration basics

You can create an Amazon EC2 Auto Scaling launch template with the AWS Management Console, AWS CLI, or an AWS SDK. For more information, see [Creating a Launch Template for an Auto Scaling group](#) in the *Amazon EC2 Auto Scaling User Guide*. Some of the settings in a launch template are similar to the settings used for managed node configuration. When deploying or updating a node group with a launch template, some settings must be specified in either the node group configuration or the launch template. Don't specify a setting in both places. If a setting exists where it shouldn't, then operations such as creating or updating a node group fail.

The following table lists the settings that are prohibited in a launch template. It also lists similar settings, if any are available, that are required in the managed node group configuration. The listed settings are the settings that appear in the console. They might have similar but different names in the AWS CLI and SDK.

Launch template – Prohibited	Amazon EKS node group configuration
Subnet under Network interfaces (Add network interface)	Subnets under Node group network configuration on the Specify networking page
IAM instance profile under Advanced details	Node IAM role under Node group configuration on the Configure Node group page
Shutdown behavior and Stop - Hibernate behavior under Advanced details . Retain default Don't include in launch template setting in launch template for both settings.	No equivalent. Amazon EKS must control the instance lifecycle, not the Auto Scaling group.

The following table lists the prohibited settings in a managed node group configuration. It also lists similar settings, if any are available, which are required in a launch template. The listed settings are the settings that appear in the console. They might have similar names in the AWS CLI and SDK.

Amazon EKS node group configuration – Prohibited	Launch template
<p>(Only if you specified a custom AMI in a launch template) AMI type under Node group compute configuration on Set compute and scaling configuration page – Console displays Specified in launch template and the AMI ID that was specified.</p> <p>If Application and OS Images (Amazon Machine Image) wasn't specified in the launch template, you can select an AMI in the node group configuration.</p>	<p>Application and OS Images (Amazon Machine Image) under Launch template contents – You must specify an ID if you have either of the following requirements:</p> <ul style="list-style-type: none"> Using a custom AMI. If you specify an AMI that doesn't meet the requirements listed in Specifying an AMI (p. 102), the node group deployment will fail. Want to provide user data to provide arguments to the <code>bootstrap.sh</code> file included with an Amazon EKS optimized AMI. You can enable your instances to assign a significantly higher number of IP addresses to Pods, assign IP addresses to Pods from a different CIDR block than the instance's, enable the <code>containerd</code> runtime, or deploy a private cluster without outbound internet access. For more information, see the following topics: <ul style="list-style-type: none"> Increase the amount of available IP addresses for your Amazon EC2 nodes (p. 318) Custom networking for pods (p. 306) Enable the containerd runtime bootstrap flag (p. 157) Private cluster requirements (p. 58) Specifying an AMI (p. 102)
<p>Disk size under Node group compute configuration on Set compute and scaling configuration page – Console displays Specified in launch template.</p>	<p>Size under Storage (Volumes) (Add new volume). You must specify this in the launch template.</p>
<p>SSH key pair under Node group configuration on the Specify Networking page – The console displays the key that was specified in the launch template or displays Not specified in launch template.</p>	<p>Key pair name under Key pair (login).</p>
<p>You can't specify source security groups that are allowed remote access when using a launch template.</p>	<p>Security groups under Network settings for the instance or Security groups under Network interfaces (Add network interface), but not both. For more information, see Using custom security groups (p. 100).</p>

Note

- If you deploy a node group using a launch template, specify zero or one **Instance type** under **Launch template contents** in a launch template. Alternatively, you can specify 0–20 instance

types for **Instance types** on the [Set compute and scaling configuration](#) page in the console. Or, you can do so using other tools that use the Amazon EKS API. If you specify an instance type in a launch template, and use that launch template to deploy your node group, then you can't specify any instance types in the console or using other tools that use the Amazon EKS API. If you don't specify an instance type in a launch template, in the console, or using other tools that use the Amazon EKS API, the t3.medium instance type is used. If your node group is using the Spot capacity type, then we recommend specifying multiple instance types using the console. For more information, see [Managed node group capacity types \(p. 83\)](#).

- If any containers that you deploy to the node group use the Instance Metadata Service Version 2, make sure to set the **Metadata response hop limit** to 2 in your launch template. For more information, see [Instance metadata and user data](#) in the *Amazon EC2 User Guide for Linux Instances*. If you deploy a managed node group without using a custom launch template, this value is automatically set for the node group in the default launch template.

Tagging Amazon EC2 instances

You can use the `TagSpecification` parameter of a launch template to specify which tags to apply to Amazon EC2 instances in your node group. The IAM entity calling the `CreateNodegroup` or `UpdateNodegroupVersion` APIs must have permissions for `ec2:RunInstances` and `ec2:CreateTags`, and the tags must be added to the launch template.

Using custom security groups

You can use a launch template to specify custom Amazon EC2 [security groups](#) to apply to instances in your node group. This can be either in the instance level security groups parameter or as part of the network interface configuration parameters. However, you can't create a launch template that specifies both instance level and network interface security groups. Consider the following conditions that apply to using custom security groups with managed node groups:

- Amazon EKS only allows launch templates with a single network interface specification.
- By default, Amazon EKS applies the [cluster security group \(p. 263\)](#) to the instances in your node group to facilitate communication between nodes and the control plane. If you specify custom security groups in the launch template using either option mentioned earlier, Amazon EKS doesn't add the cluster security group. So, you must ensure that the inbound and outbound rules of your security groups enable communication with the endpoint of your cluster. If your security group rules are incorrect, the worker nodes can't join the cluster. For more information about security group rules, see [Amazon EKS security group requirements and considerations \(p. 263\)](#).
- If you need SSH access to the instances in your node group, include a security group that allows that access.

Amazon EC2 user data

The launch template includes a section for custom user data. You can specify configuration settings for your node group in this section without manually creating individual custom AMIs. For more information about the settings available for Bottlerocket, see [Using user data](#) on GitHub.

You can supply Amazon EC2 user data in your launch template using cloud-init when launching your instances. For more information, see the [cloud-init](#) documentation. Your user data can be used to perform common configuration operations. This includes the following operations:

- [Including users or groups](#)
- [Installing packages](#)

Amazon EC2 user data in launch templates that are used with managed node groups must be in the [MIME multi-part archive](#) format for Amazon Linux AMIs and TOML format for Bottlerocket AMIs. This is because your user data is merged with Amazon EKS user data required for nodes to join the cluster. Don't specify any commands in your user data that starts or modifies kubelet. This is performed as part of the user data merged by Amazon EKS. Certain kubelet parameters, such as setting labels on nodes, can be configured directly through the managed node groups API.

Note

For more information about advanced kubelet customization, including manually starting it or passing in custom configuration parameters, see [Specifying an AMI \(p. 102\)](#). If a custom AMI ID is specified in a launch template, Amazon EKS doesn't merge user data.

The following details provide more information about the user data section.

Amazon Linux user data

You can combine multiple user data blocks together into a single MIME multi-part file. For example, you can combine a cloud booothook that configures the Docker daemon with a user data shell script that installs a custom package. A MIME multi-part file consists of the following components:

- The content type and part boundary declaration – Content-Type: multipart/mixed; boundary="==MYBOUNDARY=="
- The MIME version declaration – MIME-Version: 1.0
- One or more user data blocks, which contain the following components:
 - The opening boundary, which signals the beginning of a user data block – ==MYBOUNDARY==
 - The content type declaration for the block: Content-Type: text/cloud-config; charset="us-ascii". For more information about content types, see the [cloud-init](#) documentation.
 - The content of the user data (for example, a list of shell commands or cloud-init directives).
 - The closing boundary, which signals the end of the MIME multi-part file: -- ==MYBOUNDARY==--

The following is an example of a MIME multi-part file that you can use to create your own.

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=="==MYBOUNDARY=="

==MYBOUNDARY==
Content-Type: text/x-shellscript; charset="us-ascii"

#!/bin/bash
echo "Running custom user data script"

==MYBOUNDARY==--
```

Bottlerocket user data

Bottlerocket structures user data in the TOML format. You can provide user data to be merged with the user data provided by Amazon EKS. For example, you can provide additional kubelet settings.

```
[settings.kubernetes.system-reserved]
cpu = "10m"
memory = "100Mi"
ephemeral-storage= "1Gi"
```

For more information about the supported settings, see [Bottlerocket documentation](#). You can configure node labels and [taints \(p. 97\)](#) in your user data. However, we recommend that you

configure these within your node group instead. Amazon EKS applies these configurations when you do so.

When user data is merged, formatting isn't preserved, but the content remains the same. The configuration that you provide in your user data overrides any settings that are configured by Amazon EKS. So, if you set `settings.kubernetes.max-pods` or `settings.kubernetes.cluster-dns-ip`, values in your user data are applied to the nodes.

Amazon EKS doesn't support all valid TOML. The following is a list of known unsupported formats:

- Quotes within quoted keys: 'quoted "value"' = "value"
- Escaped quotes in values: str = "I'm a string. \"You can quote me\""
- Mixed floats and integers: numbers = [0.1, 0.2, 0.5, 1, 2, 5]
- Mixed types in arrays: contributors = ["foo@example.com", { name = "Baz", email = "baz@example.com" }]
- Bracketed headers with quoted keys: [foo."bar.baz"]

Windows user data

Windows user data uses PowerShell commands. When creating a managed node group, your custom user data combines with Amazon EKS managed user data. Your PowerShell commands come first, followed by the managed user data commands, all within one `<powershell></powershell>` tag.

Note

When no AMI ID is specified in the launch template, don't use the Windows Amazon EKS Bootstrap script in user data to configure Amazon EKS.

Example user data is as follows.

```
<powershell>
Write-Host "Running custom user data script"
</powershell>
```

Specifying an AMI

If you have either of the following requirements, then specify an AMI ID in the `imageId` field of your launch template. Select the requirement you have for additional information.

Provide user data to pass arguments to the `bootstrap.sh` file included with an Amazon EKS optimized Linux/Bottlerocket AMI

Bootstrapping is a term used to describe adding commands that can be run when an instance starts. For example, bootstrapping allows using extra `kublet` arguments. You can pass arguments to the `bootstrap.sh` script by using `eksctl` without specifying a launch template. Or you can do so by specifying the information in the user data section of a launch template.

`eksctl` without specifying a launch template

Create a file named `my-nodegroup.yaml` with the following contents. Replace every *example value* with your own values. The `--apiserver-endpoint`, `--b64-cluster-ca`, and `--dns-cluster-ip` arguments are optional. However, defining them allows the `bootstrap.sh` script to avoid making a `describeCluster` call. This is useful in private cluster setups or clusters where you're scaling in and out nodes frequently. For more information on the `bootstrap.sh` script, see the [bootstrap.sh](#) file on GitHub.

- The only required argument is the cluster name (*my-cluster*).
- To retrieve an optimized AMI ID for ami-*1234567890abcdef0*, you can use the tables in the following sections:
 - [Retrieving Amazon EKS optimized Amazon Linux AMI IDs \(p. 161\)](#)
 - [Retrieving Amazon EKS optimized Bottlerocket AMI IDs \(p. 175\)](#)
 - [Retrieving Amazon EKS optimized Windows AMI IDs \(p. 211\)](#)
- To retrieve the *certificate-authority* for your cluster, run the following command.

```
aws eks describe-cluster --query "cluster.certificateAuthority.data" --output text --name my-cluster --region region-code
```

- To retrieve the *api-server-endpoint* for your cluster, run the following command.

```
aws eks describe-cluster --query "cluster.endpoint" --output text --name my-cluster --region region-code
```

- The value for --dns-cluster-ip is your service CIDR with .10 at the end. To retrieve the *service-cidr* for your cluster, run the following command. For example, if the returned value for is ipv4 10.100.0.0/16, then your value is *10.100.0.10*.

```
aws eks describe-cluster --query "cluster.kubernetesNetworkConfig.serviceIpv4Cidr" --output text --name my-cluster --region region-code
```

- This example creates a node group using *containerd* as the runtime, but you can modify it as needed.
- This example provides a kubelet argument to set a custom max-pods value using the bootstrap.sh script included with the Amazon EKS optimized AMI. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters. For help with selecting *my-max-pods-value*, see [Amazon EKS recommended maximum Pods for each Amazon EC2 instance type \(p. 154\)](#).

```
---
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-cluster
  region: region-code

managedNodeGroups:
  - name: my-nodegroup
    ami: ami-1234567890abcdef0
    instanceType: m5.large
    privateNetworking: true
    disableIMDSv1: true
    labels: { x86-al2-specified-mng }
    overrideBootstrapCommand: |
      #!/bin/bash
      /etc/eks/bootstrap.sh my-cluster \
        --b64-cluster-ca certificate-authority \
        --apiserver-endpoint api-server-endpoint \
        --dns-cluster-ip service-cidr.10 \
        --container-runtime containerd \
        --kubelet-extra-args '--max-pods=my-max-pods-value' \
        --use-max-pods false
```

For every available `eksctl config` file option, see [Config file schema](#) in the `eksctl` documentation. The `eksctl` utility still creates a launch template for you and populates its user data with the data that you provide in the config file.

Create a node group with the following command.

```
eksctl create nodegroup --config-file=my-nodegroup.yaml
```

User data in a launch template

Specify the following information in the user data section of your launch template. Replace every *example value* with your own values. The `--apiserver-endpoint`, `--b64-cluster-ca`, and `--dns-cluster-ip` arguments are optional. However, defining them allows the `bootstrap.sh` script to avoid making a `describeCluster` call. This is useful in private cluster setups or clusters where you're scaling in and out nodes frequently. For more information on the `bootstrap.sh` script, see the [bootstrap.sh](#) file on GitHub.

- The only required argument is the cluster name (*my-cluster*).
- To retrieve the *certificate-authority* for your cluster, run the following command.

```
aws eks describe-cluster --query "cluster.certificateAuthority.data" --output text --name my-cluster --region region-code
```

- To retrieve the *api-server-endpoint* for your cluster, run the following command.

```
aws eks describe-cluster --query "cluster.endpoint" --output text --name my-cluster --region region-code
```

- The value for `--dns-cluster-ip` is your service CIDR with .10 at the end. To retrieve the *service-cidr* for your cluster, run the following command. For example, if the returned value for is `ipv4 10.100.0.0/16`, then your value is *10.100.0.10*.

```
aws eks describe-cluster --query "cluster.kubernetesNetworkConfig.serviceIpv4Cidr" --output text --name my-cluster --region region-code
```

- This example creates a node group using *containerd* as the runtime, but you can modify it as needed.
- This example provides a `kubelet` argument to set a custom `max-pods` value using the `bootstrap.sh` script included with the Amazon EKS optimized AMI. For help with selecting *my-max-pods-value*, see [Amazon EKS recommended maximum Pods for each Amazon EC2 instance type \(p. 154\)](#).

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="==MYBOUNDARY=="

==MYBOUNDARY==
Content-Type: text/x-shellscript; charset="us-ascii"

#!/bin/bash
set -ex
/etc/eks/bootstrap.sh my-cluster \
--b64-cluster-ca certificate-authority \
--apiserver-endpoint api-server-endpoint \
--dns-cluster-ip service-cidr.10 \
--container-runtime containerd \
--kubelet-extra-args '--max-pods=my-max-pods-value' \
--use-max-pods false
```

====MYBOUNDARY====

Provide user data to pass arguments to the `Start-EKSBootstrap.ps1` file included with an Amazon EKS optimized Windows AMI

Bootstrapping is a term used to describe adding commands that can be run when an instance starts. You can pass arguments to the `Start-EKSBootstrap.ps1` script by using `eksctl` without specifying a launch template. Or you can do so by specifying the information in the user data section of a launch template.

If you want to specify a custom Windows AMI ID, keep in mind the following considerations:

- You must use a launch template and give the required bootstrap commands in the user data section. To retrieve your desired Windows ID, you can use the table in [Amazon EKS optimized Windows AMIs \(p. 184\)](#).
- There are several limits and conditions. For example, you must add `eks:kube-proxy-windows` to your AWS IAM Authenticator configuration map. For more information, see [Limits and conditions when specifying an AMI ID \(p. 106\)](#).

Specify the following information in the user data section of your launch template. Replace every *example value* with your own values. The `-APIServerEndpoint`, `-Base64ClusterCA`, and `-DNSClusterIP` arguments are optional. However, defining them allows the `Start-EKSBootstrap.ps1` script to avoid making a `describeCluster` call.

- The only required argument is the cluster name (*my-cluster*).
- To retrieve the *certificate-authority* for your cluster, run the following command.

```
aws eks describe-cluster --query "cluster.certificateAuthority.data" --output text --name my-cluster --region region-code
```

- To retrieve the *api-server-endpoint* for your cluster, run the following command.

```
aws eks describe-cluster --query "cluster.endpoint" --output text --name my-cluster --region region-code
```

- The value for `--dns-cluster-ip` is your service CIDR with .10 at the end. To retrieve the *service-cidr* for your cluster, run the following command. For example, if the returned value for is `ipv4 10.100.0.0/16`, then your value is *10.100.0.10*.

```
aws eks describe-cluster --query "cluster.kubernetesNetworkConfig.serviceIpv4Cidr" --output text --name my-cluster --region region-code
```

- This example creates a node group using *containerd* as the runtime, but you can modify it as needed.

For additional arguments, see [Bootstrap script configuration parameters \(p. 186\)](#).

Note

If you're using custom service CIDR, then you need to specify it using the `-ServiceCIDR` parameter. Otherwise, the DNS resolution for Pods in the cluster will fail.

```
<powershell>
[string]$EKSBootstrapScriptFile = "$env:ProgramFiles\Amazon\EKS\Start-EKSBootstrap.ps1"
& $EKSBootstrapScriptFile -EKSClusterName my-cluster
```

```
-Base64ClusterCA certificate-authority
-APIServerEndpoint api-server-endpoint
-DNSClusterIP service-cidr.10
-ContainerRuntime containerd
</powershell>
```

Run a custom AMI due to specific security, compliance, or internal policy requirements

For more information, see [Amazon Machine Images \(AMI\)](#) in the *Amazon EC2 User Guide for Linux Instances*. The Amazon EKS AMI build specification contains resources and configuration scripts for building a custom Amazon EKS AMI based on Amazon Linux 2. For more information, see [Amazon EKS AMI Build Specification](#) on GitHub. To build custom AMIs installed with other operating systems, see [Amazon EKS Sample Custom AMIs](#) on GitHub.

Important

When specifying an AMI, Amazon EKS doesn't merge any user data. Rather, you're responsible for supplying the required bootstrap commands for nodes to join the cluster. If your nodes fail to join the cluster, the Amazon EKS `CreateNodegroup` and `UpdateNodegroupVersion` actions also fail.

Limits and conditions when specifying an AMI ID

The following are the limits and conditions involved with specifying an AMI ID with managed node groups:

- You must create a new node group to switch between specifying an AMI ID in a launch template and not specifying an AMI ID.
- You aren't notified in the console when a newer AMI version is available. To update your node group to a newer AMI version, you need to create a new version of your launch template with an updated AMI ID. Then, you need to update the node group with the new launch template version.
- The following fields can't be set in the API if you specify an AMI ID:
 - `amiType`
 - `releaseVersion`
 - `version`
- Any taints set in the API are applied asynchronously if you specify an AMI ID. To apply taints prior to a node joining the cluster, you must pass the taints to kubelet in your user data using the `--register-with-taints` command line flag. For more information, see [kubelet](#) in the Kubernetes documentation.
- When specifying a custom AMI ID for Windows managed node groups, add `eks:kube-proxy-windows` to your AWS IAM Authenticator configuration map. This is required for DNS to function properly.

1. Open the AWS IAM Authenticator configuration map for editing.

```
kubectl edit -n kube-system cm aws-auth
```

2. Add this entry to the `groups` list under each `rolearn` associated with Windows nodes. Your configuration map should look similar to [aws-auth-cm-windows.yaml](#).

```
- eks:kube-proxy-windows
```

3. Save the file and exit your text editor.

Deleting a managed node group

This topic describes how you can delete an Amazon EKS managed node group. When you delete a managed node group, Amazon EKS first sets the minimum, maximum, and desired size of your Auto Scaling group to zero. This then causes your node group to scale down.

Before each instance is terminated, Amazon EKS sends a signal to drain the Pods from that node. If the Pods haven't drained after a few minutes, Amazon EKS lets Auto Scaling continue the termination of the instance. After every instance is terminated, the Auto Scaling group is deleted.

Important

If you delete a managed node group that uses a node IAM role that isn't used by any other managed node group in the cluster, the role is removed from the [aws-auth ConfigMap \(p. 420\)](#). If any of the self-managed node groups in the cluster are using the same node IAM role, the self-managed nodes move to the NotReady status. Additionally, the cluster operation are also disrupted. You can add the mapping back to the ConfigMap to minimize disruption.

You can delete a managed node group with `eksctl` or the AWS Management Console.

`eksctl`

To delete a managed node group with `eksctl`

Enter the following command. Replace every *example value* with your own values.

```
eksctl delete nodegroup \
--cluster my-cluster \
--name my-mng \
--region region-code
```

For more options, see [Deleting and draining nodegroups](#) in the `eksctl` documentation.

AWS Management Console

To delete your managed node group with the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. On the **Clusters** page, choose the cluster that contains the node group to delete.
3. On the selected cluster page, choose the **Compute** tab.
4. In the **Node groups** section, choose the node group to delete. Then choose **Delete**.
5. In the **Delete node group** confirmation dialog box, enter the name of the node group. Then choose **Delete**.

AWS CLI

To delete your managed node group with the AWS CLI

1. Enter the following command. Replace every *example value* with your own values.

```
aws eks delete-nodegroup \
--cluster-name my-cluster \
--nodegroup-name my-mng \
--region region-code
```

2. Use the arrow keys on your keyboard to scroll through the response output. Press the **q** key when you're finished.

For more options, see the [delete-nodegroup](#) command in the *AWS CLI Command Reference*.

Self-managed nodes

A cluster contains one or more Amazon EC2 nodes that Pods are scheduled on. Amazon EKS nodes run in your AWS account and connect to the control plane of your cluster through the cluster API server endpoint. You're billed for them based on Amazon EC2 prices. For more information, see [Amazon EC2 pricing](#).

A cluster can contain several node groups. Each node group contains one or more nodes that are deployed in an [Amazon EC2 Auto Scaling group](#). The instance type of the nodes within the group can vary, such as when using [attribute-based instance type selection](#) with [Karpenter](#). All instances in a node group must use the [Amazon EKS node IAM role \(p. 501\)](#).

Amazon EKS provides specialized Amazon Machine Images (AMIs) that are called Amazon EKS optimized AMIs. The AMIs are configured to work with Amazon EKS. Their components include containerd, kubelet, and the AWS IAM Authenticator. The AMIs also contain a specialized [bootstrap script](#) that allows it to discover and connect to your cluster's control plane automatically.

If you restrict access to the public endpoint of your cluster using CIDR blocks, we recommend that you also enable private endpoint access. This is so that nodes can communicate with the cluster. Without the private endpoint enabled, the CIDR blocks that you specify for public access must include the egress sources from your VPC. For more information, see [Amazon EKS cluster endpoint access control \(p. 41\)](#).

To add self-managed nodes to your Amazon EKS cluster, see the topics that follow. If you launch self-managed nodes manually, add the following tag to each node. For more information, see [Adding and deleting tags on an individual resource](#). If you follow the steps in the guides that follow, the required tag is automatically added to nodes for you.

Key	Value
kubernetes.io/cluster/ <i>my-cluster</i>	owned

For more information about nodes from a general Kubernetes perspective, see [Nodes](#) in the Kubernetes documentation.

Topics

- [Launching self-managed Amazon Linux nodes \(p. 108\)](#)
- [Launching self-managed Bottlerocket nodes \(p. 114\)](#)
- [Launching self-managed Windows nodes \(p. 117\)](#)
- [Self-managed node updates \(p. 122\)](#)

Launching self-managed Amazon Linux nodes

This topic describes how you can launch Auto Scaling groups of Linux nodes that register with your Amazon EKS cluster. After the nodes join the cluster, you can deploy Kubernetes applications to them. You can also launch self-managed Amazon Linux 2 nodes with eksctl or the AWS Management Console. If you need to launch nodes on AWS Outposts, see [the section called "Launching nodes" \(p. 614\)](#).

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Creating an Amazon EKS cluster \(p. 25\)](#). If you have subnets in the AWS Region where you have AWS Outposts, AWS Wavelength, or AWS Local Zones enabled, those subnets must not have been passed in when you created your cluster.
- (Optional, but recommended) The Amazon VPC CNI plugin for Kubernetes add-on configured with its own IAM role that has the necessary IAM policy attached to it. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).
- Familiarity with the considerations listed in [Choosing an Amazon EC2 instance type \(p. 152\)](#). Depending on the instance type you choose, there may be additional prerequisites for your cluster and VPC.

eksctl

Prerequisite

Version `0.160.0` or later of the eksctl command line tool installed on your device or AWS CloudShell. To install or update eksctl, see [Installing or updating eksctl \(p. 13\)](#).

To launch self-managed Linux nodes using eksctl

1. (Optional) If the `AmazonEKS_CNI_Policy` managed IAM policy is attached to your [the section called "Node IAM role" \(p. 501\)](#), we recommend assigning it to an IAM role that you associate to the Kubernetes `aws-node` service account instead. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).
2. The following command creates a node group in an existing cluster. Replace `al-nodes` with a name for your node group. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters. Replace `my-cluster` with the name of your cluster. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters. Replace the remaining `example value` with your own values. The nodes are created with the same Kubernetes version as the control plane, by default.

Before choosing a value for `--node-type`, review [Choosing an Amazon EC2 instance type \(p. 152\)](#).

Replace `my-key` with the name of your Amazon EC2 key pair or public key. This key is used to SSH into your nodes after they launch. If you don't already have an Amazon EC2 key pair, you can create one in the AWS Management Console. For more information, see [Amazon EC2 key pairs](#) in the *Amazon EC2 User Guide for Linux Instances*.

Create your node group with the following command.

Important

If you want to deploy a node group to AWS Outposts, Wavelength, or Local Zone subnets, there are additional considerations:

- The subnets must not have been passed in when you created the cluster.
- You must create the node group with a config file that specifies the subnets and `volumeType: gp2`. For more information, see [Create a nodegroup from a config file](#) and [Config file schema](#) in the eksctl documentation.

```
eksctl create nodegroup \
--cluster my-cluster \
--name al-nodes \
--node-type t3.medium \
--nodes 3 \
```

```
--nodes-min 1 \
--nodes-max 4 \
--ssh-access \
--managed=false \
--ssh-public-key my-key
```

To deploy a node group that:

- can assign a significantly higher number of IP addresses to Pods than the default configuration, see [Increase the amount of available IP addresses for your Amazon EC2 nodes \(p. 318\)](#).
- can assign IPv4 addresses to Pods from a different CIDR block than that of the instance, see [Custom networking for pods \(p. 306\)](#).
- can assign IPv6 addresses to Pods and services, see [the section called “IPv6” \(p. 278\)](#).
- use the `containerd` runtime, you must deploy the node group using a config file. For more information, see [Enable the containerd runtime bootstrap flag \(p. 157\)](#).
- don't have outbound internet access, see [Private cluster requirements \(p. 58\)](#).

For a complete list of all available options and defaults, enter the following command.

```
eksctl create nodegroup --help
```

If nodes fail to join the cluster, then see [Nodes fail to join cluster \(p. 562\)](#) in the Troubleshooting guide.

An example output is as follows. Several lines are output while the nodes are created. One of the last lines of output is the following example line.

```
[#] created 1 nodegroup(s) in cluster "my-cluster"
```

3. (Optional) Deploy a [sample application \(p. 356\)](#) to test your cluster and Linux nodes.
4. We recommend blocking Pod access to IMDS if the following conditions are true:
 - You plan to assign IAM roles to all of your Kubernetes service accounts so that Pods only have the minimum permissions that they need.
 - No Pods in the cluster require access to the Amazon EC2 instance metadata service (IMDS) for other reasons, such as retrieving the current AWS Region.

For more information, see [Restrict access to the instance profile assigned to the worker node](#).

AWS Management Console

Step 1: To launch self-managed Linux nodes using the AWS Management Console

1. Download the latest version of the AWS CloudFormation template.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2022-12-23/
amazon-eks-nodegroup.yaml
```

2. Wait for your cluster status to show as ACTIVE. If you launch your nodes before the cluster is active, the nodes fail to register with the cluster and you will have to relaunch them.
3. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
4. Choose **Create stack** and then select **With new resources (standard)**.

5. For **Specify template**, select **Upload a template file** and then select **Choose file**.
6. Select the `amazon-eks-nodegroup.yaml` file that you downloaded.
7. Select **Next**.
8. On the **Specify stack details** page, enter the following parameters accordingly, and then choose **Next**:
 - **Stack name**: Choose a stack name for your AWS CloudFormation stack. For example, you can call it ***my-cluster-nodes***. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters.
 - **ClusterName**: Enter the name that you used when you created your Amazon EKS cluster. This name must equal the cluster name or your nodes can't join the cluster.
 - **ClusterControlPlaneSecurityGroup**: Choose the **SecurityGroups** value from the AWS CloudFormation output that you generated when you created your [VPC \(p. 259\)](#).

The following steps show one operation to retrieve the applicable group.

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose the name of the cluster.
3. Choose the **Networking** tab.
4. Use the **Additional security groups** value as a reference when selecting from the **ClusterControlPlaneSecurityGroup** dropdown list.
- **NodeGroupName**: Enter a name for your node group. This name can be used later to identify the Auto Scaling node group that's created for your nodes. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters.
- **NodeAutoScalingGroupMinSize**: Enter the minimum number of nodes that your node Auto Scaling group can scale in to.
- **NodeAutoScalingGroupDesiredCapacity**: Enter the desired number of nodes to scale to when your stack is created.
- **NodeAutoScalingGroupMaxSize**: Enter the maximum number of nodes that your node Auto Scaling group can scale out to.
- **NodeInstanceType**: Choose an instance type for your nodes. For more information, see [Choosing an Amazon EC2 instance type \(p. 152\)](#).
- **NodeImageIdSSMParam**: Pre-populated with the Amazon EC2 Systems Manager parameter of a recent Amazon EKS optimized AMI for a variable Kubernetes version. To use a different Kubernetes minor version supported with Amazon EKS, replace ***1.XX*** with a different [supported version \(p. 60\)](#). We recommend specifying the same Kubernetes version as your cluster.

To use the Amazon EKS optimized accelerated AMI, replace ***amazon-linux-2*** with ***amazon-linux-2-gpu***. To use the Amazon EKS optimized Arm AMI, replace ***amazon-linux-2*** with ***amazon-linux-2-arm64***.

Note

The Amazon EKS node AMI is based on Amazon Linux 2. You can track security or privacy events for Amazon Linux 2 at the [Amazon Linux Security Center](#) or subscribe to the associated [RSS feed](#). Security and privacy events include an overview of the issue, what packages are affected, and how to update your instances to correct the issue.

- **NodeImageId**: (Optional) If you're using your own custom AMI (instead of the Amazon EKS optimized AMI), enter a node AMI ID for your AWS Region. If you specify a value here, it overrides any values in the **NodeImageIdSSMParam** field.
- **NodeVolumeSize**: Specify a root volume size for your nodes, in GiB.

- **NodeVolumeType:** Specify a root volume type for your nodes.
- **KeyName:** Enter the name of an Amazon EC2 SSH key pair that you can use to connect using SSH into your nodes with after they launch. If you don't already have an Amazon EC2 key pair, you can create one in the AWS Management Console. For more information, see [Amazon EC2 key pairs](#) in the *Amazon EC2 User Guide for Linux Instances*.

Note

If you don't provide a key pair here, the AWS CloudFormation stack creation fails.

- **BootstrapArguments:** Specify any optional arguments to pass to the node bootstrap script, such as extra kubelet arguments. For more information, view the [bootstrap script usage information](#) on GitHub.

To deploy a node group that:

- can assign a significantly higher number of IP addresses to Pods than the default configuration, see [Increase the amount of available IP addresses for your Amazon EC2 nodes \(p. 318\)](#).
- can assign IPv4 addresses to Pods from a different CIDR block than that of the instance, see [Custom networking for pods \(p. 306\)](#).
- can assign IPv6 addresses to Pods and services, see [the section called "IPv6" \(p. 278\)](#).
- use the containerd runtime, you must deploy the node group using a config file. For more information, see [Enable the containerd runtime bootstrap flag \(p. 157\)](#).
- don't have outbound internet access, see [Private cluster requirements \(p. 58\)](#).
- **DisableIMDSv1:** By default, each node supports the Instance Metadata Service Version 1 (IMDSv1) and IMDSv2. You can disable IMDSv1. To prevent future nodes and Pods in the node group from using IMDSv1, set **DisableIMDSv1** to **true**. For more information about IMDS, see [Configuring the instance metadata service](#). For more information about restricting access to it on your nodes, see [Restrict access to the instance profile assigned to the worker node](#).
- **VpcId:** Enter the ID for the [VPC \(p. 259\)](#) that you created.
- **Subnets:** Choose the subnets that you created for your VPC. If you created your VPC using the steps that are described in [Creating a VPC for your Amazon EKS cluster \(p. 259\)](#), specify only the private subnets within the VPC for your nodes to launch into. You can see which subnets are private by opening each subnet link from the **Networking** tab of your cluster.

Important

- If any of the subnets are public subnets, then they must have the automatic public IP address assignment setting enabled. If the setting isn't enabled for the public subnet, then any nodes that you deploy to that public subnet won't be assigned a public IP address and won't be able to communicate with the cluster or other AWS services. If the subnet was deployed before March 26, 2020 using either of the [Amazon EKS AWS CloudFormation VPC templates \(p. 259\)](#), or by using eksctl, then automatic public IP address assignment is disabled for public subnets. For information about how to enable public IP address assignment for a subnet, see [Modifying the public IPv4 addressing attribute for your subnet](#). If the node is deployed to a private subnet, then it's able to communicate with the cluster and other AWS services through a NAT gateway.
- If the subnets don't have internet access, make sure that you're aware of the considerations and extra steps in [Private cluster requirements \(p. 58\)](#).
- If you select AWS Outposts, Wavelength, or Local Zone subnets, the subnets must not have been passed in when you created the cluster.

9. Select your desired choices on the **Configure stack options** page, and then choose **Next**.
10. Select the check box to the left of **I acknowledge that AWS CloudFormation might create IAM resources.**, and then choose **Create stack**.
11. When your stack has finished creating, select it in the console and choose **Outputs**.

12. Record the **NodeInstanceRole** for the node group that was created. You need this when you configure your Amazon EKS nodes.

Step 2: To enable nodes to join your cluster

Note

If you launched nodes inside a private VPC without outbound internet access, make sure to enable nodes to join your cluster from within the VPC.

1. Check to see if you already have an aws-auth ConfigMap.

```
kubectl describe configmap -n kube-system aws-auth
```

2. If you are shown an aws-auth ConfigMap, then update it as needed.

- a. Open the ConfigMap for editing.

```
kubectl edit -n kube-system configmap/aws-auth
```

- b. Add a new mapRoles entry as needed. Set the rolearn value to the **NodeInstanceRole** value that you recorded in the previous procedure.

```
[...]
data:
  mapRoles: |
    - rolearn: <ARN of instance role (not instance profile)>
      username: system:node:{{EC2PrivateDNSName}}
    groups:
      - system:bootstrappers
      - system:nodes
[...]
```

- c. Save the file and exit your text editor.

3. If you received an error stating "Error from server (NotFound): configmaps "aws-auth" not found, then apply the stock ConfigMap.

- a. Download the configuration map.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/clouformation/2020-10-29/aws-auth-cm.yaml
```

- b. In the aws-auth-cm.yaml file, set the rolearn value to the **NodeInstanceRole** value that you recorded in the previous procedure. You can do this with a text editor, or by replacing **my-node-instance-role** and running the following command:

```
sed -i.bak -e 's]<ARN of instance role (not instance profile)>|[my-node-instance-role]|' aws-auth-cm.yaml
```

- c. Apply the configuration. This command may take a few minutes to finish.

```
kubectl apply -f aws-auth-cm.yaml
```

4. Watch the status of your nodes and wait for them to reach the Ready status.

```
kubectl get nodes --watch
```

Enter Ctrl+C to return to a shell prompt.

Note

If you receive any authorization or resource type errors, see [Unauthorized or access denied \(kubectl\) \(p. 563\)](#) in the troubleshooting topic.

If nodes fail to join the cluster, then see [Nodes fail to join cluster \(p. 562\)](#) in the Troubleshooting guide.

5. (GPU nodes only) If you chose a GPU instance type and the Amazon EKS optimized accelerated AMI, you must apply the [NVIDIA device plugin for Kubernetes](#) as a DaemonSet on your cluster. Replace `vX.X.X` with your desired [NVIDIA/k8s-device-plugin](#) version before running the following command.

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/vX.X.X/nvidia-device-plugin.yaml
```

Step 3: Additional actions

1. (Optional) Deploy a [sample application \(p. 356\)](#) to test your cluster and Linux nodes.
2. (Optional) If the [AmazonEKS_CNI_Policy](#) managed IAM policy (if you have an IPv4 cluster) or the [AmazonEKS_CNI_IPv6_Policy](#) (that you [created yourself \(p. 276\)](#) if you have an IPv6 cluster) is attached to your [the section called "Node IAM role" \(p. 501\)](#), we recommend assigning it to an IAM role that you associate to the Kubernetes aws-node service account instead. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).
3. We recommend blocking Pod access to IMDS if the following conditions are true:
 - You plan to assign IAM roles to all of your Kubernetes service accounts so that Pods only have the minimum permissions that they need.
 - No Pods in the cluster require access to the Amazon EC2 instance metadata service (IMDS) for other reasons, such as retrieving the current AWS Region.

For more information, see [Restrict access to the instance profile assigned to the worker node](#).

Launching self-managed Bottlerocket nodes

Note

Managed node groups might offer some advantages for your use case. For more information, see [Managed node groups \(p. 81\)](#).

This topic describes how to launch Auto Scaling groups of [Bottlerocket](#) nodes that register with your Amazon EKS cluster. Bottlerocket is a Linux-based open-source operating system from AWS that you can use for running containers on virtual machines or bare metal hosts. After the nodes join the cluster, you can deploy Kubernetes applications to them. For more information about Bottlerocket, see [Using a Bottlerocket AMI with Amazon EKS](#) on GitHub and [Custom AMI support](#) in the eksctl documentation.

For information about in-place upgrades, see [Bottlerocket Update Operator](#) on GitHub.

Important

- Amazon EKS nodes are standard Amazon EC2 instances, and you are billed for them based on normal Amazon EC2 instance prices. For more information, see [Amazon EC2 pricing](#).
- You can launch Bottlerocket nodes in Amazon EKS extended clusters on AWS Outposts, but you can't launch them in local clusters on AWS Outposts. For more information, see [Amazon EKS on AWS Outposts \(p. 588\)](#).

- You can deploy to Amazon EC2 instances with x86 or Arm processors. However, you can't deploy to instances that have Inferentia chips.
- Bottlerocket is compatible with AWS CloudFormation. However, there is no official CloudFormation template that can be copied to deploy Bottlerocket nodes for Amazon EKS.
- Bottlerocket images don't come with an SSH server or a shell. You can use out-of-band access methods to allow SSH enabling the admin container and to pass some bootstrapping configuration steps with user data. For more information, see these sections in the [bottlerocket README.md](#) on GitHub:
 - [Exploration](#)
 - [Admin container](#)
 - [Kubernetes settings](#)

To launch Bottlerocket nodes using eksctl

This procedure requires eksctl version `0.160.0` or later. You can check your version with the following command:

```
eksctl version
```

For instructions on how to install or upgrade eksctl, see [Installing or updating eksctl \(p. 13\)](#).

Note

This procedure only works for clusters that were created with eksctl.

1. Copy the following contents to your device. Replace `my-cluster` with the name of your cluster. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters. Replace `ng-bottlerocket` with a name for your node group. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters. To deploy on Arm instances, replace `m5.large` with an Arm instance type. Replace `my-ec2-keypair-name` with the name of an Amazon EC2 SSH key pair that you can use to connect using SSH into your nodes with after they launch. If you don't already have an Amazon EC2 key pair, you can create one in the AWS Management Console. For more information, see [Amazon EC2 key pairs](#) in the [Amazon EC2 User Guide for Linux Instances](#). Replace all remaining `example values` with your own values. Once you've made the replacements, run the modified command to create the `bottlerocket.yaml` file.

If specifying an Arm Amazon EC2 instance type, then review the considerations in [Amazon EKS optimized Arm Amazon Linux AMIs \(p. 160\)](#) before deploying. For instructions on how to deploy using a custom AMI, see [Building Bottlerocket](#) on GitHub and [Custom AMI support](#) in the eksctl documentation. To deploy a managed node group, deploy a custom AMI using a launch template. For more information, see [Customizing managed nodes with launch templates \(p. 98\)](#).

Important

To deploy a node group to AWS Outposts, AWS Wavelength, or AWS Local Zone subnets, don't pass AWS Outposts, AWS Wavelength, or AWS Local Zone subnets when you create the cluster. You must specify the subnets in the following example. For more information see [Create a nodegroup from a config file](#) and [Config file schema](#) in the eksctl documentation. Replace `region-code` with the AWS Region that your cluster is in.

```
cat >bottlerocket.yaml <<EOF
---
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
```

```

name: my-cluster
region: region-code
version: '1.28'

iam:
  withOIDC: true

nodeGroups:
  - name: ng-bottlerocket
    instanceType: m5.large
    desiredCapacity: 3
    amiFamily: Bottlerocket
    ami: auto-ssm
    iam:
      attachPolicyARNs:
        - arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
        - arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
        - arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
    ssh:
      allow: true
      publicKeyName: my-ec2-keypair-name
EOF

```

2. Deploy your nodes with the following command.

```
eksctl create nodegroup --config-file=bottlerocket.yaml
```

An example output is as follows.

Several lines are output while the nodes are created. One of the last lines of output is the following example line.

```
[#] created 1 nodegroup(s) in cluster "my-cluster"
```

3. (Optional) Create a Kubernetes [persistent volume](#) on a Bottlerocket node using the [Amazon EBS CSI Plugin](#). The default Amazon EBS driver relies on file system tools that aren't included with Bottlerocket. For more information about creating a storage class using the driver, see [Amazon EBS CSI driver \(p. 228\)](#).
4. (Optional) By default, kube-proxy sets the `nf_conntrack_max` kernel parameter to a default value that may differ from what Bottlerocket originally sets at boot. To keep Bottlerocket's [default setting](#), edit the `kube-proxy` configuration with the following command.

```
kubectl edit -n kube-system daemonset kube-proxy
```

Add `--conntrack-max-per-core` and `--conntrack-min` to the `kube-proxy` arguments that are in the following example. A setting of `0` implies no change.

```

containers:
  - command:
    - kube-proxy
    - --v=2
    - --config=/var/lib/kube-proxy-config/config
    - --conntrack-max-per-core=0
    - --conntrack-min=0

```

5. (Optional) Deploy a [sample application \(p. 356\)](#) to test your Bottlerocket nodes.
6. We recommend blocking Pod access to IMDS if the following conditions are true:

- You plan to assign IAM roles to all of your Kubernetes service accounts so that Pods only have the minimum permissions that they need.
- No Pods in the cluster require access to the Amazon EC2 instance metadata service (IMDS) for other reasons, such as retrieving the current AWS Region.

For more information, see [Restrict access to the instance profile assigned to the worker node](#).

Launching self-managed Windows nodes

This topic describes how to launch Auto Scaling groups of Windows nodes that register with your Amazon EKS cluster. After the nodes join the cluster, you can deploy Kubernetes applications to them.

Important

- Amazon EKS nodes are standard Amazon EC2 instances, and you are billed for them based on normal Amazon EC2 instance prices. For more information, see [Amazon EC2 pricing](#).
- You can launch Windows nodes in Amazon EKS extended clusters on AWS Outposts, but you can't launch them in local clusters on AWS Outposts. For more information, see [Amazon EKS on AWS Outposts \(p. 588\)](#).

Enable Windows support for your cluster. We recommend that you review important considerations before you launch a Windows node group. For more information, see [Enabling Windows support \(p. 50\)](#).

You can launch self-managed Windows nodes with `eksctl` or the AWS Management Console.

`eksctl`

To launch self-managed Windows nodes using `eksctl`

This procedure requires that you have installed `eksctl`, and that your `eksctl` version is at least `0.160.0`. You can check your version with the following command.

```
eksctl version
```

For instructions on how to install or upgrade `eksctl`, see [Installing or updating eksctl \(p. 13\)](#).

Note

This procedure only works for clusters that were created with `eksctl`.

1. (Optional) If the `AmazonEKS_CNI_Policy` managed IAM policy (if you have an IPv4 cluster) or the `AmazonEKS_CNI_IPv6_Policy` (that you [created yourself \(p. 276\)](#) if you have an IPv6 cluster) is attached to your [the section called "Node IAM role" \(p. 501\)](#), we recommend assigning it to an IAM role that you associate to the Kubernetes aws-node service account instead. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).
2. This procedure assumes that you have an existing cluster. If you don't already have an Amazon EKS cluster and an Amazon Linux 2 node group to add a Windows node group to, we recommend that you follow the [Getting started with Amazon EKS – eksctl \(p. 13\)](#) guide. The guide provides a complete walkthrough for how to create an Amazon EKS cluster with Amazon Linux nodes.

Create your node group with the following command. Replace `region-code` with the AWS Region that your cluster is in. Replace `my-cluster` with your cluster name. The name can

contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters. Replace `ng-windows` with a name for your node group. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters. For Kubernetes version 1.23 or later, you can replace `2019` with `2022` to use Windows Server 2022. Replace the rest of the *example values* with your own values.

Important

To deploy a node group to AWS Outposts, AWS Wavelength, or AWS Local Zone subnets, don't pass the AWS Outposts, Wavelength, or Local Zone subnets when you create the cluster. Create the node group with a config file, specifying the AWS Outposts, Wavelength, or Local Zone subnets. For more information, see [Create a nodegroup from a config file](#) and [Config file schema](#) in the eksctl documentation.

Note

Amazon EKS optimized Windows AMIs can be configured to use `containerd` as a runtime. When using eksctl for launching Windows nodes, specify `containerRuntime` as `containerd` in the node group configuration. For more information, see [Enable the containerd runtime bootstrap flag \(p. 186\)](#) in this user guide or [Define container runtime](#) in the eksctl documentation.

```
eksctl create nodegroup \
--region region-code \
--cluster my-cluster \
--name ng-windows \
--node-type t2.large \
--nodes 3 \
--nodes-min 1 \
--nodes-max 4 \
--managed=false \
--node-ami-family WindowsServer2019FullContainer
```

Note

- If nodes fail to join the cluster, see [Nodes fail to join cluster \(p. 562\)](#) in the Troubleshooting guide.
- To see the available options for eksctl commands, enter the following command.

```
eksctl command -help
```

An example output is as follows. Several lines are output while the nodes are created. One of the last lines of output is the following example line.

```
[#] created 1 nodegroup(s) in cluster "my-cluster"
```

3. (Optional) Deploy a [sample application \(p. 356\)](#) to test your cluster and Windows nodes.
4. We recommend blocking Pod access to IMDS if the following conditions are true:
 - You plan to assign IAM roles to all of your Kubernetes service accounts so that Pods only have the minimum permissions that they need.
 - No Pods in the cluster require access to the Amazon EC2 instance metadata service (IMDS) for other reasons, such as retrieving the current AWS Region.

For more information, see [Restrict access to the instance profile assigned to the worker node](#).

AWS Management Console

Prerequisites

- An existing Amazon EKS cluster and a Linux node group. If you don't have these resources, we recommend that you follow one of our [Getting started with Amazon EKS \(p. 6\)](#) guides to create them. The guides describe how to create an Amazon EKS cluster with Linux nodes.
- An existing VPC and security group that meet the requirements for an Amazon EKS cluster. For more information, see [Amazon EKS VPC and subnet requirements and considerations \(p. 256\)](#) and [Amazon EKS security group requirements and considerations \(p. 263\)](#). The [Getting started with Amazon EKS \(p. 6\)](#) guide creates a VPC that meets the requirements. Alternatively, you can also follow [Creating a VPC for your Amazon EKS cluster \(p. 259\)](#) to create one manually.
- An existing Amazon EKS cluster that uses a VPC and security group that meets the requirements of an Amazon EKS cluster. For more information, see [Creating an Amazon EKS cluster \(p. 25\)](#). If you have subnets in the AWS Region where you have AWS Outposts, AWS Wavelength, or AWS Local Zones enabled, those subnets must not have been passed in when you created the cluster.

Step 1: To launch self-managed Windows nodes using the AWS Management Console

1. Wait for your cluster status to show as ACTIVE. If you launch your nodes before the cluster is active, the nodes fail to register with the cluster and you need to relaunch them.
2. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>
3. Choose **Create stack**.
4. For **Specify template**, select **Amazon S3 URL**.
5. Copy the following URL and paste it into **Amazon S3 URL**.

```
https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2023-02-09/amazon-eks-windows-nodegroup.yaml
```

6. Select **Next** twice.
7. On the **Quick create stack** page, enter the following parameters accordingly:
 - **Stack name:** Choose a stack name for your AWS CloudFormation stack. For example, you can call it **my-cluster-nodes**.
 - **ClusterName:** Enter the name that you used when you created your Amazon EKS cluster.

Important

This name must exactly match the name that you used in [Step 1: Create your Amazon EKS cluster \(p. 17\)](#). Otherwise, your nodes can't join the cluster.

- **ClusterControlPlaneSecurityGroup:** Choose the security group from the AWS CloudFormation output that you generated when you created your [VPC \(p. 259\)](#).

The following steps show one method to retrieve the applicable group.

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
 2. Choose the name of the cluster.
 3. Choose the **Networking** tab.
 4. Use the **Additional security groups** value as a reference when selecting from the **ClusterControlPlaneSecurityGroup** dropdown list.
- **NodeGroupName:** Enter a name for your node group. This name can be used later to identify the Auto Scaling node group that's created for your nodes. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters.
 - **NodeAutoScalingGroupMinSize:** Enter the minimum number of nodes that your node Auto Scaling group can scale in to.

- **NodeAutoScalingGroupDesiredCapacity:** Enter the desired number of nodes to scale to when your stack is created.
- **NodeAutoScalingGroupMaxSize:** Enter the maximum number of nodes that your node Auto Scaling group can scale out to.
- **NodeInstanceType:** Choose an instance type for your nodes. For more information, see [Choosing an Amazon EC2 instance type \(p. 152\)](#).

Note

The supported instance types for the latest version of the [Amazon VPC CNI plugin for Kubernetes](#) are listed in [vpc_ip_resource_limit.go](#) on GitHub. You might need to update your CNI version to use the latest supported instance types. For more information, see [the section called “Amazon VPC CNI plugin for Kubernetes” \(p. 266\)](#).

- **NodeImageIdSSMParam:** Pre-populated with the Amazon EC2 Systems Manager parameter of the current recommended Amazon EKS optimized Windows Core AMI ID. To use the full version of Windows, replace **Core** with **Full**.
- **NodeImageId:** (Optional) If you're using your own custom AMI (instead of the Amazon EKS optimized AMI), enter a node AMI ID for your AWS Region. If you specify a value for this field, it overrides any values in the **NodeImageIdSSMParam** field.
- **NodeVolumeSize:** Specify a root volume size for your nodes, in GiB.
- **KeyName:** Enter the name of an Amazon EC2 SSH key pair that you can use to connect using SSH into your nodes with after they launch. If you don't already have an Amazon EC2 key pair, you can create one in the AWS Management Console. For more information, see [Amazon EC2 key pairs](#) in the *Amazon EC2 User Guide for Windows Instances*.

Note

If you don't provide a key pair here, the AWS CloudFormation stack fails to be created.

- **BootstrapArguments:** Specify any optional arguments to pass to the node bootstrap script, such as extra kubelet arguments using `-KubeletExtraArgs`.

Note

You can configure Amazon EKS optimized Windows AMIs to use `containerd` as a runtime. When using an AWS CloudFormation template to create Windows nodes, specify `-ContainerRuntime containerd` in a bootstrap argument to enable the `containerd` runtime. For more information, see [Enable the containerd runtime bootstrap flag \(p. 186\)](#).

- **DisableIMDSv1:** By default, each node supports the Instance Metadata Service Version 1 (IMDSv1) and IMDSv2. You can disable IMDSv1. To prevent future nodes and Pods in the node group from using IMDSv1, set **DisableIMDSv1** to **true**. For more information about IMDS, see [Configuring the instance metadata service](#).
- **VpcId:** Select the ID for the [VPC \(p. 259\)](#) that you created.
- **NodeSecurityGroups:** Select the security group that was created for your Linux node group when you created your [VPC \(p. 259\)](#). If your Linux nodes have more than one security group attached to them, specify all of them. This for, for example, if the Linux node group was created with `eksctl`.
- **Subnets:** Choose the subnets that you created. If you created your VPC using the steps in [Creating a VPC for your Amazon EKS cluster \(p. 259\)](#), then specify only the private subnets within the VPC for your nodes to launch into.

Important

- If any of the subnets are public subnets, then they must have the automatic public IP address assignment setting enabled. If the setting isn't enabled for the public subnet, then any nodes that you deploy to that public subnet won't be assigned a public IP address and won't be able to communicate with the cluster or other AWS services. If the subnet was deployed before March 26, 2020 using either of the

[Amazon EKS AWS CloudFormation VPC templates \(p. 259\)](#), or by using `eksctl`, then automatic public IP address assignment is disabled for public subnets. For information about how to enable public IP address assignment for a subnet, see [Modifying the public IPv4 addressing attribute for your subnet](#). If the node is deployed to a private subnet, then it's able to communicate with the cluster and other AWS services through a NAT gateway.

- If the subnets don't have internet access, then make sure that you're aware of the considerations and extra steps in [Private cluster requirements \(p. 58\)](#).
 - If you select AWS Outposts, Wavelength, or Local Zone subnets, then the subnets must not have been passed in when you created the cluster.
8. Acknowledge that the stack might create IAM resources, and then choose **Create stack**.
 9. When your stack has finished creating, select it in the console and choose **Outputs**.
 10. Record the **NodeInstanceRole** for the node group that was created. You need this when you configure your Amazon EKS Windows nodes.

Step 2: To enable nodes to join your cluster

1. Check to see if you already have an aws-auth ConfigMap.

```
kubectl describe configmap -n kube-system aws-auth
```

2. If you are shown an aws-auth ConfigMap, then update it as needed.
 - a. Open the ConfigMap for editing.

```
kubectl edit -n kube-system configmap/aws-auth
```

- b. Add new mapRoles entries as needed. Set the rolearn values to the **NodeInstanceRole** values that you recorded in the previous procedures.

```
[...]
data:
  mapRoles: |
    - rolearn: <ARN of linux instance role (not instance profile)>
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
    - rolearn: <ARN of windows instance role (not instance profile)>
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
        - eks:kube-proxy-windows
[...]
```

- c. Save the file and exit your text editor.
3. If you received an error stating "Error from server (NotFound): configmaps "aws-auth" not found, then apply the stock ConfigMap.

- a. Download the configuration map.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/aws-auth-cm-windows.yaml
```

- b. In the `aws-auth-cm-windows.yaml` file, set the `rolearn` values to the applicable **NodeInstanceRole** values that you recorded in the previous procedures. You can do

this with a text editor, or by replacing the *example values* and running the following command:

```
sed -i.bak -e 's|<ARN of linux instance role (not instance profile)>|my-node-linux-instance-role|' \
-e 's|<ARN of windows instance role (not instance profile)>|my-node-windows-instance-role' aws-auth-cm-windows.yaml
```

Important

- Don't modify any other lines in this file.
 - Don't use the same IAM role for both Windows and Linux nodes.
- c. Apply the configuration. This command might take a few minutes to finish.

```
kubectl apply -f aws-auth-cm-windows.yaml
```

4. Watch the status of your nodes and wait for them to reach the Ready status.

```
kubectl get nodes --watch
```

Enter **Ctrl+C** to return to a shell prompt.

Note

If you receive any authorization or resource type errors, see [Unauthorized or access denied \(kubectl\) \(p. 563\)](#) in the troubleshooting topic.

If nodes fail to join the cluster, then see [Nodes fail to join cluster \(p. 562\)](#) in the Troubleshooting guide.

Step 3: Additional actions

1. (Optional) Deploy a [sample application \(p. 356\)](#) to test your cluster and Windows nodes.
2. (Optional) If the [AmazonEKS_CNI_Policy](#) managed IAM policy (if you have an IPv4 cluster) or the [AmazonEKS_CNI_IPv6_Policy](#) (that you [created yourself \(p. 276\)](#) if you have an IPv6 cluster) is attached to your [the section called "Node IAM role" \(p. 501\)](#), we recommend assigning it to an IAM role that you associate to the Kubernetes aws-node service account instead. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).
3. We recommend blocking Pod access to IMDS if the following conditions are true:
 - You plan to assign IAM roles to all of your Kubernetes service accounts so that Pods only have the minimum permissions that they need.
 - No Pods in the cluster require access to the Amazon EC2 instance metadata service (IMDS) for other reasons, such as retrieving the current AWS Region.

For more information, see [Restrict access to the instance profile assigned to the worker node](#).

Self-managed node updates

When a new Amazon EKS optimized AMI is released, consider replacing the nodes in your self-managed node group with the new AMI. Likewise, if you have updated the Kubernetes version for your Amazon EKS cluster, update the nodes to use nodes with the same Kubernetes version.

Important

This topic covers node updates for self-managed nodes. If you are using [Managed node groups \(p. 81\)](#), see [Updating a managed node group \(p. 91\)](#).

There are two basic ways to update self-managed node groups in your clusters to use a new AMI:

[**Migrating to a new node group \(p. 123\)**](#)

Create a new node group and migrate your Pods to that group. Migrating to a new node group is more graceful than simply updating the AMI ID in an existing AWS CloudFormation stack. This is because the migration process [taints](#) the old node group as NoSchedule and drains the nodes after a new stack is ready to accept the existing Pod workload.

[**Updating an existing self-managed node group \(p. 128\)**](#)

Update the AWS CloudFormation stack for an existing node group to use the new AMI. This method isn't supported for node groups that were created with eksctl.

Migrating to a new node group

This topic describes how you can create a new node group, gracefully migrate your existing applications to the new group, and remove the old node group from your cluster. You can migrate to a new node group using eksctl or the AWS Management Console.

eksctl

To migrate your applications to a new node group with eksctl

For more information on using eksctl for migration, see [Unmanaged nodegroup upgrades](#) in the eksctl documentation.

This procedure requires eksctl version `0.160.0` or later. You can check your version with the following command:

```
eksctl version
```

For instructions on how to install or upgrade eksctl, see [Installing or updating eksctl \(p. 13\)](#).

Note

This procedure only works for clusters and node groups that were created with eksctl.

1. Retrieve the name of your existing node groups, replacing `my-cluster` with your cluster name.

```
eksctl get nodegroups --cluster=my-cluster
```

An example output is as follows.

CLUSTER	NODEGROUP	CREATED	MIN SIZE	MAX SIZE
DESIRED CAPACITY	INSTANCE TYPE	IMAGE ID		
default	standard-nodes	2019-05-01T22:26:58Z	1	4
	t3.medium	ami-05a71d034119ffc12		3

2. Launch a new node group with eksctl with the following command. In the command, replace every `example value` with your own values. The version number can't be later than the Kubernetes version for your control plane. Also, it can't be more than two minor versions earlier than the Kubernetes version for your control plane. We recommend that you use the same version as your control plane.

We recommend blocking Pod access to IMDS if the following conditions are true:

- You plan to assign IAM roles to all of your Kubernetes service accounts so that Pods only have the minimum permissions that they need.
- No Pods in the cluster require access to the Amazon EC2 instance metadata service (IMDS) for other reasons, such as retrieving the current AWS Region.

For more information, see [Restrict access to the instance profile assigned to the worker node](#).

To block Pod access to IMDS, add the `--disable-pod-imds` option to the following command.

Note

For more available flags and their descriptions, see <https://eksctl.io/>.

```
eksctl create nodegroup \
--cluster my-cluster \
--version 1.28 \
--name standard-nodes-new \
--node-type t3.medium \
--nodes 3 \
--nodes-min 1 \
--nodes-max 4 \
--managed=false
```

3. When the previous command completes, verify that all of your nodes have reached the Ready state with the following command:

```
kubectl get nodes
```

4. Delete the original node group with the following command. In the command, replace every *example value* with your cluster and node group names:

```
eksctl delete nodegroup --cluster my-cluster --name standard-nodes-old
```

AWS Management Console and AWS CLI

To migrate your applications to a new node group with the AWS Management Console and AWS CLI

1. Launch a new node group by following the steps that are outlined in [Launching self-managed Amazon Linux nodes \(p. 108\)](#).
2. When your stack has finished creating, select it in the console and choose **Outputs**.
3. Record the **NodeInstanceRole** for the node group that was created. You need this to add the new Amazon EKS nodes to your cluster.

Note

If you attached any additional IAM policies to your old node group IAM role, attach those same policies to your new node group IAM role to maintain that functionality on the new group. This applies to you if you added permissions for the Kubernetes [Cluster Autoscaler](#), for example.

4. Update the security groups for both node groups so that they can communicate with each other. For more information, see [Amazon EKS security group requirements and considerations \(p. 263\)](#).
 - a. Record the security group IDs for both node groups. This is shown as the **NodeSecurityGroup** value in the AWS CloudFormation stack outputs.

You can use the following AWS CLI commands to get the security group IDs from the stack names. In these commands, `oldNodes` is the AWS CloudFormation stack name for your older node stack, and `newNodes` is the name of the stack that you are migrating to. Replace every *example value* with your own values.

```
oldNodes="old_node_CFN_stack_name"  
newNodes="new_node_CFN_stack_name"  
  
oldSecGroup=$(aws cloudformation describe-stack-resources --stack-name  
$oldNodes \  
--query 'StackResources[?  
ResourceType==`AWS::EC2::SecurityGroup`].PhysicalResourceId' \  
--output text)  
newSecGroup=$(aws cloudformation describe-stack-resources --stack-name  
$newNodes \  
--query 'StackResources[?  
ResourceType==`AWS::EC2::SecurityGroup`].PhysicalResourceId' \  
--output text)
```

- b. Add ingress rules to each node security group so that they accept traffic from each other.

The following AWS CLI commands add inbound rules to each security group that allow all traffic on all protocols from the other security group. This configuration allows Pods in each node group to communicate with each other while you're migrating your workload to the new group.

```
aws ec2 authorize-security-group-ingress --group-id $oldSecGroup \  
--source-group $newSecGroup --protocol -1  
aws ec2 authorize-security-group-ingress --group-id $newSecGroup \  
--source-group $oldSecGroup --protocol -1
```

5. Edit the `aws-auth` configmap to map the new node instance role in RBAC.

```
kubectl edit configmap -n kube-system aws-auth
```

Add a new `mapRoles` entry for the new node group. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

```
apiVersion: v1  
data:  
  mapRoles: |  
    - rolearn: ARN of instance role (not instance profile)  
      username: system:node:{EC2PrivateDNSName}  
      groups:  
        - system:bootstrappers  
        - system:nodes>  
    - rolearn: arn:aws:iam::111122223333:role/nodes-1-16-NodeInstanceRole-U11V27W93CX5  
      username: system:node:{EC2PrivateDNSName}  
      groups:  
        - system:bootstrappers  
        - system:nodes
```

Replace the *ARN of instance role (not instance profile)* snippet with the `NodeInstanceRole` value that you recorded in a [previous step \(p. 124\)](#). Then, save and close the file to apply the updated configmap.

6. Watch the status of your nodes and wait for your new nodes to join your cluster and reach the Ready status.

```
kubectl get nodes --watch
```

7. (Optional) If you're using the Kubernetes [Cluster Autoscaler](#), scale the deployment down to zero (0) replicas to avoid conflicting scaling actions.

```
kubectl scale deployments/cluster-autoscaler --replicas=0 -n kube-system
```

8. Use the following command to taint each of the nodes that you want to remove with NoSchedule. This is so that new Pods aren't scheduled or rescheduled on the nodes that you're replacing. For more information, see [Taints and Tolerations](#) in the Kubernetes documentation.

```
kubectl taint nodes node_name key=value:NoSchedule
```

If you're upgrading your nodes to a new Kubernetes version, you can identify and taint all of the nodes of a particular Kubernetes version (in this case, 1.26) with the following code snippet. The version number can't be later than the Kubernetes version of your control plane. It also can't be more than two minor versions earlier than the Kubernetes version of your control plane. We recommend that you use the same version as your control plane.

```
K8S_VERSION=1.26
nodes=$(kubectl get nodes -o jsonpath=".items[?(@.status.nodeInfo.kubeletVersion==\"v$K8S_VERSION\").metadata.name}]")
for node in ${nodes[@]}
do
    echo "Tainting $node"
    kubectl taint nodes $node key=value:NoSchedule
done
```

9. Determine your cluster's DNS provider.

```
kubectl get deployments -l k8s-app=kube-dns -n kube-system
```

An example output is as follows. This cluster is using CoreDNS for DNS resolution, but your cluster can return kube-dns instead):

NAME	DESIRED	CURRENT	UP-TO-DATE	AVAILABLE	AGE
coredns	1	1	1	1	31m

10. If your current deployment is running fewer than two replicas, scale out the deployment to two replicas. Replace **coredns** with **kubedns** if your previous command output returned that instead.

```
kubectl scale deployments/coredns --replicas=2 -n kube-system
```

11. Drain each of the nodes that you want to remove from your cluster with the following command:

```
kubectl drain node_name --ignore-daemonsets --delete-local-data
```

If you're upgrading your nodes to a new Kubernetes version, identify and drain all of the nodes of a particular Kubernetes version (in this case, 1.26) with the following code snippet.

```
K8S_VERSION=1.26
```

```
nodes=$(kubectl get nodes -o jsonpath=".items[?(@.status.nodeInfo.kubeletVersion==\"v$K8S_VERSION\").metadata.name]")
for node in ${nodes[@]}
do
    echo "Draining $node"
    kubectl drain $node --ignore-daemonsets --delete-local-data
done
```

- After your old nodes finished draining, revoke the security group inbound rules you authorized earlier. Then, delete the AWS CloudFormation stack to terminate the instances.

Note

If you attached any additional IAM policies to your old node group IAM role, such as adding permissions for the Kubernetes [Cluster Autoscaler](#), detach those additional policies from the role before you can delete your AWS CloudFormation stack.

- Revoke the inbound rules that you created for your node security groups earlier. In these commands, `oldNodes` is the AWS CloudFormation stack name for your older node stack, and `newNodes` is the name of the stack that you are migrating to.

```
oldNodes="old_node_CFN_stack_name"
newNodes="new_node_CFN_stack_name"

oldSecGroup=$(aws cloudformation describe-stack-resources --stack-name
$oldNodes \
--query 'StackResources[?
ResourceType==`AWS::EC2::SecurityGroup`].PhysicalResourceId' \
--output text)
newSecGroup=$(aws cloudformation describe-stack-resources --stack-name
$newNodes \
--query 'StackResources[?
ResourceType==`AWS::EC2::SecurityGroup`].PhysicalResourceId' \
--output text)
aws ec2 revoke-security-group-ingress --group-id $oldSecGroup \
--source-group $newSecGroup --protocol -1
aws ec2 revoke-security-group-ingress --group-id $newSecGroup \
--source-group $oldSecGroup --protocol -1
```

- Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
- Select your old node stack.
- Choose **Delete**.
- In the **Delete stack** confirmation dialog box, choose **Delete stack**.

- Edit the aws-auth configmap to remove the old node instance role from RBAC.

```
kubectl edit configmap -n kube-system aws-auth
```

Delete the mapRoles entry for the old node group. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

```
apiVersion: v1
data:
  mapRoles: |
    - roleArn: arn:aws:iam::111122223333:role/nodes-1-16-NodeInstanceRole-W70725MZQFF8
      username: system:node:{EC2PrivateDNSName}
    groups:
      - system:bootstrappers
      - system:nodes
```

```
- rolearn: arn:aws:iam::111122223333:role/nodes-1-15-NodeInstanceRole-U11V27W93CX5
  username: system:node:{EC2PrivateDNSName}
  groups:
    - system:bootstrappers
    - system:nodes>
```

Save and close the file to apply the updated configmap.

14. (Optional) If you are using the Kubernetes [Cluster Autoscaler](#), scale the deployment back to one replica.

Note

You must also tag your new Auto Scaling group appropriately (for example, k8s.io/cluster-autoscaler/enabled,k8s.io/cluster-autoscaler/[my-cluster](#)) and update the command for your Cluster Autoscaler deployment to point to the newly tagged Auto Scaling group. For more information, see [Cluster Autoscaler on AWS](#).

```
kubectl scale deployments/cluster-autoscaler --replicas=1 -n kube-system
```

15. (Optional) Verify that you're using the latest version of the [Amazon VPC CNI plugin for Kubernetes](#). You might need to update your CNI version to use the latest supported instance types. For more information, see [the section called "Amazon VPC CNI plugin for Kubernetes" \(p. 266\)](#).

16. If your cluster is using kube-dns for DNS resolution (see [previous step \(p. 126\)](#)), scale in the kube-dns deployment to one replica.

```
kubectl scale deployments/kube-dns --replicas=1 -n kube-system
```

Updating an existing self-managed node group

This topic describes how you can update an existing AWS CloudFormation self-managed node stack with a new AMI. You can use this procedure to update your nodes to a new version of Kubernetes following a cluster update. Otherwise, you can update to the latest Amazon EKS optimized AMI for an existing Kubernetes version.

Important

This topic covers node updates for self-managed nodes. For information about using [Managed node groups \(p. 81\)](#), see [Updating a managed node group \(p. 91\)](#).

The latest default Amazon EKS node AWS CloudFormation template is configured to launch an instance with the new AMI into your cluster before removing an old one, one at a time. This configuration ensures that you always have your Auto Scaling group's desired count of active instances in your cluster during the rolling update.

Note

This method isn't supported for node groups that were created with eksctl. If you created your cluster or node group with eksctl, see [Migrating to a new node group \(p. 123\)](#).

To update an existing node group

1. Determine the DNS provider for your cluster.

```
kubectl get deployments -l k8s-app=kube-dns -n kube-system
```

An example output is as follows. This cluster is using CoreDNS for DNS resolution, but your cluster might return kube-dns instead. Your output might look different depending on the version of kubectl that you're using.

NAME	DESIRED	CURRENT	UP-TO-DATE	AVAILABLE	AGE
coredns	1	1	1	1	31m

- If your current deployment is running fewer than two replicas, scale out the deployment to two replicas. Replace **coredns** with **kube-dns** if your previous command output returned that instead.

```
kubectl scale deployments/coredns --replicas=2 -n kube-system
```

- (Optional) If you're using the Kubernetes [Cluster Autoscaler](#), scale the deployment down to zero (0) replicas to avoid conflicting scaling actions.

```
kubectl scale deployments/cluster-autoscaler --replicas=0 -n kube-system
```

- Determine the instance type and desired instance count of your current node group. You enter these values later when you update the AWS CloudFormation template for the group.
 - Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
 - In the left navigation pane, choose **Launch Configurations**, and note the instance type for your existing node launch configuration.
 - In the left navigation pane, choose **Auto Scaling Groups**, and note the **Desired** instance count for your existing node Auto Scaling group.
- Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
- Select your node group stack, and then choose **Update**.
- Select **Replace current template** and select **Amazon S3 URL**.
- For **Amazon S3 URL**, paste the following URL into the text area to ensure that you're using the latest version of the node AWS CloudFormation template. Then, choose **Next**:

```
https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2022-12-23/amazon-eks-nodegroup.yaml
```

- On the **Specify stack details** page, fill out the following parameters, and choose **Next**:
 - NodeAutoScalingGroupDesiredCapacity** – Enter the desired instance count that you recorded in a [previous step \(p. 129\)](#). Or, enter your new desired number of nodes to scale to when your stack is updated.
 - NodeAutoScalingGroupMaxSize** – Enter the maximum number of nodes to which your node Auto Scaling group can scale out. This value must be at least one node more than your desired capacity. This is so that you can perform a rolling update of your nodes without reducing your node count during the update.
 - NodeInstanceType** – Choose the instance type you recorded in a [previous step \(p. 129\)](#). Alternatively, choose a different instance type for your nodes. Before choosing a different instance type, review [Choosing an Amazon EC2 instance type \(p. 152\)](#). Each Amazon EC2 instance type supports a maximum number of elastic network interfaces (network interface) and each network interface supports a maximum number of IP addresses. Because each worker node and Pod is assigned its own IP address, it's important to choose an instance type that will support the maximum number of Pods that you want to run on each Amazon EC2 node. For a list of the number of network interfaces and IP addresses supported by instance types, see [IP addresses per network interface per instance type](#). For example, the m5.large instance type supports a maximum of 30 IP addresses for the worker node and Pods.

Note

The supported instance types for the latest version of the [Amazon VPC CNI plugin for Kubernetes](#) are shown in [vpc_ip_resource_limit.go](#) on GitHub. You might need to update your Amazon VPC CNI plugin for Kubernetes version to use the latest supported

instance types. For more information, see [the section called “Amazon VPC CNI plugin for Kubernetes” \(p. 266\)](#).

Important

Some instance types might not be available in all AWS Regions.

- **NodeImageIdSSMParam** – The Amazon EC2 Systems Manager parameter of the AMI ID that you want to update to. The following value uses the latest Amazon EKS optimized AMI for Kubernetes version 1.28.

```
/aws/service/eks/optimized-ami/1.28/amazon-linux-2/recommended/image_id
```

You can replace [1.28](#) with a [supported Kubernetes version \(p. 71\)](#) that's the same. Or, it should be up to one version earlier than the Kubernetes version running on your control plane. We recommend that you keep your nodes at the same version as your control plane. If you want to use the Amazon EKS optimized accelerated AMI, then replace [amazon-linux-2](#) with [amazon-linux-2-gpu](#).

Note

Using the Amazon EC2 Systems Manager parameter enables you to update your nodes in the future without having to look up and specify an AMI ID. If your AWS CloudFormation stack is using this value, any stack update always launches the latest recommended Amazon EKS optimized AMI for your specified Kubernetes version. This is even the case even if you don't change any values in the template.

- **NodeImageId** – To use your own custom AMI, enter the ID for the AMI to use.

Important

This value overrides any value specified for **NodeImageIdSSMParam**. If you want to use the **NodeImageIdSSMParam** value, ensure that the value for **NodeImageId** is blank.

- **DisableIMDSv1** – By default, each node supports the Instance Metadata Service Version 1 (IMDSv1) and IMDSv2. However, you can disable IMDSv1. Select **true** if you don't want any nodes or any Pods scheduled in the node group to use IMDSv1. For more information about IMDS, see [Configuring the instance metadata service](#). If you've implemented IAM roles for service accounts, assign necessary permissions directly to all Pods that require access to AWS services. This way, no Pods in your cluster require access to IMDS for other reasons, such as retrieving the current AWS Region. Then, you can also disable access to IMDSv2 for Pods that don't use host networking. For more information, see [Restrict access to the instance profile assigned to the worker node](#).

10. (Optional) On the **Options** page, tag your stack resources. Choose **Next**.

11. On the **Review** page, review your information, acknowledge that the stack might create IAM resources, and then choose **Update stack**.

Note

The update of each node in the cluster takes several minutes. Wait for the update of all nodes to complete before performing the next steps.

12. If your cluster's DNS provider is kube-dns, scale in the kube-dns deployment to one replica.

```
kubectl scale deployments/kube-dns --replicas=1 -n kube-system
```

13. (Optional) If you are using the Kubernetes [Cluster Autoscaler](#), scale the deployment back to your desired amount of replicas.

```
kubectl scale deployments/cluster-autoscaler --replicas=1 -n kube-system
```

14. (Optional) Verify that you're using the latest version of the [Amazon VPC CNI plugin for Kubernetes](#). You might need to update your Amazon VPC CNI plugin for Kubernetes version to use the latest supported instance types. For more information, see [the section called “Amazon VPC CNI plugin for Kubernetes” \(p. 266\)](#).

AWS Fargate

This topic discusses using Amazon EKS to run Kubernetes Pods on AWS Fargate. Fargate is a technology that provides on-demand, right-sized compute capacity for [containers](#). With Fargate, you don't have to provision, configure, or scale groups of virtual machines on your own to run containers. You also don't need to choose server types, decide when to scale your node groups, or optimize cluster packing. For more information, see [What is AWS Fargate?](#) in the *Amazon Elastic Container Service User Guide for AWS Fargate*.

You can control which Pods start on Fargate and how they run with [Fargate profiles \(p. 136\)](#). Fargate profiles are defined as part of your Amazon EKS cluster. Amazon EKS integrates Kubernetes with Fargate by using controllers that are built by AWS using the upstream, extensible model provided by Kubernetes. These controllers run as part of the Amazon EKS managed Kubernetes control plane and are responsible for scheduling native Kubernetes Pods onto Fargate. The Fargate controllers include a new scheduler that runs alongside the default Kubernetes scheduler in addition to several mutating and validating admission controllers. When you start a Pod that meets the criteria for running on Fargate, the Fargate controllers that are running in the cluster recognize, update, and schedule the Pod onto Fargate.

This topic describes the different components of Pods that run on Fargate, and calls out special considerations for using Fargate with Amazon EKS.

AWS Fargate considerations

Here are some things to consider about using Fargate on Amazon EKS.

- AWS Fargate with Amazon EKS isn't available in AWS GovCloud (US-East) and AWS GovCloud (US-West).
- Each Pod that runs on Fargate has its own isolation boundary. They don't share the underlying kernel, CPU resources, memory resources, or elastic network interface with another Pod.
- Network Load Balancers and Application Load Balancers (ALBs) can be used with Fargate with IP targets only. For more information, see [Create a network load balancer \(p. 371\)](#) and [Application load balancing on Amazon EKS \(p. 375\)](#).
- Fargate exposed services only run on target type IP mode, and not on node IP mode. The recommended way to check the connectivity from a service running on a managed node and a service running on Fargate is to connect via service name.
- Pods must match a Fargate profile at the time that they're scheduled to run on Fargate. Pods that don't match a Fargate profile might be stuck as Pending. If a matching Fargate profile exists, you can delete pending Pods that you have created to reschedule them onto Fargate.
- Daemonsets aren't supported on Fargate. If your application requires a daemon, reconfigure that daemon to run as a sidecar container in your Pods.
- Privileged containers aren't supported on Fargate.
- Pods running on Fargate can't specify HostPort or HostNetwork in the Pod manifest.
- The default nofile and nproc soft limit is 1024 and the hard limit is 65535 for Fargate Pods.
- GPUs aren't currently available on Fargate.
- Pods that run on Fargate are only supported on private subnets (with NAT gateway access to AWS services, but not a direct route to an Internet Gateway), so your cluster's VPC must have private subnets available. For clusters without outbound internet access, see [Private cluster requirements \(p. 58\)](#).
- You can use the [Vertical Pod Autoscaler \(p. 363\)](#) to set the initial correct size of CPU and memory for your Fargate Pods, and then use the [Horizontal Pod Autoscaler \(p. 367\)](#) to scale those Pods. If you want the Vertical Pod Autoscaler to automatically re-deploy Pods to Fargate with larger CPU and

memory combinations, set the mode for the Vertical Pod Autoscaler to either Auto or Recreate to ensure correct functionality. For more information, see the [Vertical Pod Autoscaler](#) documentation on GitHub.

- DNS resolution and DNS hostnames must be enabled for your VPC. For more information, see [Viewing and updating DNS support for your VPC](#).
- Amazon EKS Fargate adds defense-in-depth for Kubernetes applications by isolating each Pod within a Virtual Machine (VM). This VM boundary prevents access to host-based resources used by other Pods in the event of a container escape, which is a common method of attacking containerized applications and gain access to resources outside of the container.

Using Amazon EKS doesn't change your responsibilities under the [shared responsibility model \(p. 459\)](#). You should carefully consider the configuration of cluster security and governance controls. The safest way to isolate an application is always to run it in a separate cluster.

- Fargate profiles support specifying subnets from VPC secondary CIDR blocks. You might want to specify a secondary CIDR block. This is because there's a limited number of IP addresses available in a subnet. As a result, there's also a limited number of Pods that can be created in the cluster. By using different subnets for Pods, you can increase the number of available IP addresses. For more information, see [Adding IPv4 CIDR blocks to a VPC](#).
- The Amazon EC2 instance metadata service (IMDS) isn't available to Pods that are deployed to Fargate nodes. If you have Pods that are deployed to Fargate that need IAM credentials, assign them to your Pods using [IAM roles for service accounts \(p. 464\)](#). If your Pods need access to other information available through IMDS, then you must hard code this information into your Pod spec. This includes the AWS Region or Availability Zone that a Pod is deployed to.
- You can't deploy Fargate Pods to AWS Outposts, AWS Wavelength, or AWS Local Zones.
- Amazon EKS must periodically patch Fargate Pods to keep them secure. We attempt the updates in a way that reduces impact, but there are times when Pods must be deleted if they aren't successfully evicted. There are some actions you can take to minimize disruption. For more information, see [Fargate OS patching \(p. 142\)](#).
- The [Amazon VPC CNI plugin for Amazon EKS](#) is installed on Fargate nodes. You can't use [the section called "Alternate compatible CNI plugins" \(p. 332\)](#) with Fargate nodes.
- A Pod running on Fargate automatically mounts an Amazon EFS file system. You can't use dynamic persistent volume provisioning with Fargate nodes, but you can use static provisioning.
- You can't mount Amazon EBS volumes to Fargate Pods.
- You can run the Amazon EBS CSI controller on Fargate nodes, but the Amazon EBS CSI node DaemonSet can only run on Amazon EC2 instances.
- After a [Kubernetes Job](#) is marked Completed or Failed, the Pods that the Job creates normally continue to exist. This behavior allows you to view your logs and results, but with Fargate you will incur costs if you don't clean up the Job afterwards.

To automatically delete the related Pods after a Job completes or fails, you can specify a time period using the time-to-live (TTL) controller. The following example shows specifying `.spec.ttlSecondsAfterFinished` in your Job manifest.

```
apiVersion: batch/v1
kind: Job
metadata:
  name: busybox
spec:
  template:
    spec:
      containers:
      - name: busybox
        image: busybox
        command: ["/bin/sh", "-c", "sleep 10"]
  restartPolicy: Never
```

```
ttlSecondsAfterFinished: 60 # <-- TTL controller
```

Getting started with AWS Fargate using Amazon EKS

This topic describes how to get started running Pods on AWS Fargate with your Amazon EKS cluster.

If you restrict access to the public endpoint of your cluster using CIDR blocks, we recommend that you also enable private endpoint access. This way, Fargate Pods can communicate with the cluster. Without the private endpoint enabled, the CIDR blocks that you specify for public access must include the outbound sources from your VPC. For more information, see [Amazon EKS cluster endpoint access control \(p. 41\)](#).

Prerequisite

An existing cluster. AWS Fargate with Amazon EKS isn't available in AWS GovCloud (US-East) and AWS GovCloud (US-West). If you don't already have an Amazon EKS cluster, see [Getting started with Amazon EKS \(p. 6\)](#).

Ensure that existing nodes can communicate with Fargate Pods

If you're working with a new cluster with no nodes, or a cluster with only [managed node groups \(p. 81\)](#), you can skip to [Create a Fargate Pod execution role \(p. 133\)](#).

Assume that you're working with an existing cluster that already has nodes that are associated with it. Make sure that Pods on these nodes can communicate freely with the Pods that are running on Fargate. Pods that are running on Fargate are automatically configured to use the cluster security group for the cluster that they're associated with. Ensure that any existing nodes in your cluster can send and receive traffic to and from the cluster security group. [Managed node groups \(p. 81\)](#) are automatically configured to use the cluster security group as well, so you don't need to modify or check them for this compatibility.

For existing node groups that were created with `eksctl` or the Amazon EKS managed AWS CloudFormation templates, you can add the cluster security group to the nodes manually. Or, alternatively, you can modify the Auto Scaling group launch template for the node group to attach the cluster security group to the instances. For more information, see [Changing an instance's security groups](#) in the *Amazon VPC User Guide*.

You can check for a security group for your cluster in the AWS Management Console under the **Networking** section for the cluster. Or, you can do this using the following AWS CLI command. When using this command, replace `my-cluster` with the name of your cluster.

```
aws eks describe-cluster --name my-cluster --query
cluster.resourcesVpcConfig.clusterSecurityGroupId
```

Create a Fargate Pod execution role

When your cluster creates Pods on AWS Fargate, the components that run on the Fargate infrastructure must make calls to AWS APIs on your behalf. The Amazon EKS Pod execution role provides the IAM permissions to do this. To create an AWS Fargate Pod execution role, see [Amazon EKS Pod execution IAM role \(p. 504\)](#).

Note

If you created your cluster with `eksctl` using the `--fargate` option, your cluster already has a Pod execution role that you can find in the IAM console with the pattern `eksctl-my-cluster-FargatePodExecutionRole-ABCDEFGHIJKL`. Similarly, if you use `eksctl` to create your Fargate profiles, `eksctl` creates your Pod execution role if one isn't already created.

Create a Fargate profile for your cluster

Before you can schedule Pods that are running on Fargate in your cluster, you must define a Fargate profile that specifies which Pods use Fargate when they're launched. For more information, see [AWS Fargate profile \(p. 136\)](#).

Note

If you created your cluster with eksctl using the `--fargate` option, then a Fargate profile is already created for your cluster with selectors for all Pods in the `kube-system` and `default` namespaces. Use the following procedure to create Fargate profiles for any other namespaces you would like to use with Fargate.

You can create a Fargate profile using `eksctl` or the AWS Management Console.

`eksctl`

This procedure requires `eksctl` version `0.160.0` or later. You can check your version with the following command:

```
eksctl version
```

For instructions on how to install or upgrade `eksctl`, see [Installing or updating eksctl \(p. 13\)](#).

To create a Fargate profile with `eksctl`

Create your Fargate profile with the following `eksctl` command, replacing every *example value* with your own values. You're required to specify a namespace. However, the `--labels` option isn't required.

```
eksctl create fargateprofile \
    --cluster my-cluster \
    --name my-fargate-profile \
    --namespace my-kubernetes-namespace \
    --labels key=value
```

You can use certain wildcards for `my-kubernetes-namespace` and `key=value` labels. For more information, see [Fargate profile wildcards \(p. 137\)](#).

AWS Management Console

To create a Fargate profile for a cluster with the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose the cluster to create a Fargate profile for.
3. Choose the **Compute** tab.
4. Under **Fargate profiles**, choose **Add Fargate profile**.
5. On the **Configure Fargate profile** page, do the following:
 - a. For **Name**, enter a name for your Fargate profile. The name must be unique.
 - b. For **Pod execution role**, choose the Pod execution role to use with your Fargate profile. Only the IAM roles with the `eks-fargate-pods.amazonaws.com` service principal are shown. If you don't see any roles listed, you must create one. For more information, see [Amazon EKS Pod execution IAM role \(p. 504\)](#).
 - c. Choose the **Subnets** dropdown and deselect any subnet with `Public` in its name. Only private subnets are supported for Pods that are running on Fargate.
 - d. For **Tags**, you can optionally tag your Fargate profile. These tags don't propagate to other resources that are associated with the profile such as Pods.

- e. Choose **Next**.
6. On the **Configure Pod selection** page, do the following:
 - a. For **Namespace**, enter a namespace to match for Pods.
 - You can use specific namespaces to match, such as **kube-system** or **default**.
 - You can use certain wildcards (for example, **prod-***) to match multiple namespaces (for example, **prod-deployment** and **prod-test**). For more information, see [Fargate profile wildcards \(p. 137\)](#).
 - b. (Optional) Add Kubernetes labels to the selector. Specifically add them to the one that the Pods in the specified namespace need to match.
 - You can add the label **infrastructure: fargate** to the selector so that only Pods in the specified namespace that also have the **infrastructure: fargate** Kubernetes label match the selector.
 - You can use certain wildcards (for example, **key?: value?**) to match multiple namespaces (for example, **keya: valuea** and **keyb: valueb**). For more information, see [Fargate profile wildcards \(p. 137\)](#).
 - c. Choose **Next**.
7. On the **Review and create** page, review the information for your Fargate profile and choose **Create**.

Update CoreDNS

By default, CoreDNS is configured to run on Amazon EC2 infrastructure on Amazon EKS clusters. If you want to *only* run your Pods on Fargate in your cluster, complete the following steps.

Note

If you created your cluster with `eksctl` using the `--fargate` option, then you can skip to [Next steps \(p. 136\)](#).

1. Create a Fargate profile for CoreDNS with the following command. Replace `my-cluster` with your cluster name, `111122223333` with your account ID, `AmazonEKSFargatePodExecutionRole` with the name of your Pod execution role, and `0000000000000001`, `0000000000000002`, and `0000000000000003` with the IDs of your private subnets. If you don't have a Pod execution role, you must [create one \(p. 133\)](#) first. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

Important

The role ARN can't include a path. The format of the role ARN must be `arn:aws:iam::111122223333:role/role-name`. For more information, see [aws-auth ConfigMap does not grant access to the cluster \(p. 518\)](#).

```
aws eks create-fargate-profile \
--fargate-profile-name coredns \
--cluster-name my-cluster \
--pod-execution-role-arn
arn:aws:iam::111122223333:role/AmazonEKSFargatePodExecutionRole \
--selectors namespace=kube-system,labels={k8s-app=kube-dns} \
--subnets subnet-0000000000000001 subnet-0000000000000002 subnet-0000000000000003
```

2. Run the following command to remove the `eks.amazonaws.com/compute-type : ec2` annotation from the CoreDNS Pods.

```
kubectl patch deployment coredns \
-n kube-system \
--type json \
```

```
-p='[{"op": "remove", "path": "/spec/template/metadata/annotations/eks.amazonaws.com~1compute-type"}]'
```

Next steps

- You can start migrating your existing applications to run on Fargate with the following workflow.
 1. [Create a Fargate profile \(p. 138\)](#) that matches your application's Kubernetes namespace and Kubernetes labels.
 2. Delete and re-create any existing Pods so that they're scheduled on Fargate. For example, the following command triggers a rollout of the `coredns` deployment. You can modify the namespace and deployment type to update your specific Pods.

```
kubectl rollout restart -n kube-system deployment coredns
```

- Deploy the [Application load balancing on Amazon EKS \(p. 375\)](#) to allow Ingress objects for your Pods running on Fargate.
- You can use the [Vertical Pod Autoscaler \(p. 363\)](#) to set the initial correct size of CPU and memory for your Fargate Pods, and then use the [Horizontal Pod Autoscaler \(p. 367\)](#) to scale those Pods. If you want the Vertical Pod Autoscaler to automatically re-deploy Pods to Fargate with higher CPU and memory combinations, set the Vertical Pod Autoscaler's mode to either Auto or Recreate. This is to ensure correct functionality. For more information, see the [Vertical Pod Autoscaler](#) documentation on GitHub.
- You can set up the [AWS Distro for OpenTelemetry](#) (ADOT) collector for application monitoring by following [these instructions](#).

AWS Fargate profile

Before you schedule Pods on Fargate in your cluster, you must define at least one Fargate profile that specifies which Pods use Fargate when launched.

As an administrator, you can use a Fargate profile to declare which Pods run on Fargate. You can do this through the profile's selectors. You can add up to five selectors to each profile. Each selector must contain a namespace. The selector can also include labels. The label field consists of multiple optional key-value pairs. Pods that match a selector are scheduled on Fargate. Pods are matched using a namespace and the labels that are specified in the selector. If a namespace selector is defined without labels, Amazon EKS attempts to schedule all the Pods that run in that namespace onto Fargate using the profile. If a to-be-scheduled Pod matches any of the selectors in the Fargate profile, then that Pod is scheduled on Fargate.

If a Pod matches multiple Fargate profiles, you can specify which profile a Pod uses by adding the following Kubernetes label to the Pod specification: `eks.amazonaws.com/fargate-profile: my-fargate-profile`. The Pod must match a selector in that profile to be scheduled onto Fargate. Kubernetes affinity/anti-affinity rules do not apply and aren't necessary with Amazon EKS Fargate Pods.

When you create a Fargate profile, you must specify a Pod execution role. This execution role is for the Amazon EKS components that run on the Fargate infrastructure using the profile. It's added to the cluster's Kubernetes [Role Based Access Control](#) (RBAC) for authorization. That way, the `kubelet` that runs on the Fargate infrastructure can register with your Amazon EKS cluster and appear in your cluster as a node. The Pod execution role also provides IAM permissions to the Fargate infrastructure to allow read access to Amazon ECR image repositories. For more information, see [Amazon EKS Pod execution IAM role \(p. 504\)](#).

Fargate profiles can't be changed. However, you can create a new updated profile to replace an existing profile, and then delete the original.

Note

Any Pods that are running using a Fargate profile are stopped and put into a pending state when the profile is deleted.

If any Fargate profiles in a cluster are in the DELETING status, you must wait until after the Fargate profile is deleted before you create other profiles in that cluster.

Amazon EKS and Fargate spread Pods across each of the subnets that's defined in the Fargate profile. However, you might end up with an uneven spread. If you must have an even spread, use two Fargate profiles. Even spread is important in scenarios where you want to deploy two replicas and don't want any downtime. We recommend that each profile has only one subnet.

Fargate profile components

The following components are contained in a Fargate profile.

Pod execution role

When your cluster creates Pods on AWS Fargate, the kubelet that's running on the Fargate infrastructure must make calls to AWS APIs on your behalf. For example, it needs to make calls to pull container images from Amazon ECR. The Amazon EKS Pod execution role provides the IAM permissions to do this.

When you create a Fargate profile, you must specify a Pod execution role to use with your Pods. This role is added to the cluster's Kubernetes [Role-based access control](#) (RBAC) for authorization. This is so that the kubelet that's running on the Fargate infrastructure can register with your Amazon EKS cluster and appear in your cluster as a node. For more information, see [Amazon EKS Pod execution IAM role \(p. 504\)](#).

Subnets

The IDs of subnets to launch Pods into that use this profile. At this time, Pods that are running on Fargate aren't assigned public IP addresses. Therefore, only private subnets with no direct route to an Internet Gateway are accepted for this parameter.

Selectors

The selectors to match for Pods to use this Fargate profile. You might specify up to five selectors in a Fargate profile. The selectors have the following components:

- **Namespace** – You must specify a namespace for a selector. The selector only matches Pods that are created in this namespace. However, you can create multiple selectors to target multiple namespaces.
- **Labels** – You can optionally specify Kubernetes labels to match for the selector. The selector only matches Pods that have all of the labels that are specified in the selector.

Fargate profile wildcards

In addition to characters allowed by Kubernetes, you're allowed to use * and ? in the selector criteria for namespaces, label keys, and label values:

- * represents none, one, or multiple characters. For example, **prod*** can represent prod and prod-metrics.
- ? represents a single character (for example, **value?** can represent valuea). However, it can't represent value and value-a, because ? can only represent exactly one character.

These wildcard characters can be used in any position and in combination (for example, **prod***, ***dev**, and **frontend*?**). Other wildcards and forms of pattern matching, such as regular expressions, aren't supported.

If there are multiple matching profiles for the namespace and labels in the Pod spec, Fargate picks up the profile based on alphanumeric sorting by profile name. For example, if both profile A (with the name `beta-workload`) and profile B (with the name `prod-workload`) have matching selectors for the Pods to be launched, Fargate picks profile A (`beta-workload`) for the Pods. The Pods have labels with profile A on the Pods (for example, `eks.amazonaws.com/fargate-profile=beta-workload`).

If you want to migrate existing Fargate Pods to new profiles that use wildcards, there are two ways to do so:

- Create a new profile with matching selectors, then delete the old profiles. Pods labeled with old profiles are rescheduled to new matching profiles.
- If you want to migrate workloads but aren't sure what Fargate labels are on each Fargate Pod, you can use the following method. Create a new profile with a name that sorts alphabetically first among the profiles on the same cluster. Then, recycle the Fargate Pods that need to be migrated to new profiles.

Creating a Fargate profile

This topic describes how to create a Fargate profile. AWS Fargate with Amazon EKS isn't available in AWS GovCloud (US-East) and AWS GovCloud (US-West). You also must have created a Pod execution role to use for your Fargate profile. For more information, see [Amazon EKS Pod execution IAM role \(p. 504\)](#). Pods that are running on Fargate are only supported on private subnets with [NAT gateway](#) access to AWS services, but not a direct route to an Internet Gateway. This is so that your cluster's VPC must have private subnets available. You can create a profile with `eksctl` or the AWS Management Console.

This procedure requires `eksctl` version `0.160.0` or later. You can check your version with the following command:

```
eksctl version
```

For instructions on how to install or upgrade `eksctl`, see [Installing or updating eksctl \(p. 13\)](#).

`eksctl`

To create a Fargate profile with `eksctl`

Create your Fargate profile with the following `eksctl` command, replacing every *example value* with your own values. You're required to specify a namespace. However, the `--labels` option isn't required.

```
eksctl create fargateprofile \
--cluster my-cluster \
--name my-fargate-profile \
--namespace my-kubernetes-namespace \
--labels key=value
```

You can use certain wildcards for `my-kubernetes-namespace` and `key=value` labels. For more information, see [Fargate profile wildcards \(p. 137\)](#).

AWS Management Console

To create a Fargate profile for a cluster with the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose the cluster to create a Fargate profile for.
3. Choose the **Compute** tab.

4. Under **Fargate profiles**, choose **Add Fargate profile**.
5. On the **Configure Fargate profile** page, do the following:
 - a. For **Name**, enter a unique name for your Fargate profile, such as **my-profile**.
 - b. For **Pod execution role**, choose the Pod execution role to use with your Fargate profile. Only the IAM roles with the `eks-fargate-pods.amazonaws.com` service principal are shown. If you don't see any roles listed, you must create one. For more information, see [Amazon EKS Pod execution IAM role \(p. 504\)](#).
 - c. Choose the **Subnets** dropdown and deselect any subnet with **Public** in its name. Only private subnets are supported for Pods that are running on Fargate.
 - d. For **Tags**, you can optionally tag your Fargate profile. These tags don't propagate to other resources that are associated with the profile, such as Pods.
 - e. Choose **Next**.
6. On the **Configure Pod selection** page, do the following:
 - a. For **Namespace**, enter a namespace to match for Pods.
 - You can use specific namespaces to match, such as **kube-system** or **default**.
 - You can use certain wildcards (for example, **prod-***) to match multiple namespaces (for example, **prod-deployment** and **prod-test**). For more information, see [Fargate profile wildcards \(p. 137\)](#).
 - b. (Optional) Add Kubernetes labels to the selector. Specifically, add them to the one that the Pods in the specified namespace need to match.
 - You can add the label **infrastructure: fargate** to the selector so that only Pods in the specified namespace that also have the **infrastructure: fargate** Kubernetes label match the selector.
 - You can use certain wildcards (for example, **key?: value?**) to match multiple namespaces (for example, **keya: valuea** and **keyb: valueb**). For more information, see [Fargate profile wildcards \(p. 137\)](#).
 - c. Choose **Next**.
7. On the **Review and create** page, review the information for your Fargate profile and choose **Create**.

Deleting a Fargate profile

This topic describes how to delete a Fargate profile.

When you delete a Fargate profile, any Pods that were scheduled onto Fargate with the profile are deleted. If those Pods match another Fargate profile, then they're scheduled on Fargate with that profile. If they no longer match any Fargate profiles, then they aren't scheduled onto Fargate and might remain as pending.

Only one Fargate profile in a cluster can be in the **DELETING** status at a time. Wait for a Fargate profile to finish deleting before you can delete any other profiles in that cluster.

You can delete a profile with `eksctl`, the AWS Management Console, or the AWS CLI. Select the tab with the name of the tool that you want to use to delete your profile.

`eksctl`

To delete a Fargate profile with `eksctl`

Use the following command to delete a profile from a cluster. Replace every **example value** with your own values.

```
eksctl delete fargateprofile --name my-profile --cluster my-cluster
```

AWS Management Console

To delete a Fargate profile from a cluster with the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, choose **Clusters**. In the list of clusters, choose the cluster that you want to delete the Fargate profile from.
3. Choose the **Compute** tab.
4. Choose the Fargate profile to delete, and then choose **Delete**.
5. On the **Delete Fargate profile** page, enter the name of the profile, and then choose **Delete**.

AWS CLI

To delete a Fargate profile with AWS CLI

Use the following command to delete a profile from a cluster. Replace every *example value* with your own values.

```
aws eks delete-fargate-profile --fargate-profile-name my-profile --cluster-name my-cluster
```

Fargate Pod configuration

This section describes some of the unique Pod configuration details for running Kubernetes Pods on AWS Fargate.

Pod CPU and memory

With Kubernetes, you can define requests, a minimum vCPU amount, and memory resources that are allocated to each container in a Pod. Pods are scheduled by Kubernetes to ensure that at least the requested resources for each Pod are available on the compute resource. For more information, see [Managing compute resources for containers](#) in the Kubernetes documentation.

Note

Since Amazon EKS Fargate runs only one Pod per node, the scenario of evicting Pods in case of fewer resources doesn't occur. All Amazon EKS Fargate Pods run with guaranteed priority, so the requested CPU and memory must be equal to the limit for all of the containers. For more information, see [Configure Quality of Service for Pods](#) in the Kubernetes documentation.

When Pods are scheduled on Fargate, the vCPU and memory reservations within the Pod specification determine how much CPU and memory to provision for the Pod.

- The maximum request out of any Init containers is used to determine the Init request vCPU and memory requirements.
- Requests for all long-running containers are added up to determine the long-running request vCPU and memory requirements.
- The larger of the previous two values is chosen for the vCPU and memory request to use for your Pod.
- Fargate adds 256 MB to each Pod's memory reservation for the required Kubernetes components (`kubelet`, `kube-proxy`, and `containerd`).

Fargate rounds up to the following compute configuration that most closely matches the sum of vCPU and memory requests in order to ensure Pods always have the resources that they need to run.

If you don't specify a vCPU and memory combination, then the smallest available combination is used (.25 vCPU and 0.5 GB memory).

The following table shows the vCPU and memory combinations that are available for Pods running on Fargate.

vCPU value	Memory value
.25 vCPU	0.5 GB, 1 GB, 2 GB
.5 vCPU	1 GB, 2 GB, 3 GB, 4 GB
1 vCPU	2 GB, 3 GB, 4 GB, 5 GB, 6 GB, 7 GB, 8 GB
2 vCPU	Between 4 GB and 16 GB in 1-GB increments
4 vCPU	Between 8 GB and 30 GB in 1-GB increments
8 vCPU	Between 16 GB and 60 GB in 4-GB increments
16 vCPU	Between 32 GB and 120 GB in 8-GB increments

The additional memory reserved for the Kubernetes components can cause a Fargate task with more vCPUs than requested to be provisioned. For example, a request for 1 vCPU and 8 GB memory will have 256 MB added to its memory request, and will provision a Fargate task with 2 vCPUs and 9 GB memory, since no task with 1 vCPU and 9 GB memory is available.

There is no correlation between the size of the Pod running on Fargate and the node size reported by Kubernetes with `kubectl get nodes`. The reported node size is often larger than the Pod's capacity. You can verify Pod capacity with the following command. Replace `default` with your Pod's namespace and `pod-name` with the name of your Pod.

```
kubectl describe pod --namespace default pod-name
```

An example output is as follows.

```
[...]
annotations:
  CapacityProvisioned: 0.25vCPU 0.5GB
[...]
```

The `CapacityProvisioned` annotation represents the enforced Pod capacity and it determines the cost of your Pod running on Fargate. For pricing information for the compute configurations, see [AWS Fargate Pricing](#).

Fargate storage

A Pod running on Fargate automatically mounts an Amazon EFS file system. You can't use dynamic persistent volume provisioning with Fargate nodes, but you can use static provisioning. For more information, see [Amazon EFS CSI Driver](#) on GitHub.

When provisioned, each Pod running on Fargate receives a default 20 GiB of ephemeral storage. This type of storage is deleted after a Pod stops. New Pods launched onto Fargate have encryption of the ephemeral storage volume enabled by default. The ephemeral Pod storage is encrypted with an AES-256 encryption algorithm using AWS Fargate managed keys.

Note

The default usable storage for Amazon EKS Pods that run on Fargate is less than 20 GiB. This is because some space is used by the kubelet and other Kubernetes modules that are loaded inside the Pod.

You can increase the total amount of ephemeral storage up to a maximum of 175 GiB. To configure the size with Kubernetes, specify the requests of ephemeral-storage resource to each container in a Pod. When Kubernetes schedules Pods, it ensures that the sum of the resource requests for each Pod is less than the capacity of the Fargate task. For more information, see [Resource Management for Pods and Containers](#) in the Kubernetes documentation.

Amazon EKS Fargate provisions more ephemeral storage than requested for the purposes of system use. For example, a request of 100 GiB will provision a Fargate task with 115 GiB ephemeral storage.

Fargate OS patching

Amazon EKS periodically patches the OS for AWS Fargate nodes to keep them secure. As part of the patching process, we recycle the nodes to install OS patches. Updates are attempted in a way that creates the least impact on your services. However, if Pods aren't successfully evicted, there are times when they must be deleted. The following are actions that you can take to minimize potential disruptions:

- Set appropriate Pod disruption budgets (PDBs) to control the number of Pods that are down simultaneously.
- Create Amazon EventBridge rules to handle failed evictions before the Pods are deleted.
- Create a notification configuration in AWS User Notifications.

Amazon EKS works closely with the Kubernetes community to make bug fixes and security patches available as quickly as possible. All Fargate Pods start on the most recent Kubernetes patch version, which is available from Amazon EKS for the Kubernetes version of your cluster. If you have a Pod with an older patch version, Amazon EKS might recycle it to update it to the latest version. This ensures that your Pods are equipped with the latest security updates. That way, if there's a critical [Common Vulnerabilities and Exposures](#) (CVE) issue, you're kept up to date to reduce security risks.

To limit the number of Pods that are down at one time when Pods are recycled, you can set Pod disruption budgets (PDBs). You can use PDBs to define minimum availability based on the requirements of each of your applications while still allowing updates to occur. For more information, see [Specifying a Disruption Budget for your Application](#) in the *Kubernetes Documentation*.

Amazon EKS uses the [Eviction API](#) to safely drain the Pod while respecting the PDBs that you set for the application. Pods are evicted by Availability Zone to minimize impact. If the eviction succeeds, the new Pod gets the latest patch and no further action is required.

When the eviction for a Pod fails, Amazon EKS sends an event to your account with details about the Pods that failed eviction. You can act on the message before the scheduled termination time. The specific time varies based on the urgency of the patch. When it's time, Amazon EKS attempts to evict the Pods again. However, this time a new event isn't sent if the eviction fails. If the eviction fails again, your existing Pods are deleted periodically so that the new Pods can have the latest patch.

The following is a sample event received when the Pod eviction fails. It contains details about the cluster, Pod name, Pod namespace, Fargate profile, and the scheduled termination time.

```
{  
    "version": "0",  
    "id": "12345678-90ab-cdef-0123-4567890abcde",  
    "detail-type": "EKS Fargate Pod Scheduled Termination",  
    "source": "aws.eks",
```

```

"account": "111122223333",
"time": "2021-06-27T12:52:44Z",
"region": "region-code",
"resources": [
    "default/my-database-deployment"
],
"detail": {
    "clusterName": "my-cluster",
    "fargateProfileName": "my-fargate-profile",
    "podName": "my-pod-name",
    "podNamespace": "default",
    "evictErrorMessage": "Cannot evict pod as it would violate the pod's disruption budget",
    "scheduledTerminationTime": "2021-06-30T12:52:44.832Z[UTC]"
}
}

```

In addition, having multiple PDBs associated with a Pod can cause an eviction failure event. This event returns the following error message.

```
"evictErrorMessage": "This pod has multiple PodDisruptionBudget, which the eviction subresource does not support",
```

You can create a desired action based on this event. For example, you can adjust your Pod disruption budget (PDB) to control how the Pods are evicted. More specifically, suppose that you start with a PDB that specifies the target percentage of Pods that are available. Before your Pods are force terminated during an upgrade, you can adjust the PDB to a different percentage of Pods. To receive this event, you must create an Amazon EventBridge rule in the AWS account and AWS Region that the cluster belongs to. The rule must use the following **Custom pattern**. For more information, see [Creating Amazon EventBridge rules that react to events](#) in the *Amazon EventBridge User Guide*.

```
{
  "source": ["aws.eks"],
  "detail-type": ["EKS Fargate Pod Scheduled Termination"]
}
```

A suitable target can be set for the event to capture it. For a complete list of available targets, see [Amazon EventBridge targets](#) in the *Amazon EventBridge User Guide*. You can also create a notification configuration in AWS User Notifications. When using the AWS Management Console to create the notification, under **Event Rules**, choose **Elastic Kubernetes Service (EKS)** for **AWS service name** and **EKS Fargate Pod Scheduled Termination** for **Event type**. For more information, see [Getting started with AWS User Notifications](#) in the AWS User Notifications User Guide.

Fargate metrics

You can collect system metrics and CloudWatch usage metrics for AWS Fargate.

Application metrics

For applications running on Amazon EKS and AWS Fargate, you can use the AWS Distro for OpenTelemetry (ADOT). ADOT allows you to collect system metrics and send them to CloudWatch Container Insights dashboards. To get started with ADOT for applications running on Fargate, see [Using CloudWatch Container Insights with AWS Distro for OpenTelemetry](#) in the ADOT documentation.

Usage metrics

You can use CloudWatch usage metrics to provide visibility into your account's usage of resources. Use these metrics to visualize your current service usage on CloudWatch graphs and dashboards.

AWS Fargate usage metrics correspond to AWS service quotas. You can configure alarms that alert you when your usage approaches a service quota. For more information about Fargate service quotas, see [Amazon EKS service quotas \(p. 455\)](#).

AWS Fargate publishes the following metrics in the AWS/Usage namespace.

Metric	Description
ResourceCount	The total number of the specified resource running on your account. The resource is defined by the dimensions associated with the metric.

The following dimensions are used to refine the usage metrics that are published by AWS Fargate.

Dimension	Description
Service	The name of the AWS service containing the resource. For AWS Fargate usage metrics, the value for this dimension is Fargate.
Type	The type of entity that's being reported. Currently, the only valid value for AWS Fargate usage metrics is Resource.
Resource	<p>The type of resource that's running.</p> <p>Currently, AWS Fargate returns information on your Fargate On-Demand usage. The resource value for Fargate On-Demand usage is OnDemand.</p> <p>Note Fargate On-Demand usage combines Amazon EKS Pods using Fargate, Amazon ECS tasks using the Fargate launch type and Amazon ECS tasks using the FARGATE capacity provider.</p>
Class	The class of resource being tracked. Currently, AWS Fargate doesn't use the class dimension.

Creating a CloudWatch alarm to monitor Fargate resource usage metrics

AWS Fargate provides CloudWatch usage metrics that correspond to the AWS service quotas for Fargate On-Demand resource usage. In the Service Quotas console, you can visualize your usage on a graph. You can also configure alarms that alert you when your usage approaches a service quota. For more information, see [Fargate metrics \(p. 143\)](#).

Use the following steps to create a CloudWatch alarm based on the Fargate resource usage metrics.

To create an alarm based on your Fargate usage quotas (AWS Management Console)

1. Open the Service Quotas console at <https://console.aws.amazon.com/servicequotas/>.
2. In the left navigation pane, choose **AWS services**.
3. From the **AWS services** list, search for and select **AWS Fargate**.
4. In the **Service quotas** list, choose the Fargate usage quota you want to create an alarm for.
5. In the Amazon CloudWatch alarms section, choose **Create**.
6. For **Alarm threshold**, choose the percentage of your applied quota value that you want to set as the alarm value.

7. For **Alarm name**, enter a name for the alarm and then choose **Create**.

Fargate logging

Amazon EKS on Fargate offers a built-in log router based on Fluent Bit. This means that you don't explicitly run a Fluent Bit container as a sidecar, but Amazon runs it for you. All that you have to do is configure the log router. The configuration happens through a dedicated ConfigMap that must meet the following criteria:

- Named aws-logging
- Created in a dedicated namespace called aws-observability
- Can't exceed 5300 characters.

Once you've created the ConfigMap, Amazon EKS on Fargate automatically detects it and configures the log router with it. Fargate uses a version of AWS for Fluent Bit, an upstream compliant distribution of Fluent Bit managed by AWS. For more information, see [AWS for Fluent Bit](#) on GitHub.

The log router allows you to use the breadth of services at AWS for log analytics and storage. You can stream logs from Fargate directly to Amazon CloudWatch, Amazon OpenSearch Service. You can also stream logs to destinations such as [Amazon S3](#), [Amazon Kinesis Data Streams](#), and partner tools through [Amazon Kinesis Data Firehose](#).

Prerequisites

- An existing Fargate profile that specifies an existing Kubernetes namespace that you deploy Fargate Pods to. For more information, see [Create a Fargate profile for your cluster \(p. 134\)](#).
- An existing Fargate Pod execution role. For more information, see [Create a Fargate Pod execution role \(p. 133\)](#).

Log router configuration

To configure the log router

In the following steps, replace every *example value* with your own values.

1. Create a dedicated Kubernetes namespace named aws-observability.

- a. Save the following contents to a file named *aws-observability-namespace.yaml* on your computer. The value for name must be aws-observability and the aws-observability: enabled label is required.

```
kind: Namespace
apiVersion: v1
metadata:
  name: aws-observability
  labels:
    aws-observability: enabled
```

- b. Create the namespace.

```
kubectl apply -f aws-observability-namespace.yaml
```

2. Create a ConfigMap with a Fluent Conf data value to ship container logs to a destination. Fluent Conf is Fluent Bit, which is a fast and lightweight log processor configuration language that's used to

route container logs to a log destination of your choice. For more information, see [Configuration File](#) in the Fluent Bit documentation.

Important

The main sections included in a typical Fluent Conf are Service, Input, Filter, and Output. The Fargate log router however, only accepts:

- The Filter and Output sections.
- A Parser section.

If you provide any other sections, they will be rejected.

The Fargate log router manages the Service and Input sections. It has the following Input section, which can't be modified and isn't needed in your ConfigMap. However, you can get insights from it, such as the memory buffer limit and the tag applied for logs.

```
[INPUT]
  Name tail
  Buffer_Max_Size 66KB
  DB /var/log/flb_kube.db
  Mem_Buf_Limit 45MB
  Path /var/log/containers/*.log
  Read_From_Head On
  Refresh_Interval 10
  Rotate_Wait 30
  Skip_Long_Lines On
  Tag kube.*
```

When creating the ConfigMap, take into account the following rules that Fargate uses to validate fields:

- [FILTER], [OUTPUT], and [PARSER] are supposed to be specified under each corresponding key. For example, [FILTER] must be under filters.conf. You can have one or more [FILTER]s under filters.conf. The [OUTPUT] and [PARSER] sections should also be under their corresponding keys. By specifying multiple [OUTPUT] sections, you can route your logs to different destinations at the same time.
- Fargate validates the required keys for each section. Name and match are required for each [FILTER] and [OUTPUT]. Name and format are required for each [PARSER]. The keys are case-insensitive.
- Environment variables such as \${ENV_VAR} aren't allowed in the ConfigMap.
- The indentation has to be the same for either directive or key-value pair within each filters.conf, output.conf, and parsers.conf. Key-value pairs have to be indented more than directives.
- Fargate validates against the following supported filters: grep, parser, record_modifier, rewrite_tag, throttle, nest, modify, and kubernetes.
- Fargate validates against the following supported output: es, firehose, kinesis_firehose, cloudwatch, cloudwatch_logs, and kinesis.
- At least one supported Output plugin has to be provided in the ConfigMap to enable logging. Filter and Parser aren't required to enable logging.

You can also run Fluent Bit on Amazon EC2 using the desired configuration to troubleshoot any issues that arise from validation. Create your ConfigMap using one of the following examples.

Important

Amazon EKS Fargate logging doesn't support dynamic configuration of ConfigMaps. Any changes to ConfigMaps are applied to new Pods only. Changes aren't applied to existing Pods.

Create a ConfigMap using the example for your desired log destination.

Note

You can also use Amazon Kinesis Data Streams for your log destination. If you use Kinesis Data Streams, make sure that the pod execution role has been granted the `kinesis:PutRecords` permission. For more information, see [Amazon Kinesis Data Streams Permissions](#) in the *Fluent Bit: Official Manual*.

CloudWatch

To create a ConfigMap for CloudWatch

You have two output options when using CloudWatch:

- [An output plugin written in C](#)
- [An output plugin written in Golang](#)

The following example shows you how to use the `cloudwatch_logs` plugin to send logs to CloudWatch.

1. Save the following contents to a file named `aws-logging-cloudwatch-configmap.yaml`. Replace `region-code` with the AWS Region that your cluster is in. The parameters under [OUTPUT] are required.

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: aws-logging
  namespace: aws-observability
data:
  flb_log_cw: "false"  # Set to true to ship Fluent Bit process logs to
  CloudWatch.
  filters.conf: |
    [FILTER]
      Name parser
      Match *
      Key_name log
      Parser crio
    [FILTER]
      Name kubernetes
      Match kube./*
      Merge_Log On
      Keep_Log Off
      Buffer_Size 0
      Kube_Meta_Cache_TTL 300s
  output.conf: |
    [OUTPUT]
      Name cloudwatch_logs
      Match kube./*
      region region-code
      log_group_name my-logs
      log_stream_prefix from-fluent-bit-
      log_retention_days 60
      auto_create_group true
  parsers.conf: |
    [PARSER]
```

```
Name crio
Format Regex
Regex ^(?<time>[^ ]+) (?<stream>stdout|stderr) (?<logtag>P|F) (?<log>.*)
Time_Key time
Time_Format %Y-%m-%dT%H:%M:%S.%L%z
```

2. Apply the manifest to your cluster.

```
kubectl apply -f aws-logging-cloudwatch-configmap.yaml
```

3. Download the CloudWatch IAM policy to your computer. You can also [view the policy](#) on GitHub.

```
curl -O https://raw.githubusercontent.com/aws-samples/amazon-eks-fluent-logging-examples/mainline/examples/fargate/cloudwatchlogs/permissions.json
```

Amazon OpenSearch Service

To create a ConfigMap for Amazon OpenSearch Service

If you want to send logs to Amazon OpenSearch Service, you can use `es` output, which is a plugin written in C. The following example shows you how to use the plugin to send logs to OpenSearch.

1. Save the following contents to a file named `aws-logging-opensearch-configmap.yaml`. Replace every `example value` with your own values.

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: aws-logging
  namespace: aws-observability
data:
  output.conf: |
    [OUTPUT]
    Name es
    Match *
    Host search-example-gjxdclagiprbglqn42jsty66y.region-code.es.amazonaws.com
    Port 443
    Index example
    Type example_type
    AWS_Auth On
    AWS_Region region-code
    tls On
```

2. Apply the manifest to your cluster.

```
kubectl apply -f aws-logging-opensearch-configmap.yaml
```

3. Download the OpenSearch IAM policy to your computer. You can also [view the policy](#) on GitHub.

```
curl -O https://raw.githubusercontent.com/aws-samples/amazon-eks-fluent-logging-examples/mainline/examples/fargate/amazon-elasticsearch/permissions.json
```

Make sure that OpenSearch Dashboards' access control is configured properly. The `all_access` role in OpenSearch Dashboards needs to have the Fargate Pod execution role

and the IAM role mapped. The same mapping must be done for the `security_manager` role. You can add the previous mappings by selecting Menu, then Security, then Roles, and then select the respective roles. For more information, see [How do I troubleshoot CloudWatch Logs so that it streams to my Amazon ES domain?](#).

Kinesis Data Firehose

To create a ConfigMap for Kinesis Data Firehose

You have two output options when sending logs to Kinesis Data Firehose:

- [`kinesis_firehose`](#) – An output plugin written in C.
- [`firehose`](#) – An output plugin written in Golang.

The following example shows you how to use the `kinesis_firehose` plugin to send logs to Kinesis Data Firehose.

1. Save the following contents to a file named `aws-logging-firehose-configmap.yaml`. Replace `region-code` with the AWS Region that your cluster is in.

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: aws-logging
  namespace: aws-observability
data:
  output.conf: |
    [OUTPUT]
    Name kinesis_firehose
    Match *
    region region-code
    delivery_stream my-stream-firehose
```

2. Apply the manifest to your cluster.

```
kubectl apply -f aws-logging-firehose-configmap.yaml
```

3. Download the Kinesis Data Firehose IAM policy to your computer. You can also [view the policy](#) on GitHub.

```
curl -o https://raw.githubusercontent.com/aws-samples/amazon-eks-fluent-logging-examples/mainline/examples/fargate/kinesis-firehose/permissions.json
```

3. Create an IAM policy from the policy file you downloaded in a previous step.

```
aws iam create-policy --policy-name eks-fargate-logging-policy --policy-document
file://permissions.json
```

4. Attach the IAM policy to the pod execution role specified for your Fargate profile with the following command. Replace `111122223333` with your account ID. Replace `AmazonEKSFargatePodExecutionRole` with your Pod execution role (for more information, see [Create a Fargate Pod execution role \(p. 133\)](#)). If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov::`.

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::111122223333:policy/eks-fargate-logging-policy \
--role-name AmazonEKSFargatePodExecutionRole
```

Kubernetes filter support

This feature requires the following minimum Kubernetes version and platform level, or later.

Kubernetes version	Platform level
1.23 and later	eks.1

The Fluent Bit Kubernetes filter allows you to add Kubernetes metadata to your log files. For more information about the filter, see [Kubernetes](#) in the Fluent Bit documentation. You can apply a filter using the API server endpoint.

```
filters.conf: |
[FILTER]
  Name      kubernetes
  Match    kube./*
  Merge_Log  On
  Buffer_Size  0
  Kube_Meta_Cache_TTL 300s
```

Important

- Kube_URL, Kube_CA_File, Kube_Token_Command, and Kube_Token_File are service owned configuration parameters and must not be specified. Amazon EKS Fargate populates these values.
- Kube_Meta_Cache_TTL is the time Fluent Bit waits until it communicates with the API server for the latest metadata. If Kube_Meta_Cache_TTL isn't specified, Amazon EKS Fargate appends a default value of 30 minutes to lessen the load on the API server.

To ship Fluent Bit process logs to your account

You can optionally ship Fluent Bit process logs to Amazon CloudWatch using the following ConfigMap. Shipping Fluent Bit process logs to CloudWatch requires additional log ingestion and storage costs. Replace `region-code` with the AWS Region that your cluster is in.

```
kind: ConfigMap
apiVersion: v1
metadata:
  name: aws-logging
  namespace: aws-observability
  labels:
data:
  # Configuration files: server, input, filters and output
  # =====
  flb_log_cw: "true" # Ships Fluent Bit process logs to CloudWatch.

  output.conf: |
    [OUTPUT]
      Name cloudwatch
      Match kube./*
      region region-code
      log_group_name fluent-bit-cloudwatch
      log_stream_prefix from-fluent-bit-
      auto_create_group true
```

The logs are in the AWS Region that the cluster resides in under CloudWatch. The log group name is `my-cluster-fluent-bit-logs` and the Fluent Bit logstream name is `fluent-bit-podname-pod-namespace`.

Note

- The process logs are shipped only when the Fluent Bit process successfully starts. If there is a failure while starting Fluent Bit, the process logs are missed. You can only ship process logs to CloudWatch.
- To debug shipping process logs to your account, you can apply the previous ConfigMap to get the process logs. Fluent Bit failing to start is usually due to your ConfigMap not being parsed or accepted by Fluent Bit while starting.

To stop shipping Fluent Bit process logs

Shipping Fluent Bit process logs to CloudWatch requires additional log ingestion and storage costs. To exclude process logs in an existing ConfigMap setup, do the following steps.

1. Locate the CloudWatch log group automatically created for your Amazon EKS cluster's Fluent Bit process logs after enabling Fargate logging. It follows the format `{cluster_name}-fluent-bit-logs`.
2. Delete the existing CloudWatch log streams created for each Pod's process logs in the CloudWatch log group.
3. Edit the ConfigMap and set `flb_log_cw: "false"`.
4. Restart any existing Pods in the cluster.

Test application

1. Deploy a sample Pod.
 - a. Save the following contents to a file named `sample-app.yaml` on your computer.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: sample-app
  namespace: same-namespace-as-your-fargate-profile
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
        - name: nginx
          image: nginx:latest
          ports:
            - name: http
              containerPort: 80
```

- b. Apply the manifest to the cluster.

```
kubectl apply -f sample-app.yaml
```

2. View the NGINX logs using the destination(s) that you configured in the ConfigMap.

Size considerations

We suggest that you plan for up to 50 MB of memory for the log router. If you expect your application to generate logs at very high throughput then you should plan for up to 100 MB.

Troubleshooting

To confirm whether the logging feature is enabled or disabled for some reason, such as an invalid ConfigMap, and why it's invalid, check your Pod events with `kubectl describe pod pod_name`. The output might include Pod events that clarify whether logging is enabled or not, such as the following example output.

```
[...]
Annotations:           CapacityProvisioned: 0.25vCPU 0.5GB
                      Logging: LoggingDisabled: LOGGING_CONFIGMAP_NOT_FOUND
                      kubernetes.io/psp: eks.privileged
[...]
Events:
  Type      Reason     Age          From
  ----      -----     ---         ---
  -----
  Warning   LoggingDisabled <unknown>  fargate-scheduler
            Disabled logging because aws-logging configmap was not found. configmap "aws-
logging" not found
```

The Pod events are ephemeral with a time period depending on the settings. You can also view a Pod's annotations using `kubectl describe pod pod-name`. In the Pod annotation, there is information about whether the logging feature is enabled or disabled and the reason.

Choosing an Amazon EC2 instance type

Amazon EC2 provides a wide selection of instance types for worker nodes. Each instance type offers different compute, memory, storage, and network capabilities. Each instance is also grouped in an instance family based on these capabilities. For a list, see [Available instance types](#) in the *Amazon EC2 User Guide for Linux Instances* and [Available instance types](#) in the *Amazon EC2 User Guide for Windows Instances*. Amazon EKS releases several variations of Amazon EC2 AMIs to enable support. To make sure that the instance type you select is compatible with Amazon EKS, consider the following criteria.

- All Amazon EKS AMIs don't currently support the g5g and mac families.
- Arm and non-accelerated Amazon EKS AMIs don't support the g3, g4, inf, and p families.
- Accelerated Amazon EKS AMIs don't support the a, c, hpc, m, and t families.

When choosing between instance types that are supported by Amazon EKS, consider the following capabilities of each type.

Number of instances in a node group

In general, fewer, larger instances are better, especially if you have a lot of Daemonsets. Each instance requires API calls to the API server, so the more instances you have, the more load on the API server.

Operating system

Review the supported instance types for [Linux](#), [Windows](#), and [Bottlerocket](#). Before creating Windows instances, review [the section called "Enabling Windows support" \(p. 49\)](#).

Hardware architecture

Do you need x86 or Arm? You can only deploy Linux on Arm. Before deploying Arm instances, review [the section called "Arm" \(p. 160\)](#). Do you need instances built on the Nitro System ([Linux](#) or [Windows](#)) or that have [Accelerated](#) capabilities? If you need accelerated capabilities, you can only use Linux with Amazon EKS.

Maximum number of Pods

Since each Pod is assigned its own IP address, the number of IP addresses supported by an instance type is a factor in determining the number of Pods that can run on the instance. To manually determine how many Pods an instance type supports, see [Amazon EKS recommended maximum Pods for each Amazon EC2 instance type \(p. 154\)](#).

Note

If you're using an Amazon EKS optimized Amazon Linux 2 AMI that's v20220406 or newer, you can use a new instance type without upgrading to the latest AMI. For these AMIs, the AMI auto-calculates the necessary max-pods value if it isn't listed in the [eni-max-pods.txt](#) file. Instance types that are currently in preview may not be supported by Amazon EKS by default. Values for max-pods for such types still need to be added to eni-max-pods.txt in our AMI.

[AWS Nitro System](#) instance types optionally support significantly more IP addresses than non-Nitro System instance types. However, not all IP addresses assigned for an instance are available to Pods. To assign a significantly larger number of IP addresses to your instances, you must have version 1.9.0 or later of the Amazon VPC CNI add-on installed in your cluster and configured appropriately. For more information, see [Increase the amount of available IP addresses for your Amazon EC2 nodes \(p. 318\)](#). To assign the largest number of IP addresses to your instances, you must have version 1.10.1 or later of the Amazon VPC CNI add-on installed in your cluster and deploy the cluster with the IPv6 family.

IP family

You can use any supported instance type when using the IPv4 family for a cluster, which allows your cluster to assign private IPv4 addresses to your Pods and Services. But if you want to use the IPv6 family for your cluster, then you must use [AWS Nitro System](#) instance types or bare metal instance types. Only IPv4 is supported for Windows instances. Your cluster must be running version 1.10.1 or later of the Amazon VPC CNI add-on. For more information about using IPv6, see [Tutorial: Assigning IPv6 addresses to Pods and services \(p. 278\)](#).

Version of the Amazon VPC CNI add-on that you're running

The latest version of the [Amazon VPC CNI plugin for Kubernetes](#) supports [these instance types](#). You may need to update your Amazon VPC CNI add-on version to take advantage of the latest supported instance types. For more information, see [the section called "Amazon VPC CNI plugin for Kubernetes" \(p. 266\)](#). The latest version supports the latest features for use with Amazon EKS. Earlier versions don't support all features. You can view features supported by different versions in the [Changelog](#) on GitHub.

AWS Region that you're creating your nodes in

Not all instance types are available in all AWS Regions.

Whether you're using security groups for Pods

If you're using security groups for Pods, only specific instance types are supported. For more information, see [Tutorial: Security groups for Pods \(p. 324\)](#).

Amazon EKS recommended maximum Pods for each Amazon EC2 instance type

Since each Pod is assigned its own IP address, the number of IP addresses supported by an instance type is a factor in determining the number of Pods that can run on the instance. Amazon EKS provides a script that you can download and run to determine the Amazon EKS recommended maximum number of Pods to run on each instance type. The script uses hardware attributes of each instance, and configuration options, to determine the maximum Pods number. You can use the number returned in these steps to enable capabilities such as [assigning IP addresses to Pods from a different subnet than the instance's \(p. 306\)](#) and [significantly increasing the number of IP addresses for your instance \(p. 318\)](#). If you're using a managed node group with multiple instance types, use a value that would work for all instance types.

1. Download a script that you can use to calculate the maximum number of Pods for each instance type.

```
curl -0 https://raw.githubusercontent.com/aws-labs/amazon-eks-ami/master/files/max-pods-calculator.sh
```

2. Mark the script as executable on your computer.

```
chmod +x max-pods-calculator.sh
```

3. Run the script, replacing *m5.large* with the instance type that you plan to deploy and *1.9.0-eksbuild.1* with your Amazon VPC CNI add-on version. To determine your add-on version, see the update procedures in [Working with the Amazon VPC CNI plugin for Kubernetes Amazon EKS add-on \(p. 266\)](#).

```
./max-pods-calculator.sh --instance-type m5.large --cni-version 1.9.0-eksbuild.1
```

An example output is as follows.

29

You can add the following options to the script to see the maximum Pods supported when using optional capabilities.

- `--cni-custom-networking-enabled` – Use this option when you want to assign IP addresses from a different subnet than your instance's. For more information, see [the section called "Custom networking" \(p. 306\)](#). Adding this option to the previous script with the same example values yields 20.
- `--cni-prefix-delegation-enabled` – Use this option when you want to assign significantly more IP addresses to each elastic network interface. This capability requires an Amazon Linux instance that runs on the Nitro System and version 1.9.0 or later of the Amazon VPC CNI add-on. For more information, see [the section called "Increase available IP addresses" \(p. 318\)](#). Adding this option to the previous script with the same example values yields 110.

You can also run the script with the `--help` option to see all available options.

Note

The max Pods calculator script limits the return value to 110 based on [Kubernetes scalability thresholds](#) and recommended settings. If your instance type has greater than 30 vCPUs, this limit jumps to 250, a number based on internal Amazon EKS scalability team testing. For more information, see the [Amazon VPC CNI plugin increases pods per node limits](#) blog post.

Amazon EKS optimized AMIs

You can deploy nodes with pre-built Amazon EKS optimized [Amazon Machine Images](#) (AMIs) or your own custom AMIs. For information about each type of Amazon EKS optimized AMI, see one of the following topics. For instructions on how to create your own custom AMI, see [Amazon EKS optimized Amazon Linux AMI build script \(p. 173\)](#).

Topics

- [Amazon EKS ended support for Dockershim \(p. 155\)](#)
- [Amazon EKS optimized Amazon Linux AMIs \(p. 156\)](#)
- [Amazon EKS optimized Bottlerocket AMIs \(p. 174\)](#)
- [Amazon EKS optimized Ubuntu Linux AMIs \(p. 184\)](#)
- [Amazon EKS optimized Windows AMIs \(p. 184\)](#)

Amazon EKS ended support for Dockershim

Kubernetes no longer supports Dockershim. The Kubernetes team removed the runtime in Kubernetes version 1.24. For more information, see [Kubernetes is Moving on From Dockershim: Commitments and Next Steps](#) on the [Kubernetes Blog](#).

Amazon EKS also ended support for Dockershim starting with the Kubernetes version 1.24 release. Amazon EKS AMIs that are officially published have containerd as the only runtime starting with version 1.24. This topic covers some details, but more information is available in [All you need to know about moving to containerd on Amazon EKS](#).

There's a kubectl plugin that you can use to see which of your Kubernetes workloads mount the Docker socket volume. For more information, see [Detector for Docker Socket \(DDS\)](#) on GitHub. Amazon EKS AMIs that run Kubernetes versions that are earlier than 1.24 use Docker as the default runtime. However, these Amazon EKS AMIs have a bootstrap flag option that you can use to test out your workloads on any supported cluster using containerd. For more information, see [Enable the containerd runtime bootstrap flag \(p. 157\)](#).

We will continue to publish AMIs for existing Kubernetes versions until the end of their support date. For more information, see [Amazon EKS Kubernetes release calendar \(p. 61\)](#). If you require more time to test your workloads on containerd, use a supported version before 1.24. But, when you want to upgrade official Amazon EKS AMIs to version 1.24 or later, make sure to validate that your workloads run on containerd.

The containerd runtime provides more reliable performance and security. containerd is the runtime that's being standardized on across Amazon EKS. Fargate and Bottlerocket already use containerd only. containerd helps to minimize the number of Amazon EKS AMI releases that are required to address Dockershim [Common Vulnerabilities and Exposures](#) (CVEs). Because Dockershim already uses containerd internally, you might not need to make any changes. However, there are some situations where changes might or must be required:

- You must make changes to applications that mount the Docker socket. For example, container images that are built with a container are impacted. Many monitoring tools also mount the Docker socket. You might need to wait for updates or re-deploy workloads for runtime monitoring.
- You might need to make changes for applications that are reliant on specific Docker settings. For example, the HTTPS_PROXY protocol is no longer supported. You must update applications that use this protocol. For more information, see [dockerd](#) in the [Docker Docs](#).
- If you use the Amazon ECR credential helper to pull images, you must switch to the kubelet image credential provider. For more information, see [Configure a kubelet image credential provider](#) in the Kubernetes documentation.

- Because Amazon EKS 1.24 no longer supports Docker, some flags that the [Amazon EKS bootstrap script](#) previously supported are no longer supported. Before moving to Amazon EKS 1.24 or later, you must remove any reference to flags that are now unsupported:
 - `--container-runtime dockerd` (`containerd` is the only supported value)
 - `--enable-docker-bridge`
 - `--docker-config-json`
- If you already have Fluentd configured for Container Insights, then you must migrate Fluentd to Fluent Bit before changing to `containerd`. The Fluentd parsers are configured to only parse log messages in JSON format. Unlike `dockerd`, the `containerd` container runtime has log messages that aren't in JSON format. If you don't migrate to Fluent Bit, some of the configured Fluentd's parsers will generate a massive amount of errors inside the Fluentd container. For more information on migrating, see [Set up Fluent Bit as a DaemonSet to send logs to CloudWatch Logs](#).
- If you use a custom AMI and you are upgrading to Amazon EKS 1.24, then you must make sure that IP forwarding is enabled for your worker nodes. This setting wasn't needed with Docker but is required for `containerd`. It is needed to troubleshoot Pod-to-Pod, Pod-to-external, or Pod-to-apiserver network connectivity.

To verify this setting on a worker node, run either of the following commands:

- `sysctl net.ipv4.ip_forward`
- `cat /proc/sys/net/ipv4/ip_forward`

If the output is `0`, then run either of the following commands to activate the `net.ipv4.ip_forward` kernel variable:

- `sysctl -w net.ipv4.ip_forward=1`
- `echo 1 > /proc/sys/net/ipv4/ip_forward`

For the setting's activation on Amazon EKS AMIs in the `containerd` runtime, see [install-worker.sh](#) on GitHub.

Amazon EKS optimized Amazon Linux AMIs

The Amazon EKS optimized Amazon Linux AMI is built on top of Amazon Linux 2, and is configured to serve as the base image for Amazon EKS nodes. The AMI is configured to work with Amazon EKS and it includes the following components:

- `kubelet`
- AWS IAM Authenticator
- Docker (Amazon EKS version 1.23 and earlier)
- `containerd`

Note

- You can track security or privacy events for Amazon Linux 2 at the [Amazon Linux security center](#) or subscribe to the associated [RSS feed](#). Security and privacy events include an overview of the issue, what packages are affected, and how to update your instances to correct the issue.
- Before deploying an accelerated or Arm AMI, review the information in [Amazon EKS optimized accelerated Amazon Linux AMIs \(p. 158\)](#) and [Amazon EKS optimized Arm Amazon Linux AMIs \(p. 160\)](#).
- You can use an optional bootstrap flag to enable the `containerd` runtime for Amazon EKS optimized Amazon Linux 2 AMIs. This feature provides a clear path to migrate to `containerd`.

when updating to version 1.24 or later. Amazon EKS ended support for Docker starting with the Kubernetes version 1.24 launch. The containerd runtime is widely adopted in the Kubernetes community and is a graduated project with the CNCF. You can test it by adding a node group to a new or existing cluster. For more information, see [Enable the containerd runtime bootstrap flag \(p. 157\)](#).

- Starting with Kubernetes version 1.28, you will no longer be able to use Amazon EC2 P2 instances with the Amazon EKS optimized accelerated Amazon Linux AMIs out of the box. These AMIs for Kubernetes versions 1.28 or later will support NVIDIA 525 series or later drivers, which are incompatible with the P2 instances. However, NVIDIA 525 series or later drivers are compatible with the P3, P4, and P5 instances, so you can use those instances with the AMIs for Kubernetes version 1.28 or later. Before your Amazon EKS clusters are upgraded to version 1.28, migrate any P2 instances to P3, P4, and P5 instances. You should also proactively upgrade your applications to work with the NVIDIA 525 series or later.

Enable the containerd runtime bootstrap flag

The Amazon EKS optimized Amazon Linux 2 AMI contains an optional bootstrap flag to enable the containerd runtime. This feature provides a clear path to migrate to containerd. Amazon EKS ended support for Docker starting with the Kubernetes version 1.24 launch. For more information, see [Amazon EKS ended support for Docker shim \(p. 155\)](#).

You can enable the bootstrap flag by creating one of the following types of node groups.

Self-managed

Create the node group using the instructions in [Launching self-managed Amazon Linux nodes \(p. 108\)](#). Specify an Amazon EKS optimized AMI and the following text for the `BootstrapArguments` parameter.

```
--container-runtime containerd
```

Managed

If you use `eksctl`, create a file named `my-nodegroup.yaml` with the following contents. Replace every *example value* with your own values. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters. To retrieve an optimized AMI ID for `ami-1234567890abcdef0`, see [Retrieving Amazon EKS optimized Amazon Linux AMI IDs \(p. 161\)](#).

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
  name: my-cluster
  region: region-code
  version: 1.23
managedNodeGroups:
  - name: my-nodegroup
    ami: ami-1234567890abcdef0
    overrideBootstrapCommand: |
      #!/bin/bash
      /etc/eks/bootstrap.sh my-cluster --container-runtime containerd
```

Note

If you launch many nodes simultaneously, you may also want to specify values for the `--apiserver-endpoint`, `--b64-cluster-ca`, and `--dns-cluster-ip` bootstrap arguments to avoid errors. For more information, see [Specifying an AMI \(p. 102\)](#).

Run the following command to create the node group.

```
eksctl create nodegroup -f my-nodegroup.yaml
```

If you prefer to use a different tool to create your managed node group, you must deploy the node group using a launch template. In your launch template, specify an [Amazon EKS optimized AMI ID \(p. 161\)](#), then [deploy the node group using a launch template \(p. 98\)](#) and provide the following user data. This user data passes arguments into the bootstrap.sh file. For more information about the bootstrap file, see [bootstrap.sh](#) on GitHub.

```
/etc/eks/bootstrap.sh my-cluster --container-runtime containerd
```

Amazon EKS optimized accelerated Amazon Linux AMIs

The Amazon EKS optimized accelerated Amazon Linux AMI is built on top of the standard Amazon EKS optimized Amazon Linux AMI. It's configured to serve as an optional image for Amazon EKS nodes to support GPU and [Inferentia](#) based workloads.

In addition to the standard Amazon EKS optimized AMI configuration, the accelerated AMI includes the following:

- NVIDIA drivers
- The nvidia-container-runtime (as the default runtime)
- AWS Neuron container runtime

Note

- The Amazon EKS optimized accelerated AMI only supports GPU and Inferentia based instance types. Make sure to specify these instance types in your node AWS CloudFormation template. By using the Amazon EKS optimized accelerated AMI, you agree to [NVIDIA's user license agreement \(EULA\)](#).
- The Amazon EKS optimized accelerated AMI was previously referred to as the *Amazon EKS optimized AMI with GPU support*.
- Previous versions of the Amazon EKS optimized accelerated AMI installed the nvidia-docker repository. The repository is no longer included in Amazon EKS AMI version v20200529 and later.

To enable GPU based workloads

The following procedure describes how to run a workload on a GPU based instance with the Amazon EKS optimized accelerated AMI. For other options, see the following references:

- For more information about using Inferentia based workloads, see [Machine learning inference using AWS Inferentia \(p. 415\)](#).
 - For more information about using Neuron, see [Containers - Kubernetes - Getting Started](#) in the [AWS Neuron Documentation](#).
1. After your GPU nodes join your cluster, you must apply the [NVIDIA device plugin for Kubernetes](#) as a DaemonSet on your cluster. Replace *vX.X.X* with your desired [NVIDIA/k8s-device-plugin](#) version before running the following command.

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/vX.X.X/nvidia-device-plugin.yaml
```

2. You can verify that your nodes have allocatable GPUs with the following command.

```
kubectl get nodes "-o=custom-columns=NAME:.metadata.name,GPU:.status.allocatable.nvidia\n\\.com/gpu"
```

To deploy a Pod to test that your GPU nodes are configured properly

1. Create a file named nvidia-smi.yaml with the following contents. Replace **tag** with your desired tag for [nvidia/cuda](#). This manifest launches an [NVIDIA CUDA](#) container that runs nvidia-smi on a node.

```
apiVersion: v1
kind: Pod
metadata:
  name: nvidia-smi
spec:
  restartPolicy: OnFailure
  containers:
  - name: nvidia-smi
    image: nvidia/cuda:tag
    args:
    - "nvidia-smi"
    resources:
      limits:
        nvidia.com/gpu: 1
```

2. Apply the manifest with the following command.

```
kubectl apply -f nvidia-smi.yaml
```

3. After the Pod has finished running, view its logs with the following command.

```
kubectl logs nvidia-smi
```

An example output is as follows.

```
Mon Aug  6 20:23:31 20XX
+-----+
| NVIDIA-SMI XXX.XX          Driver Version: XXX.XX |
+-----+
| GPU  Name     Persistence-M| Bus-Id     Disp.A  Volatile Uncorr. ECC |
| Fan  Temp   Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M. |
|=====+=====+=====+=====+=====+=====+=====+=====|
| 0  Tesla V100-SXM2...  On   | 00000000:00:1C.0 Off |          0 |
| N/A   46C   P0    47W / 300W |      0MiB / 16160MiB |     0%       Default |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+
| Processes:                               GPU Memory |
| GPU     PID  Type  Process name           Usage     |
|=====+=====+=====+=====
| No running processes found               |
+-----+
```

Amazon EKS optimized Arm Amazon Linux AMIs

Arm instances deliver significant cost savings for scale-out and Arm-based applications such as web servers, containerized microservices, caching fleets, and distributed data stores. When adding Arm nodes to your cluster, review the following considerations.

Considerations

- If your cluster was deployed before August 17, 2020, you must do a one-time upgrade of critical cluster add-on manifests. This is so that Kubernetes can pull the correct image for each hardware architecture in use in your cluster. For more information about updating cluster add-ons, see [Update the Kubernetes version for your Amazon EKS cluster \(p. 34\)](#). If you deployed your cluster on or after August 17, 2020, then your CoreDNS, kube-proxy, and Amazon VPC CNI plugin for Kubernetes add-ons are already multi-architecture capable.
- Applications deployed to Arm nodes must be compiled for Arm.
- If you have DaemonSets that are deployed in an existing cluster, or you want to deploy them to a new cluster that you also want to deploy Arm nodes in, then verify that your DaemonSet can run on all hardware architectures in your cluster.
- You can run Arm node groups and x86 node groups in the same cluster. If you do, consider deploying multi-architecture container images to a container repository such as Amazon Elastic Container Registry and then adding node selectors to your manifests so that Kubernetes knows what hardware architecture a Pod can be deployed to. For more information, see [Pushing a multi-architecture image in the Amazon ECR User Guide](#) and the [Introducing multi-architecture container images for Amazon ECR](#) blog post.

More information

For more information about using Amazon EKS optimized Amazon Linux AMIs, see the following sections:

- To use Amazon Linux with managed node groups, see [Managed node groups \(p. 81\)](#).
- To launch self-managed Amazon Linux nodes, see [Retrieving Amazon EKS optimized Amazon Linux AMI IDs \(p. 161\)](#).
- For version information, see [Amazon EKS optimized Amazon Linux AMI versions \(p. 160\)](#).
- To retrieve the latest IDs of the Amazon EKS optimized Amazon Linux AMIs, see [Retrieving Amazon EKS optimized Amazon Linux AMI IDs \(p. 161\)](#).
- For open-source scripts that are used to build the Amazon EKS optimized AMI, see [Amazon EKS optimized Amazon Linux AMI build script \(p. 173\)](#).

Amazon EKS optimized Amazon Linux AMI versions

Amazon EKS optimized Amazon Linux AMIs are versioned by Kubernetes version and the release date of the AMI in the following format:

`k8s_major_version.k8s_minor_version.k8s_patch_version-release_date`

Each AMI release includes various versions of kubelet, Docker, the Linux kernel, and containerd. The accelerated AMI also includes various versions of the NVIDIA driver. You can find this version information in the [Changelog](#) on GitHub.

Retrieving Amazon EKS optimized Amazon Linux AMI IDs

You can programmatically retrieve the Amazon Machine Image (AMI) ID for Amazon EKS optimized AMIs by querying the AWS Systems Manager Parameter Store API. This parameter eliminates the need for you to manually look up Amazon EKS optimized AMI IDs. For more information about the Systems Manager Parameter Store API, see [GetParameter](#). The [IAM principal](#) that you use must have the `ssm:GetParameter` IAM permission to retrieve the Amazon EKS optimized AMI metadata.

You can retrieve the AMI ID with the AWS CLI or the AWS Management Console.

AWS CLI

You can retrieve the image ID of the latest recommended Amazon EKS optimized Amazon Linux AMI with the following command by using the sub-parameter `image_id`. Replace `1.28` with a [supported version \(p. 71\)](#). Replace `region-code` with the AWS Region that your cluster is in. Replace `amazon-linux-2` with `amazon-linux-2-gpu` to see the accelerated AMI ID and `amazon-linux-2-arm64` to see the Arm ID.

```
aws ssm get-parameter --name /aws/service/eks/optimized-ami/1.28/amazon-linux-2/recommended/image_id --region region-code --query "Parameter.Value" --output text
```

An example output is as follows.

```
ami-1234567890abcdef0
```

AWS Management Console

You can query for the recommended Amazon EKS optimized AMI ID using a URL. The URL opens the Amazon EC2 Systems Manager console with the value of the ID for the parameter. In the following URL, replace `1.28` with a [supported version \(p. 71\)](#) and `region-code` with an [Amazon EKS supported Region](#) for which you want the AMI ID. Replace `amazon-linux-2` with `amazon-linux-2-gpu` to see the accelerated AMI ID and `amazon-linux-2-arm64` to see the Arm ID.

```
https://console.aws.amazon.com/systems-manager/parameters/aws/service/eks/optimized-ami/1.28/amazon-linux-2/recommended/image_id/description?region=region-code
```

The following tables have links to the latest IDs of the Amazon EKS optimized Amazon Linux AMIs.

1.28

Kubernetes version 1.28

AWS Region	x86	x86 accelerated	Arm
US East (Ohio) (us-east-2)	View AMI ID	View AMI ID	View AMI ID
US East (N. Virginia) (us-east-1)	View AMI ID	View AMI ID	View AMI ID
US West (Oregon) (us-west-2)	View AMI ID	View AMI ID	View AMI ID
US West (N. California) (us-west-1)	View AMI ID	View AMI ID	View AMI ID

AWS Region	x86	x86 accelerated	Arm
Africa (Cape Town) (af-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID	View AMI ID	View AMI ID
Canada (Central) (ca-central-1)	View AMI ID	View AMI ID	View AMI ID
China (Beijing) (cn-north-1)	View AMI ID	View AMI ID	View AMI ID
China (Ningxia) (cn-northwest-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Frankfurt) (eu-central-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Zurich) (eu-central-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Ireland) (eu-west-1)	View AMI ID	View AMI ID	View AMI ID
Europe (London) (eu-west-2)	View AMI ID	View AMI ID	View AMI ID

AWS Region	x86	x86 accelerated	Arm
Europe (Milan) (eu-south-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Spain) (eu-south-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Paris) (eu-west-3)	View AMI ID	View AMI ID	View AMI ID
Europe (Stockholm) (eu-north-1)	View AMI ID	View AMI ID	View AMI ID
Israel (Tel Aviv) (il-central-1)	View AMI ID	View AMI ID	View AMI ID
Middle East (Bahrain) (me-south-1)	View AMI ID	View AMI ID	View AMI ID
Middle East (UAE) (me-central-1)	View AMI ID	View AMI ID	View AMI ID
South America (São Paulo) (sa-east-1)	View AMI ID	View AMI ID	View AMI ID
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID	View AMI ID	View AMI ID
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID	View AMI ID	View AMI ID

1.27

Kubernetes version 1.27

AWS Region	x86	x86 accelerated	Arm
US East (Ohio) (us-east-2)	View AMI ID	View AMI ID	View AMI ID
US East (N. Virginia) (us-east-1)	View AMI ID	View AMI ID	View AMI ID
US West (Oregon) (us-west-2)	View AMI ID	View AMI ID	View AMI ID
US West (N. California) (us-west-1)	View AMI ID	View AMI ID	View AMI ID
Africa (Cape Town) (af-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID	View AMI ID	View AMI ID

AWS Region	x86	x86 accelerated	Arm
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID	View AMI ID	View AMI ID
Canada (Central) (ca-central-1)	View AMI ID	View AMI ID	View AMI ID
China (Beijing) (cn-north-1)	View AMI ID	View AMI ID	View AMI ID
China (Ningxia) (cn-northwest-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Frankfurt) (eu-central-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Zurich) (eu-central-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Ireland) (eu-west-1)	View AMI ID	View AMI ID	View AMI ID
Europe (London) (eu-west-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Milan) (eu-south-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Spain) (eu-south-2)	View AMI ID	View AMI ID	View AMI ID

AWS Region	x86	x86 accelerated	Arm
Europe (Paris) (eu-west-3)	View AMI ID	View AMI ID	View AMI ID
Europe (Stockholm) (eu-north-1)	View AMI ID	View AMI ID	View AMI ID
Israel (Tel Aviv) (il-central-1)	View AMI ID	View AMI ID	View AMI ID
Middle East (Bahrain) (me-south-1)	View AMI ID	View AMI ID	View AMI ID
Middle East (UAE) (me-central-1)	View AMI ID	View AMI ID	View AMI ID
South America (São Paulo) (sa-east-1)	View AMI ID	View AMI ID	View AMI ID
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID	View AMI ID	View AMI ID
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID	View AMI ID	View AMI ID

1.26

Kubernetes version 1.26

AWS Region	x86	x86 accelerated	Arm
US East (Ohio) (us-east-2)	View AMI ID	View AMI ID	View AMI ID
US East (N. Virginia) (us-east-1)	View AMI ID	View AMI ID	View AMI ID
US West (Oregon) (us-west-2)	View AMI ID	View AMI ID	View AMI ID
US West (N. California) (us-west-1)	View AMI ID	View AMI ID	View AMI ID
Africa (Cape Town) (af-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID	View AMI ID	View AMI ID

AWS Region	x86	x86 accelerated	Arm
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID	View AMI ID	View AMI ID
Canada (Central) (ca-central-1)	View AMI ID	View AMI ID	View AMI ID
China (Beijing) (cn-north-1)	View AMI ID	View AMI ID	View AMI ID
China (Ningxia) (cn-northwest-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Frankfurt) (eu-central-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Zurich) (eu-central-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Ireland) (eu-west-1)	View AMI ID	View AMI ID	View AMI ID
Europe (London) (eu-west-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Milan) (eu-south-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Spain) (eu-south-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Paris) (eu-west-3)	View AMI ID	View AMI ID	View AMI ID
Europe (Stockholm) (eu-north-1)	View AMI ID	View AMI ID	View AMI ID
Israel (Tel Aviv) (il-central-1)	View AMI ID	View AMI ID	View AMI ID

AWS Region	x86	x86 accelerated	Arm
Middle East (Bahrain) (me-south-1)	View AMI ID	View AMI ID	View AMI ID
Middle East (UAE) (me-central-1)	View AMI ID	View AMI ID	View AMI ID
South America (São Paulo) (sa-east-1)	View AMI ID	View AMI ID	View AMI ID
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID	View AMI ID	View AMI ID
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID	View AMI ID	View AMI ID

1.25

Kubernetes version 1.25

AWS Region	x86	x86 accelerated	Arm
US East (Ohio) (us-east-2)	View AMI ID	View AMI ID	View AMI ID
US East (N. Virginia) (us-east-1)	View AMI ID	View AMI ID	View AMI ID
US West (Oregon) (us-west-2)	View AMI ID	View AMI ID	View AMI ID
US West (N. California) (us-west-1)	View AMI ID	View AMI ID	View AMI ID
Africa (Cape Town) (af-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID	View AMI ID	View AMI ID

AWS Region	x86	x86 accelerated	Arm
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID	View AMI ID	View AMI ID
Canada (Central) (ca-central-1)	View AMI ID	View AMI ID	View AMI ID
China (Beijing) (cn-north-1)	View AMI ID	View AMI ID	View AMI ID
China (Ningxia) (cn-northwest-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Frankfurt) (eu-central-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Zurich) (eu-central-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Ireland) (eu-west-1)	View AMI ID	View AMI ID	View AMI ID
Europe (London) (eu-west-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Milan) (eu-south-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Spain) (eu-south-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Paris) (eu-west-3)	View AMI ID	View AMI ID	View AMI ID
Europe (Stockholm) (eu-north-1)	View AMI ID	View AMI ID	View AMI ID
Israel (Tel Aviv) (il-central-1)	View AMI ID	View AMI ID	View AMI ID
Middle East (Bahrain) (me-south-1)	View AMI ID	View AMI ID	View AMI ID
Middle East (UAE) (me-central-1)	View AMI ID	View AMI ID	View AMI ID
South America (São Paulo) (sa-east-1)	View AMI ID	View AMI ID	View AMI ID

AWS Region	x86	x86 accelerated	Arm
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID	View AMI ID	View AMI ID
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID	View AMI ID	View AMI ID

1.24

Kubernetes version 1.24

AWS Region	x86	x86 accelerated	Arm
US East (Ohio) (us-east-2)	View AMI ID	View AMI ID	View AMI ID
US East (N. Virginia) (us-east-1)	View AMI ID	View AMI ID	View AMI ID
US West (Oregon) (us-west-2)	View AMI ID	View AMI ID	View AMI ID
US West (N. California) (us-west-1)	View AMI ID	View AMI ID	View AMI ID
Africa (Cape Town) (af-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID	View AMI ID	View AMI ID

AWS Region	x86	x86 accelerated	Arm
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID	View AMI ID	View AMI ID
Canada (Central) (ca-central-1)	View AMI ID	View AMI ID	View AMI ID
China (Beijing) (cn-north-1)	View AMI ID	View AMI ID	View AMI ID
China (Ningxia) (cn-northwest-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Frankfurt) (eu-central-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Zurich) (eu-central-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Ireland) (eu-west-1)	View AMI ID	View AMI ID	View AMI ID
Europe (London) (eu-west-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Milan) (eu-south-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Spain) (eu-south-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Paris) (eu-west-3)	View AMI ID	View AMI ID	View AMI ID
Europe (Stockholm) (eu-north-1)	View AMI ID	View AMI ID	View AMI ID
Israel (Tel Aviv) (il-central-1)	View AMI ID	View AMI ID	View AMI ID
Middle East (Bahrain) (me-south-1)	View AMI ID	View AMI ID	View AMI ID
Middle East (UAE) (me-central-1)	View AMI ID	View AMI ID	View AMI ID
South America (São Paulo) (sa-east-1)	View AMI ID	View AMI ID	View AMI ID
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID	View AMI ID	View AMI ID
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID	View AMI ID	View AMI ID

1.23

Kubernetes version 1.23

AWS Region	x86	x86 accelerated	Arm
US East (Ohio) (us-east-2)	View AMI ID	View AMI ID	View AMI ID
US East (N. Virginia) (us-east-1)	View AMI ID	View AMI ID	View AMI ID
US West (Oregon) (us-west-2)	View AMI ID	View AMI ID	View AMI ID
US West (N. California) (us-west-1)	View AMI ID	View AMI ID	View AMI ID
Africa (Cape Town) (af-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID	View AMI ID	View AMI ID
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID	View AMI ID	View AMI ID
Canada (Central) (ca-central-1)	View AMI ID	View AMI ID	View AMI ID
China (Beijing) (cn-north-1)	View AMI ID	View AMI ID	View AMI ID

AWS Region	x86	x86 accelerated	Arm
China (Ningxia) (cn-northwest-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Frankfurt) (eu-central-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Zurich) (eu-central-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Ireland) (eu-west-1)	View AMI ID	View AMI ID	View AMI ID
Europe (London) (eu-west-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Milan) (eu-south-1)	View AMI ID	View AMI ID	View AMI ID
Europe (Spain) (eu-south-2)	View AMI ID	View AMI ID	View AMI ID
Europe (Paris) (eu-west-3)	View AMI ID	View AMI ID	View AMI ID
Europe (Stockholm) (eu-north-1)	View AMI ID	View AMI ID	View AMI ID
Israel (Tel Aviv) (il-central-1)	View AMI ID	View AMI ID	View AMI ID
Middle East (Bahrain) (me-south-1)	View AMI ID	View AMI ID	View AMI ID
Middle East (UAE) (me-central-1)	View AMI ID	View AMI ID	View AMI ID
South America (São Paulo) (sa-east-1)	View AMI ID	View AMI ID	View AMI ID
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID	View AMI ID	View AMI ID
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID	View AMI ID	View AMI ID

Important

These AMIs require the latest AWS CloudFormation node template. Make sure that you update any existing AWS CloudFormation node stacks with the latest template before you attempt to use these AMIs.

<https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2022-12-23/amazon-eks-nodegroup.yaml>

The AWS CloudFormation node template launches your nodes with Amazon EC2 user data that triggers a specialized [bootstrap script](#). This script allows your nodes to discover and connect to your cluster's control plane automatically. For more information, see [Launching self-managed Amazon Linux nodes \(p. 108\)](#).

Amazon EKS optimized Amazon Linux AMI build script

Amazon Elastic Kubernetes Service (Amazon EKS) has open-source scripts that are used to build the Amazon EKS optimized AMI. These build scripts are available [on GitHub](#).

The Amazon EKS optimized Amazon Linux AMI is built on top of Amazon Linux 2, specifically for use as a node in Amazon EKS clusters. You can use this repository to view the specifics of how the Amazon EKS team configures kubelet, Docker, the AWS IAM Authenticator for Kubernetes, and more.

The build scripts repository includes a [HashiCorp packer](#) template and build scripts to generate an AMI. These scripts are the source of truth for Amazon EKS optimized AMI builds, so you can follow the GitHub repository to monitor changes to our AMIs. For example, perhaps you want your own AMI to use the same version of Docker that the Amazon EKS team uses for the official AMI.

The GitHub repository also contains the specialized [bootstrap script](#) that runs at boot time to configure your instance's certificate data, control plane endpoint, cluster name, and more.

Additionally, the GitHub repository contains our Amazon EKS node AWS CloudFormation templates. These templates make it easier to spin up an instance running the Amazon EKS optimized AMI and register it with a cluster.

For more information, see the repositories on GitHub at <https://github.com/awslabs/amazon-eks-ami>.

Amazon EKS optimized Amazon Linux 2 contains an optional bootstrap flag to enable the `containerd` runtime.

Configuring VT1 for your custom Amazon Linux AMI

Custom Amazon Linux AMIs in Amazon EKS can support the VT1 video transcoding instance family for Amazon Linux 2, Ubuntu 18, and Ubuntu 20. VT1 supports the Xilinx U30 media transcoding cards with accelerated H.264/AVC and H.265/HEVC codecs. To get the benefit of these accelerated instances, you must follow these steps:

1. Create and launch a base AMI from Amazon Linux 2, Ubuntu 18, or Ubuntu 20.
2. After the based AMI is launched, Install the [XRT driver](#) and runtime on the node.
3. [Creating an Amazon EKS cluster \(p. 25\)](#).
4. Install the Kubernetes [FPGA plugin](#) on your cluster.

```
kubectl apply -f fpga-device-plugin.yaml
```

The plugin will now advertise Xilinx U30 devices per node on your Amazon EKS cluster. You can use the FFMPEG docker image to run example video transcoding workloads on your Amazon EKS cluster.

Configuring DL1 for your custom Amazon Linux 2 AMI

Custom Amazon Linux 2 AMIs in Amazon EKS can support deep learning workloads at scale through additional configuration and Kubernetes add-ons. This document describes the components required to set up a generic Kubernetes solution for an on-premise setup or as a baseline in a larger cloud configuration. To support this function, you will have to perform the following steps in your custom environment:

- SynapseAI® Software drivers loaded on the system – These are included in the [AMIs available on Github](#).

The Habana device plugin -- A Daemonset that allows you to automatically enable the registration of Habana devices in your Kubernetes cluster and track device health.

- Helm 3.x
 - [Helm chart to install MPI Operator.](#)
 - MPI Operator
1. Create and launch a base AMI from Amazon Linux 2, Ubuntu 18, or Ubuntu 20.
 2. Follow [these instructions](#) to set up the environment for DL1.

Amazon EKS optimized Bottlerocket AMIs

[Bottlerocket](#) is an open source Linux distribution that's sponsored and supported by AWS. Bottlerocket is purpose-built for hosting container workloads. With Bottlerocket, you can improve the availability of containerized deployments and reduce operational costs by automating updates to your container infrastructure. Bottlerocket includes only the essential software to run containers, which improves resource usage, reduces security threats, and lowers management overhead. The Bottlerocket AMI includes containerd, kubelet, and AWS IAM Authenticator. In addition to managed node groups and self-managed nodes, Bottlerocket is also supported by [Karpenter](#).

Advantages

Using Bottlerocket with your Amazon EKS cluster has the following advantages:

- **Higher uptime with lower operational cost and lower management complexity** – Bottlerocket has a smaller resource footprint, shorter boot times, and is less vulnerable to security threats than other Linux distributions. Bottlerocket's smaller footprint helps to reduce costs by using less storage, compute, and networking resources.
- **Improved security from automatic OS updates** – Updates to Bottlerocket are applied as a single unit which can be rolled back, if necessary. This removes the risk of corrupted or failed updates that can leave the system in an unusable state. With Bottlerocket, security updates can be automatically applied as soon as they're available in a minimally disruptive manner and be rolled back if failures occur.
- **Premium support** – AWS provided builds of Bottlerocket on Amazon EC2 is covered under the same AWS Support plans that also cover AWS services such as Amazon EC2, Amazon EKS, and Amazon ECR.

Considerations

Consider the following when using Bottlerocket for your AMI type:

- Bottlerocket supports Amazon EC2 instances with x86_64 and arm64 processors. The Bottlerocket isn't recommended for use with Amazon EC2 instances with an Inferentia chip.
- Currently, there's no AWS CloudFormation template that you can use to deploy Bottlerocket nodes with.
- Bottlerocket images don't include an SSH server or a shell. You can employ out-of-band access methods to allow SSH. These approaches enable the admin container and to pass some bootstrapping configuration steps with user data. For more information, refer to the following sections in [Bottlerocket OS](#) on GitHub:
 - [Exploration](#)
 - [Admin container](#)
 - [Kubernetes settings](#)

- Bottlerocket uses different container types:
 - By default, a [control container](#) is enabled. This container runs the [AWS Systems Manager agent](#) that you can use to run commands or start shell sessions on Amazon EC2 Bottlerocket instances. For more information, see [Setting up Session Manager](#) in the [AWS Systems Manager User Guide](#).
 - If an SSH key is given when creating the node group, an admin container is enabled. We recommend using the admin container only for development and testing scenarios. We don't recommend using it for production environments. For more information, see [Admin container](#) on GitHub.

More information

For more information about using Amazon EKS optimized Bottlerocket AMIs, see the following sections:

- For details about Bottlerocket, see the [documentation](#) and [releases](#) on GitHub.
- To use Bottlerocket with managed node groups, see [Managed node groups \(p. 81\)](#).
- To launch self-managed Bottlerocket nodes, see [Launching self-managed Bottlerocket nodes \(p. 114\)](#).
- To retrieve the latest IDs of the Amazon EKS optimized Bottlerocket AMIs, see [Retrieving Amazon EKS optimized Bottlerocket AMI IDs \(p. 175\)](#).
- For details on compliance support, see [Bottlerocket compliance support \(p. 184\)](#).

Retrieving Amazon EKS optimized Bottlerocket AMI IDs

You can retrieve the Amazon Machine Image (AMI) ID for Amazon EKS optimized AMIs by querying the AWS Systems Manager Parameter Store API. Using this parameter, you don't need to manually look up Amazon EKS optimized AMI IDs. For more information about the Systems Manager Parameter Store API, see [GetParameter](#). The [IAM principal](#) that you use must have the `ssm:GetParameter` IAM permission to retrieve the Amazon EKS optimized AMI metadata.

You can retrieve the AMI ID with the AWS CLI or the AWS Management Console.

AWS CLI

You can retrieve the image ID of the latest recommended Amazon EKS optimized Bottlerocket AMI with the following AWS CLI command by using the sub-parameter `image_id`. Replace [1.28](#) with a [supported version \(p. 71\)](#) and `region-code` with an [Amazon EKS supported Region](#) for which you want the AMI ID.

```
aws ssm get-parameter --name /aws/service/bottlerocket/aws-k8s-1.28/x86_64/latest/  
image_id --region region-code --query "Parameter.Value" --output text
```

An example output is as follows.

```
ami-1234567890abcdef0
```

AWS Management Console

You can query for the recommended Amazon EKS optimized AMI ID using a URL in the AWS Management Console. The URL opens the Amazon EC2 Systems Manager console with the value of the ID for the parameter. In the following URL, replace [1.28](#) with a [supported version \(p. 71\)](#) and `region-code` with an [Amazon EKS supported Region](#) for which you want the AMI ID.

```
https://console.aws.amazon.com/systems-manager/parameters/aws/service/bottlerocket/aws-k8s-1.28/x86\_64/latest/image\_id?description=region-code
```

The following tables have links to the latest IDs of the Amazon EKS optimized Bottlerocket AMIs.

1.28

Kubernetes version 1.28

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID	N/A	View AMI ID	N/A
China (Ningxia) (cn-northwest-1)	View AMI ID	N/A	View AMI ID	N/A
Europe (Frankfurt) (eu-central-1)	View AMI ID			
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
Europe (Paris) (eu-west-3)	View AMI ID			
Europe (Stockholm) (eu-north-1)	View AMI ID			
Israel (Tel Aviv) (il-central-1)	View AMI ID			
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

1.27

Kubernetes version 1.27

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID	N/A	View AMI ID	N/A
China (Ningxia) (cn-northwest-1)	View AMI ID	N/A	View AMI ID	N/A
Europe (Frankfurt) (eu-central-1)	View AMI ID			
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			
Europe (Paris) (eu-west-3)	View AMI ID			
Europe (Stockholm) (eu-north-1)	View AMI ID			
Israel (Tel Aviv) (il-central-1)	View AMI ID			
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

1.26

Kubernetes version 1.26

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID	N/A	View AMI ID	N/A
China (Ningxia) (cn-northwest-1)	View AMI ID	N/A	View AMI ID	N/A
Europe (Frankfurt) (eu-central-1)	View AMI ID			
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			
Europe (Paris) (eu-west-3)	View AMI ID			
Europe (Stockholm) (eu-north-1)	View AMI ID			
Israel (Tel Aviv) (il-central-1)	View AMI ID			
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

1.25

Kubernetes version 1.25

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID	N/A	View AMI ID	N/A
China (Ningxia) (cn-northwest-1)	View AMI ID	N/A	View AMI ID	N/A
Europe (Frankfurt) (eu-central-1)	View AMI ID			

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			
Europe (Paris) (eu-west-3)	View AMI ID			
Europe (Stockholm) (eu-north-1)	View AMI ID			
Israel (Tel Aviv) (il-central-1)	View AMI ID			
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

1.24

Kubernetes version 1.24

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID	N/A	View AMI ID	N/A
China (Ningxia) (cn-northwest-1)	View AMI ID	N/A	View AMI ID	N/A
Europe (Frankfurt) (eu-central-1)	View AMI ID			
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			
Europe (Paris) (eu-west-3)	View AMI ID			
Europe (Stockholm) (eu-north-1)	View AMI ID			
Israel (Tel Aviv) (il-central-1)	View AMI ID			
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

1.23

Kubernetes version 1.23

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID	N/A	View AMI ID	N/A
China (Ningxia) (cn-northwest-1)	View AMI ID	N/A	View AMI ID	N/A
Europe (Frankfurt) (eu-central-1)	View AMI ID			
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			
Europe (Paris) (eu-west-3)	View AMI ID			

AWS Region	x86 (Standard)	x86 (NVIDIA)	Arm (Standard)	Arm (NVIDIA)
Europe (Stockholm) (eu-north-1)	View AMI ID			
Israel (Tel Aviv) (il-central-1)	View AMI ID			
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

Bottlerocket compliance support

Bottlerocket complies with recommendations defined by various organizations:

- There is a [CIS Benchmark](#) defined for Bottlerocket. In a default configuration, Bottlerocket image has most of the controls required by CIS Level 1 configuration profile. You can implement the controls required for a CIS Level 2 configuration profile. For more information, see [Validating Amazon EKS optimized Bottlerocket AMI against the CIS Benchmark](#) on the AWS blog.
- The optimized feature set and reduced attack surface means that Bottlerocket instances require less configuration to satisfy PCI DSS requirements. The [CIS Benchmark for Bottlerocket](#) is an excellent resource for hardening guidance, and supports your requirements for secure configuration standards under PCI DSS requirement 2.2. You can also leverage [Fluent Bit](#) to support your requirements for operating system level audit logging under PCI DSS requirement 10.2. AWS publishes new (patched) Bottlerocket instances periodically to help you meet PCI DSS requirement 6.2 (for v3.2.1) and requirement 6.3.3 (for v4.0).
- Bottlerocket is an HIPAA-eligible feature authorized for use with regulated workloads for both Amazon EC2 and Amazon EKS. For more information, see the [Architecting for HIPAA Security and Compliance on Amazon EKS](#) whitepaper.

Amazon EKS optimized Ubuntu Linux AMIs

Canonical has partnered with Amazon EKS to create node AMIs that you can use in your clusters.

[Canonical](#) delivers a built-for-purpose Kubernetes Node OS image. This minimized Ubuntu image is optimized for Amazon EKS and includes the custom AWS kernel that is jointly developed with AWS. For more information, see [Ubuntu on Amazon Elastic Kubernetes Service \(EKS\)](#). For information about support, see the [Third-party software](#) section of the [AWS Premium Support FAQs](#).

Amazon EKS optimized Windows AMIs

Windows Amazon EKS optimized AMIs are built on top of Windows Server 2019 and Windows Server 2022. They are configured to serve as the base image for Amazon EKS nodes. By default, the AMIs include the following components:

- [kubelet](#)

- [kube-proxy](#)
- [AWS IAM Authenticator for Kubernetes](#)
- [csi-proxy](#)
- [Docker](#) (only available for Kubernetes version 1.23)

Important

For Windows Amazon EKS optimized AMIs versions that include the Docker component, those that are published in September 2022 or later include the Docker CE (Moby project) runtime instead of the Docker EE (Mirantis) runtime. For more information, see [Amazon ECS and Amazon EKS optimized Amazon Machine Images for Microsoft Windows Server now use Docker CE runtime.](#)

- [containerd](#)

Note

You can track security or privacy events for Windows Server with the [Microsoft security update guide.](#)

Amazon EKS offers AMIs that are optimized for Windows containers in the following variants:

- Amazon EKS-optimized Windows Server 2019 Core AMI
- Amazon EKS-optimized Windows Server 2019 Full AMI
- Amazon EKS-optimized Windows Server 2022 Core AMI
- Amazon EKS-optimized Windows Server 2022 Full AMI

Important

- The Amazon EKS-optimized Windows Server 20H2 Core AMI is deprecated. No new versions of this AMI will be released.
- To ensure that you have the latest security updates by default, Amazon EKS maintains at least the four most recent Windows Amazon EKS-optimized AMIs. After releasing new Windows Amazon EKS-optimized AMIs, Amazon EKS makes the Windows Amazon EKS-optimized AMIs that are older private. If there is a private AMI that you need access to, let us know by filing a ticket with AWS Support.

Release calendar

The following table lists the release and end of support dates for Windows versions on Amazon EKS. If an end date is blank, it's because the version is still supported.

Windows version	Amazon EKS release	Amazon EKS end of support
Windows Server 2022 Core	10/17/2022	
Windows Server 2022 Full	10/17/2022	
Windows Server 20H2 Core	8/12/2021	8/9/2022
Windows Server 2004 Core	8/19/2020	12/14/2021
Windows Server 2019 Core	10/7/2019	
Windows Server 2019 Full	10/7/2019	
Windows Server 1909 Core	10/7/2019	12/8/2020

Bootstrap script configuration parameters

When you create a Windows node, there's a script on the node that allows for configuring different parameters. Depending on your setup, this script can be found on the node at a location similar to: C:\Program Files\Amazon\EKS\Start-EKSBootstrap.ps1. You can specify custom parameter values by specifying them as arguments to the bootstrap script. For example, you can update the user data in the launch template. For more information, see [Amazon EC2 user data \(p. 100\)](#).

The script includes the following parameters:

- -EKSClusterName – Specifies the Amazon EKS cluster name for this worker node to join.
- -KubeletExtraArgs – Specifies extra arguments for kubelet (optional).
- -KubeProxyExtraArgs – Specifies extra arguments for kube-proxy (optional).
- -APIServerEndpoint – Specifies the Amazon EKS cluster API server endpoint (optional). Only valid when used with -Base64ClusterCA. Bypasses calling Get-EKSCluster.
- -Base64ClusterCA – Specifies the base64 encoded cluster CA content (optional). Only valid when used with -APIServerEndpoint. Bypasses calling Get-EKSCluster.
- -DNSClusterIP – Overrides the IP address to use for DNS queries within the cluster (optional). Defaults to 10.100.0.10 or 172.20.0.10 based on the IP address of the primary interface.
- -ContainerRuntime – Specifies the container runtime to be used on the node.
- -ServiceCIDR – Overrides the Kubernetes service IP address range from which cluster services are addressed. Defaults to 172.20.0.0/16 or 10.100.0.0/16 based on the IP address of the primary interface.
- -ExcludedSnatCIDRs – A list of IPv4 CIDRs to exclude from Source Network Address Translation (SNAT). This means that the pod private IP which is VPC addressable wouldn't be translated to the IP address of the instance ENI's primary IPv4 address for outbound traffic. By default, the IPv4 CIDR of the VPC for the Amazon EKS Windows node is added. Specifying CIDRs to this parameter also additionally excludes the specified CIDRs. For more information, see [SNAT for Pods \(p. 289\)](#).

Enable the containerd runtime bootstrap flag

For Kubernetes version 1.23, you can use an optional bootstrap flag to enable the containerd runtime for Amazon EKS optimized Windows AMIs. This feature gives you a clear path to migrate to containerd when updating to version 1.24 or later. Amazon EKS ended support for Docker starting with the Kubernetes version 1.24 launch. For more information, see [Amazon EKS ended support for Dockershim \(p. 155\)](#).

For Amazon EKS version 1.23, the supported values for the container runtime are docker and containerd. The container runtime is specified when launching the Windows nodes using either eksctl or the AWS Management Console.

- If the specified value is docker and the Amazon EKS version is 1.23, then Docker is used as the runtime on the node.
- If any other value is specified, then the bootstrap fails and the node isn't able to join the cluster.
- If this flag isn't specified, then the default value of the container runtime is selected. For Amazon EKS version 1.23 and earlier, the default is Docker. For 1.24 and later clusters, it is containerd.

When launching Windows nodes in your Amazon EKS cluster, follow the steps in [Launching self-managed Windows nodes \(p. 117\)](#). Windows self-managed nodes with the containerd runtime can be launched using eksctl or the AWS Management Console.

eksctl

To enable the containerd runtime with eksctl

For Windows self-managed nodes, the container runtime can be specified in the configuration while creating new node groups. You can use the following `test-windows-with-containerd.yaml` as reference.

Note

You must use `eksctl` version [0.95.0](#) or later to use the `ContainerRuntime` setting in the configuration file.

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: windows-containerd-cluster
  region: us-west-2
  version: 'X.XX'

nodeGroups:
  - name: windows-ng
    instanceType: m5.2xlarge
    amiFamily: WindowsServer2019FullContainer
    volumeSize: 100
    minSize: 2
    maxSize: 3
    containerRuntime: containerd
  - name: linux-ng
    amiFamily: AmazonLinux2
    minSize: 2
    maxSize: 3
```

The node groups can then be created using the following command.

```
eksctl create cluster -f test-windows-with-containerd.yaml
```

Note

Starting with `eksctl` version 0.95, you can no longer use `preBootstrapCommands` to configure `ContainerRuntime` for Windows nodes.

For more information, see [Creating a nodegroup from a config file](#), [defining containerd runtime](#), and [Config file schema](#) in the `eksctl` documentation.

AWS Management Console

To enable the `containerd` runtime with the AWS Management Console

In the AWS CloudFormation template, there's a parameter named `BootstrapArguments` which can be used to pass in additional arguments to the bootstrap script. A parameter named `ContainerRuntime` can be used to select a particular runtime on the node.

Specify the following in `BootstrapArguments` to enable the `containerd` runtime:

```
-ContainerRuntime containerd
```

Launch self-managed Windows Server 2022 nodes with `eksctl`

Amazon EKS optimized Windows Server 2022 AMIs are available for Kubernetes version 1.23 or higher. You can use the following `test-windows-2022.yaml` as reference for running Windows Server 2022 as self-managed nodes.

Note

You must use eksctl version [0.116.0](#) or later to run self-managed Windows Server 2022 nodes.

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: windows-2022-cluster
  region: us-west-2
  version: '1.23'

nodeGroups:
  - name: windows-ng
    instanceType: m5.2xlarge
    amiFamily: WindowsServer2022FullContainer
    volumeSize: 100
    minSize: 2
    maxSize: 3
  - name: linux-ng
    amiFamily: AmazonLinux2
    minSize: 2
    maxSize: 3
```

The node groups can then be created using the following command.

```
eksctl create cluster -f test-windows-2022.yaml
```

gMSA authentication support

Amazon EKS Windows Pods allow different types of group Managed Service Account (gMSA) authentication.

- Amazon EKS supports Active Directory domain identities for authentication. For more information on domain-joined gMSA, see [Windows Authentication on Amazon EKS Windowspods](#) on the AWS blog.
- Amazon EKS offers a plugin that enables non-domain-joined Windows nodes to retrieve gMSA credentials with a portable user identity. For more information on domainless gMSA, see [Domainless Windows Authentication for Amazon EKS Windowspods](#) on the AWS blog.

Cached container images

Amazon EKS Windows optimized AMIs have certain container images cached for both the docker and containerd runtimes. Container images are cached when building custom AMIs using Amazon-managed build components. For more information, see [Using the Amazon-managed build component \(p. 226\)](#).

For Amazon EKS 1.23 and lower

The docker runtime is the default and has the following container images cached on Amazon EKS Windows AMIs. Retrieve this image list by running docker images on the Amazon EKS Windows node:

- `amazonaws.com/eks/pause-windows`
- `mcr.microsoft.com/windows/nanoserver`
- `mcr.microsoft.com/windows/servercore`

The containerd runtime only has one container image. Retrieve this image list by running `ctr -n k8s.io images list`:

- `amazonaws.com/eks/pause-windows`

For Amazon EKS 1.24 and higher

There is no docker runtime. The following cached container images are for the containerd runtime:

- `amazonaws.com/eks/pause-windows`
- `mcr.microsoft.com/windows/nanoserver`
- `mcr.microsoft.com/windows/servercore`

More information

For more information about using Amazon EKS optimized Windows AMIs, see the following sections:

- To use Windows with managed node groups, see [Managed node groups \(p. 81\)](#).
- To launch self-managed Windows nodes, see [Launching self-managed Windows nodes \(p. 117\)](#).
- For version information, see [Amazon EKS optimized Windows AMI versions \(p. 189\)](#).
- To retrieve the latest IDs of the Amazon EKS optimized Windows AMIs, see [Retrieving Amazon EKS optimized Windows AMI IDs \(p. 211\)](#).
- To use Amazon EC2 Image Builder to create custom Amazon EKS optimized Windows AMIs, see [Creating custom Amazon EKS optimized Windows AMIs \(p. 225\)](#).

Amazon EKS optimized Windows AMI versions

This topic lists versions of the Amazon EKS optimized Windows AMIs and their corresponding versions of `kubelet`, `Docker` (only available for Kubernetes version 1.23), `containerd`, and `csi-proxy`.

The Amazon EKS optimized AMI metadata, including the AMI ID, for each variant can be retrieved programmatically. For more information, see [Retrieving Amazon EKS optimized Windows AMI IDs \(p. 211\)](#).

AMIs are versioned by Kubernetes version and the release date of the AMI in the following format:

`k8s_major_version.k8s_minor_version-release_date`

Note

Amazon EKS managed node groups support the November 2022 and later releases of the Windows AMIs.

Amazon EKS optimized Windows Server 2022 Core AMI

The following tables list the current and previous versions of the Amazon EKS optimized Windows Server 2022 Core AMI.

Kubernetes version 1.28

Kubernetes version 1.28

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.28-2023-09-27	1.28.2	1.6.6	1.1.2	Fixed a security advisory in kubelet.
1.28-2023.09.12	1.28.1	1.6.6	1.1.2	

Kubernetes version 1.27

Kubernetes version 1.27

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.27-2023-09-27	1.27.6	1.6.6	1.1.2	Fixed a security advisory in kubelet.
1.27-2023.09.12	1.27.4	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.27-2023.08.17	1.27.4	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.27-2023.08.08	1.27.3	1.6.6	1.1.1	
1.27-2023.07.11	1.27.3	1.6.6	1.1.1	
1.27-2023.06.20	1.27.1	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.27-2023.06.14	1.27.1	1.6.6	1.1.1	Added support for host port mapping in CNI. Merged pull request #93 .
1.27-2023.06.06	1.27.1	1.6.6	1.1.1	Fixed containers-roadmap issue #2042 , which caused nodes to fail pulling private Amazon ECR images.
1.27-2023.05.17	1.27.1	1.6.6	1.1.1	

Kubernetes version 1.26

Kubernetes version 1.26

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.26-2023.09.12	1.26.7	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.26-2023.08.17	1.26.7	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.26-2023.08.08	1.26.6	1.6.6	1.1.1	
1.26-2023.07.11	1.26.6	1.6.6	1.1.1	
1.26-2023.06.20	1.26.4	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.26-2023.06.14	1.26.4	1.6.6	1.1.1	Upgraded Kubernetes to 1.26.4. Added support for host port mapping in CNI. Merged pull request #93 .
1.26-2023.05.09	1.26.2	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.26-2023.04.26	1.26.2	1.6.6	1.1.1	
1.26-2023.04.11	1.26.2	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.26-2023.03.24	1.26.2	1.6.6	1.1.1	

Kubernetes version 1.25

Kubernetes version 1.25

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.25-2023.09.12	1.25.12	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets

AMI version	kubelet version	container version	csi-proxy version	Release notes
				the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.25-2023.08.17	1.25.12	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.25-2023.08.08	1.25.9	1.6.6	1.1.1	
1.25-2023.07.11	1.25.9	1.6.6	1.1.1	
1.25-2023.06.20	1.25.9	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.25-2023.06.14	1.25.9	1.6.6	1.1.1	Upgraded Kubernetes to 1.25.9. Added support for host port mapping in CNI. Merged pull request #93 .
1.25-2023.05.09	1.25.7	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.25-2023.04.11	1.25.7	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.25-2023.03.27	1.25.6	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.
1.25-2023.03.20	1.25.6	1.6.6	1.1.1	
1.25-2023.02.14	1.25.6	1.6.6	1.1.1	

Kubernetes version 1.24

Kubernetes version 1.24

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.24-2023.09.12	1.24.16	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the

AMI version	kubelet version	container version	csi-proxy version	Release notes
				Kubernetes API server. Merged pull request #100 .
1.24-2023.08.17	1.24.16	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.24-2023.08.08	1.24.13	1.6.6	1.1.1	
1.24-2023.07.11	1.24.13	1.6.6	1.1.1	
1.24-2023.06.20	1.24.13	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.24-2023.06.14	1.24.13	1.6.6	1.1.1	Upgraded Kubernetes to 1.24.13. Added support for host port mapping in CNI. Merged pull request #93 .
1.24-2023.05.09	1.24.7	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.24-2023.04.11	1.24.7	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.24-2023.03.27	1.24.7	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.
1.24-2023.03.20	1.24.7	1.6.6	1.1.1	Kubernetes version downgraded to 1.24.7 because 1.24.10 has a reported issue in kube-proxy.
1.24-2023.02.14	1.24.10	1.6.6	1.1.1	
1.24-2023.01.23	1.24.7	1.6.6	1.1.1	
1.24-2023.01.11	1.24.7	1.6.6	1.1.1	
1.24-2022.12.13	1.24.7	1.6.6	1.1.1	
1.24-2022.10.11	1.24.7	1.6.6	1.1.1	

Kubernetes version 1.23

Kubernetes version 1.23

AMI version	kubelet version	Docker version	container version	csi-proxy version	Release notes
1.23-2023.09.12	1.23.17	20.10.21	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.23-2023.08.17	1.23.17	20.10.21	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.23-2023.08.08	1.23.17	20.10.21	1.6.6	1.1.1	
1.23-2023.07.11	1.23.17	10.10.21	1.6.6	1.1.1	
1.23-2023.06.20	1.23.17	20.10.21	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.23-2023.06.14	1.23.17	20.10.21	1.6.6	1.1.1	Added support for host port mapping in CNI. Merged pull request #93 .
1.23-2023.05.09	1.23.17	20.10.21	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.23-2023.04.11	1.23.17	20.10.21	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.23-2023.03.27	1.23.16	20.10.21	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.
1.23-2023.03.20	1.23.16	20.10.21	1.6.6	1.1.1	
1.23-2023.02.14	1.23.16	20.10.21	1.6.6	1.1.1	
1.23-2023.01.23	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2023.01.11	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2022.12.13	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2022.11.08	1.23.12	20.10.21	1.6.6	1.1.1	

AMI version	kubelet version	Docker version	container version	csi-proxy version	Release notes
1.23-2022.10.11	1.23.12	20.10.17	1.6.6	1.1.1	

Amazon EKS optimized Windows Server 2022 Full AMI

The following tables list the current and previous versions of the Amazon EKS optimized Windows Server 2022 Full AMI.

Kubernetes version 1.28

Kubernetes version 1.28

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.28-2023-09-27	1.28.2	1.6.6	1.1.2	Fixed a security advisory in kubelet.
1.28-2023.09.12	1.28.1	1.6.6	1.1.2	

Kubernetes version 1.27

Kubernetes version 1.27

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.27-2023-09-27	1.27.6	1.6.6	1.1.2	Fixed a security advisory in kubelet.
1.27-2023.09.12	1.27.4	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.27-2023.08.17	1.27.4	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.27-2023.08.08	1.27.3	1.6.6	1.1.1	
1.27-2023.07.11	1.27.3	1.6.6	1.1.1	
1.27-2023.06.20	1.27.1	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.27-2023.06.14	1.27.1	1.6.6	1.1.1	Added support for host port mapping in CNI. Merged pull request #93 .
1.27-2023.06.06	1.27.1	1.6.6	1.1.1	Fixed containers-roadmap issue #2042 , which caused nodes to fail pulling private Amazon ECR images.
1.27-2023.05.18	1.27.1	1.6.6	1.1.1	

Kubernetes version 1.26

Kubernetes version 1.26

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.26-2023.09.12	1.26.7	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.26-2023.08.17	1.26.7	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.26-2023.08.08	1.26.6	1.6.6	1.1.1	
1.26-2023.07.11	1.26.6	1.6.6	1.1.1	
1.26-2023.06.20	1.26.4	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.26-2023.06.14	1.26.4	1.6.6	1.1.1	Upgraded Kubernetes to 1.26.4. Added support for host port mapping in CNI. Merged pull request #93 .
1.26-2023.05.09	1.26.2	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.26-2023.04.26	1.26.2	1.6.6	1.1.1	

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.26-2023.04.11	1.26.2	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.26-2023.03.24	1.26.2	1.6.6	1.1.1	

Kubernetes version 1.25

Kubernetes version 1.25

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.25-2023.09.12	1.25.12	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.25-2023.08.17	1.25.12	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.25-2023.08.08	1.25.9	1.6.6	1.1.1	
1.25-2023.07.11	1.25.9	1.6.6	1.1.1	
1.25-2023.06.20	1.25.9	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.25-2023.06.14	1.25.9	1.6.6	1.1.1	Upgraded Kubernetes to 1.25.9. Added support for host port mapping in CNI. Merged pull request #93 .
1.25-2023.05.09	1.25.7	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.25-2023.04.11	1.25.7	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.25-2023.03.27	1.25.6	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.25-2023.03.20	1.25.6	1.6.6	1.1.1	
1.25-2023.02.14	1.25.6	1.6.6	1.1.1	

Kubernetes version 1.24

Kubernetes version 1.24

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.24-2023.09.12	1.24.16	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.24-2023.08.17	1.24.16	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.24-2023.08.08	1.24.13	1.6.6	1.1.1	
1.24-2023.07.11	1.24.13	1.6.6	1.1.1	
1.24-2023.06.20	1.24.13	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.24-2023.06.14	1.24.13	1.6.6	1.1.1	Upgraded Kubernetes to 1.24.13. Added support for host port mapping in CNI. Merged pull request #93 .
1.24-2023.05.09	1.24.7	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.24-2023.04.11	1.24.7	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.24-2023.03.27	1.24.7	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.24-2023.03.20	1.24.7	1.6.6	1.1.1	Kubernetes version downgraded to 1.24.7 because 1.24.10 has a reported issue in kube-proxy.
1.24-2023.02.14	1.24.10	1.6.6	1.1.1	
1.24-2023.01.23	1.24.7	1.6.6	1.1.1	
1.24-2023.01.11	1.24.7	1.6.6	1.1.1	
1.24-2022.12.14	1.24.7	1.6.6	1.1.1	
1.24-2022.10.11	1.24.7	1.6.6	1.1.1	

Kubernetes version 1.23

Kubernetes version 1.23

AMI version	kubelet version	Docker version	container version	csi-proxy version	Release notes
1.23-2023.09.12	1.23.17	20.10.21	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.23-2023.08.17	1.23.17	20.10.21	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.23-2023.08.08	1.23.17	20.10.21	1.6.6	1.1.1	
1.23-2023.07.11	1.23.17	20.10.21	1.6.6	1.1.1	
1.23-2023.06.20	1.23.17	20.10.21	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.23-2023.06.14	1.23.17	20.10.21	1.6.6	1.1.1	Added support for host port mapping in CNI. Merged pull request #93 .
1.23-2023.05.09	1.23.17	20.10.21	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (<code>ExcludedSnatCIDRs</code>).

AMI version	kubelet version	Docker version	container version	csi-proxy version	Release notes
1.23-2023.04.11	1.23.17	20.10.21	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.23-2023.03.27	1.23.16	20.10.21	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.
1.23-2023.03.20	1.23.16	20.10.21	1.6.6	1.1.1	
1.23-2023.02.14	1.23.16	20.10.21	1.6.6	1.1.1	
1.23-2023.01.23	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2023.01.11	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2022.12.14	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2022.11.08	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2022.10.11	1.23.12	20.10.17	1.6.6	1.1.1	

Amazon EKS optimized Windows Server 2019 Core AMI

The following tables list the current and previous versions of the Amazon EKS optimized Windows Server 2019 Core AMI.

Kubernetes version 1.28

Kubernetes version 1.28

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.28-2023-09-27	1.28.2	1.6.6	1.1.2	Fixed a security advisory in kubelet.
1.28-2023.09.12	1.28.1	1.6.6	1.1.2	

Kubernetes version 1.27

Kubernetes version 1.27

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.27-2023-09-27	1.27.6	1.6.6	1.1.2	Fixed a security advisory in kubelet.
1.27-2023.09.12	1.27.4	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes

AMI version	kubelet version	container version	csi-proxy version	Release notes
				connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.27-2023.08.17	1.27.4	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.27-2023.08.08	1.27.3	1.6.6	1.1.1	
1.27-2023.07.11	1.27.3	1.6.6	1.1.1	
1.27-2023.06.20	1.27.1	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.27-2023.06.14	1.27.1	1.6.6	1.1.1	Added support for host port mapping in CNI. Merged pull request #93 .
1.27-2023.06.06	1.27.1	1.6.6	1.1.1	Fixed containers-roadmap issue #2042 , which caused nodes to fail pulling private Amazon ECR images.
11.27-2023.05.18	1.27.1	1.6.6	1.1.1	

Kubernetes version 1.26

Kubernetes version 1.26

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.26-2023.09.12	1.26.7	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.26-2023.08.17	1.26.7	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.26-2023.08.08	1.26.6	1.6.6	1.1.1	
1.26-2023.07.11	1.26.6	1.6.6	1.1.1	

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.26-2023.06.20	1.26.4	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.26-2023.06.14	1.26.4	1.6.6	1.1.1	Upgraded Kubernetes to 1.26.4. Added support for host port mapping in CNI. Merged pull request #93 .
1.26-2023.05.09	1.26.2	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.26-2023.04.26	1.26.2	1.6.6	1.1.1	
1.26-2023.04.11	1.26.2	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.26-2023.03.24	1.26.2	1.6.6	1.1.1	

Kubernetes version 1.25

Kubernetes version 1.25

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.25-2023.09.12	1.25.12	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.25-2023.08.17	1.25.12	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.25-2023.08.08	1.25.9	1.6.6	1.1.1	
1.25-2023.07.11	1.25.9	1.6.6	1.1.1	
1.25-2023.06.20	1.25.9	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.25-2023.06.14	1.25.9	1.6.6	1.1.1	Upgraded Kubernetes to 1.25.9. Added support for host port

AMI version	kubelet version	container version	csi-proxy version	Release notes
				mapping in CNI. Merged pull request #93 .
1.25-2023.05.09	1.25.7	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.25-2023.04.11	1.25.7	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.25-2023.03.27	1.25.6	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.
1.25-2023.03.20	1.25.6	1.6.6	1.1.1	
1.25-2023.02.14	1.25.6	1.6.6	1.1.1	

Kubernetes version 1.24

Kubernetes version 1.24

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.24-2023.09.12	1.24.16	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.24-2023.08.17	1.24.16	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.24-2023.08.08	1.24.13	1.6.6	1.1.1	
1.24-2023.07.11	1.24.13	1.6.6	1.1.1	
1.24-2023.06.20	1.24.13	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.24-2023.06.14	1.24.13	1.6.6	1.1.1	Upgraded Kubernetes to 1.24.13. Added support for host port

AMI version	kubelet version	container version	csi-proxy version	Release notes
				mapping in CNI. Merged pull request #93 .
1.24-2023.05.09	1.24.7	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.24-2023.04.11	1.24.7	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.24-2023.03.27	1.24.7	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.
1.24-2023.03.20	1.24.7	1.6.6	1.1.1	Kubernetes version downgraded to 1.24.7 because 1.24.10 has a reported issue in kube-proxy.
1.24-2023.02.14	1.24.10	1.6.6	1.1.1	
1.24-2023.01.23	1.24.7	1.6.6	1.1.1	
1.24-2023.01.11	1.24.7	1.6.6	1.1.1	
1.24-2022.12.13	1.24.7	1.6.6	1.1.1	
1.24-2022.11.08	1.24.7	1.6.6	1.1.1	

Kubernetes version 1.23

Kubernetes version 1.23

AMI version	kubelet version	Docker version	container version	csi-proxy version	Release notes
1.23-2023.09.12	1.23.17	20.10.21	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.23-2023.08.17	1.23.17	20.10.21	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.23-2023.08.08	1.23.17	20.10.21	1.6.6	1.1.1	

AMI version	kubelet version	Docker version	container version	csi-proxy version	Release notes
1.23-2023.07.11	1.23.17	20.10.21	1.6.6	1.1.1	
1.23-2023.06.20	1.23.17	20.10.21	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.23-2023.06.14	1.23.17	20.10.21	1.6.6	1.1.1	Added support for host port mapping in CNI. Merged pull request #93 .
1.23-2023.05.09	1.23.17	20.10.21	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.23-2023.04.11	1.23.17	20.10.21	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.23-2023.03.27	1.23.16	20.10.21	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.
1.23-2023.03.20	1.23.16	20.10.21	1.6.6	1.1.1	
1.23-2023.02.14	1.23.16	20.10.21	1.6.6	1.1.1	
1.23-2023.01.23	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2023.01.11	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2022.12.14	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2022.11.08	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2022.10.12	1.23.12	20.10.17	1.6.6	1.1.1	
1.23-2022.10.12	1.23.12	20.10.17	1.6.6	1.1.1	
1.23-2022.09.13	1.23.9	20.10.17	1.6.6	1.1.1	
1.23-2022.08.09	1.23.7	20.10.9	1.6.2	1.1.1	

Amazon EKS optimized Windows Server 2019 Full AMI

The following tables list the current and previous versions of the Amazon EKS optimized Windows Server 2019 Full AMI.

Kubernetes version 1.28

Kubernetes version 1.28

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.28-2023-09-27	1.28.2	1.6.6	1.1.2	Fixed a security advisory in kubelet.
1.28-2023.09.12	1.28.1	1.6.6	1.1.2	

Kubernetes version 1.27

Kubernetes version 1.27

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.27-2023-09-27	1.27.6	1.6.6	1.1.2	Fixed a security advisory in kubelet.
1.27-2023.09.12	1.27.4	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.27-2023.08.17	1.27.4	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.27-2023.08.08	1.27.3	1.6.6	1.1.1	
1.27-2023.07.11	1.27.3	1.6.6	1.1.1	
1.27-2023.06.20	1.27.1	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.27-2023.06.14	1.27.1	1.6.6	1.1.1	Added support for host port mapping in CNI. Merged pull request #93 .
1.27-2023.06.06	1.27.1	1.6.6	1.1.1	Fixed containers-roadmap issue #2042 , which caused nodes to fail pulling private Amazon ECR images.
1.27-2023.05.17	1.27.1	1.6.6	1.1.1	

Kubernetes version 1.26

Kubernetes version 1.26

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.26-2023.09.12	1.26.7	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.26-2023.08.17	1.26.7	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.26-2023.08.08	1.26.6	1.6.6	1.1.1	
1.26-2023.07.11	1.26.6	1.6.6	1.1.1	
1.26-2023.06.20	1.26.4	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.26-2023.06.14	1.26.4	1.6.6	1.1.1	Upgraded Kubernetes to 1.26.4. Added support for host port mapping in CNI. Merged pull request #93 .
1.26-2023.05.09	1.26.2	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.26-2023.04.26	1.26.2	1.6.6	1.1.1	
1.26-2023.04.11	1.26.2	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.26-2023.03.24	1.26.2	1.6.6	1.1.1	

Kubernetes version 1.25

Kubernetes version 1.25

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.25-2023.09.12	1.25.12	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets

AMI version	kubelet version	container version	csi-proxy version	Release notes
				the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.25-2023.08.17	1.25.12	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.25-2023.08.08	1.25.9	1.6.6	1.1.1	
1.25-2023.07.11	1.25.9	1.6.6	1.1.1	
1.25-2023.06.20	1.25.9	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.25-2023.06.14	1.25.9	1.6.6	1.1.1	Upgraded Kubernetes to 1.25.9. Added support for host port mapping in CNI. Merged pull request #93 .
1.25-2023.05.09	1.25.7	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.25-2023.04.11	1.25.7	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.25-2023.03.27	1.25.6	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.
1.25-2023.03.20	1.25.6	1.6.6	1.1.1	
1.25-2023.02.14	1.25.6	1.6.6	1.1.1	

Kubernetes version 1.24

Kubernetes version 1.24

AMI version	kubelet version	container version	csi-proxy version	Release notes
1.24-2023.09.12	1.24.16	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the

AMI version	kubelet version	container version	csi-proxy version	Release notes
				Kubernetes API server. Merged pull request #100 .
1.24-2023.08.17	1.24.16	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.24-2023.08.08	1.24.13	1.6.6	1.1.1	
1.24-2023.07.11	1.24.13	1.6.6	1.1.1	
1.24-2023.06.21	1.24.13	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.24-2023.06.14	1.24.13	1.6.6	1.1.1	Upgraded Kubernetes to 1.24.13. Added support for host port mapping in CNI. Merged pull request #93 .
1.24-2023.05.09	1.24.7	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.24-2023.04.11	1.24.7	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.24-2023.03.27	1.24.7	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.
1.24-2023.03.20	1.24.7	1.6.6	1.1.1	Kubernetes version downgraded to 1.24.7 because 1.24.10 has a reported issue in kube-proxy.
1.24-2023.02.14	1.24.10	1.6.6	1.1.1	
1.24-2023.01.23	1.24.7	1.6.6	1.1.1	
1.24-2023.01.11	1.24.7	1.6.6	1.1.1	
1.24-2022.12.14	1.24.7	1.6.6	1.1.1	
1.24-2022.10.12	1.24.7	1.6.6	1.1.1	

Kubernetes version 1.23

Kubernetes version 1.23

AMI version	kubelet version	Docker version	container version	csi-proxy version	Release notes
1.23-2023.09.12	1.23.17	20.10.21	1.6.6	1.1.2	Upgraded the Amazon VPC CNI plugin to use the Kubernetes connector binary, which gets the Pod IP address from the Kubernetes API server. Merged pull request #100 .
1.23-2023.08.17	1.23.17	20.10.21	1.6.6	1.1.2	Includes patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955.
1.23-2023.08.08	1.23.17	20.10.21	1.6.6	1.1.1	
1.23-2023.07.11	1.23.17	20.10.21	1.6.6	1.1.1	
1.23-2023.06.20	1.23.17	20.10.21	1.6.6	1.1.1	Resolved issue that was causing the DNS suffix search list to be incorrectly populated.
1.23-2023.06.14	1.23.17	20.10.21	1.6.6	1.1.1	Added support for host port mapping in CNI. Merged pull request #93 .
1.23-2023.05.09	1.23.17	20.10.21	1.6.6	1.1.1	Fixed a bug causing network connectivity issue #1126 on pods after node restart. Introduced a new bootstrap script configuration parameter (p. 186) (ExcludedSnatCIDRs).
1.23-2023.04.11	1.23.17	20.10.21	1.6.6	1.1.1	Added recovery mechanism for kubelet and kube-proxy on service crash.
1.23-2023.03.27	1.23.16	20.10.21	1.6.6	1.1.1	Installed a domainless gMSA plugin to facilitate gMSA authentication for Windows containers on Amazon EKS.
1.23-2023.03.20	1.23.16	20.10.21	1.6.6	1.1.1	
1.23-2023.02.14	1.23.16	20.10.21	1.6.6	1.1.1	
1.23-2023.01.23	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2023.01.11	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2022.12.14	1.23.12	20.10.21	1.6.6	1.1.1	
1.23-2022.11.08	1.23.12	20.10.21	1.6.6	1.1.1	

AMI version	kubelet version	Docker version	container version	csi-proxy version	Release notes
1.23-2022.10.12	1.23.12	20.10.17	1.6.6	1.1.1	
1.23-2022.09.13	1.23.9	20.10.17	1.6.6	1.1.1	
1.23-2022.08.09	1.23.7	20.10.9	1.6.2	1.1.1	

Retrieving Amazon EKS optimized Windows AMI IDs

You can programmatically retrieve the Amazon Machine Image (AMI) ID for Amazon EKS optimized AMIs by querying the AWS Systems Manager Parameter Store API. This parameter eliminates the need for you to manually look up Amazon EKS optimized AMI IDs. For more information about the Systems Manager Parameter Store API, see [GetParameter](#). The [IAM principal](#) that you use must have the `ssm:GetParameter` IAM permission to retrieve the Amazon EKS optimized AMI metadata.

You can retrieve the AMI ID with the AWS CLI or the AWS Management Console.

AWS CLI

You can retrieve the image ID of the latest recommended Amazon EKS optimized Windows AMI with the following command by using the sub-parameter `image_id`. You can replace `1.28` with any supported Amazon EKS version and can replace `region-code` with an [Amazon EKS supported Region](#) for which you want the AMI ID. Replace `Core` with `Full` to see the Windows Server full AMI ID. For Kubernetes version 1.23 or later, you can replace `2019` with `2022` to see the Windows Server 2022 AMI ID.

```
aws ssm get-parameter --name /aws/service/ami-windows-latest/Windows_Server-2019-English-Core-EKS_Optimized-1.28/image_id --region region-code --query "Parameter.Value" --output text
```

An example output is as follows.

```
ami-1234567890abcdef0
```

AWS Management Console

You can query for the recommended Amazon EKS optimized AMI ID using a URL. The URL opens the Amazon EC2 Systems Manager console with the value of the ID for the parameter. In the following URL, you can replace `1.27` with any supported Amazon EKS version and can replace `region-code` with an [Amazon EKS supported Region](#) for which you want the AMI ID. Replace `Core` with `Full` to see the Windows Server full AMI ID. For Kubernetes version 1.23 or later, you can replace `2019` with `2022` to see the Windows Server 2022 AMI ID.

```
https://console.aws.amazon.com/systems-manager/parameters/aws/service/ami-windows-latest/Windows_Server-2019-English-Core-EKS_Optimized-1.28/image_id?description?region=region-code
```

The following tables have links to the latest IDs of the Amazon EKS optimized Windows AMIs.

Both Windows Server 2019 and Windows Server 2022 are Long-Term Servicing Channel (LTSC) releases, whereas Versions 20H2 is a Semi-Annual Channel (SAC) release. We no longer support SAC releases. For more information about these release types, see [Windows Server release information](#) in the Microsoft

documentation. For more information about Windows OS version support, see [Intro to Windows support in Kubernetes](#).

1.28

Kubernetes version 1.28

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID			
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID			
China (Ningxia) (cn-northwest-1)	View AMI ID			
Europe (Frankfurt) (eu-central-1)	View AMI ID			
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			
Europe (Paris) (eu-west-3)	View AMI ID			
Europe (Stockholm) (eu-north-1)	View AMI ID			
Israel (Tel Aviv) (il-central-1)	View AMI ID			
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

1.27

Kubernetes version 1.27

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID			
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID			
China (Ningxia) (cn-northwest-1)	View AMI ID			
Europe (Frankfurt) (eu-central-1)	View AMI ID			
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			
Europe (Paris) (eu-west-3)	View AMI ID			
Europe (Stockholm) (eu-north-1)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
Israel (Tel Aviv) (il-central-1)	View AMI ID			
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

1.26

Kubernetes version 1.26

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID			
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID			
China (Ningxia) (cn-northwest-1)	View AMI ID			
Europe (Frankfurt) (eu-central-1)	View AMI ID			
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			
Europe (Paris) (eu-west-3)	View AMI ID			
Europe (Stockholm) (eu-north-1)	View AMI ID			
Israel (Tel Aviv) (il-central-1)	View AMI ID			
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

1.25

Kubernetes version 1.25

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID			
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID			
China (Ningxia) (cn-northwest-1)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
Europe (Frankfurt) (eu-central-1)	View AMI ID			
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			
Europe (Paris) (eu-west-3)	View AMI ID			
Europe (Stockholm) (eu-north-1)	View AMI ID			
Israel (Tel Aviv) (il-central-1)	View AMI ID			
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

1.24

Kubernetes version 1.24

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID			
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID			
China (Ningxia) (cn-northwest-1)	View AMI ID			
Europe (Frankfurt) (eu-central-1)	View AMI ID			
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			
Europe (Paris) (eu-west-3)	View AMI ID			
Europe (Stockholm) (eu-north-1)	View AMI ID			
Israel (Tel Aviv) (il-central-1)	View AMI ID			
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

1.23

Kubernetes version 1.23

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
US East (Ohio) (us-east-2)	View AMI ID			
US East (N. Virginia) (us-east-1)	View AMI ID			
US West (Oregon) (us-west-2)	View AMI ID			
US West (N. California) (us-west-1)	View AMI ID			
Africa (Cape Town) (af-south-1)	View AMI ID			
Asia Pacific (Hong Kong) (ap-east-1)	View AMI ID			
Asia Pacific (Mumbai) (ap-south-1)	View AMI ID			
Asia Pacific (Hyderabad) (ap-south-2)	View AMI ID			
Asia Pacific (Tokyo) (ap-northeast-1)	View AMI ID			
Asia Pacific (Seoul) (ap-northeast-2)	View AMI ID			
Asia Pacific (Osaka) (ap-northeast-3)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
Asia Pacific (Singapore) (ap-southeast-1)	View AMI ID			
Asia Pacific (Sydney) (ap-southeast-2)	View AMI ID			
Asia Pacific (Jakarta) (ap-southeast-3)	View AMI ID			
Asia Pacific (Melbourne) (ap-southeast-4)	View AMI ID			
Canada (Central) (ca-central-1)	View AMI ID			
China (Beijing) (cn-north-1)	View AMI ID			
China (Ningxia) (cn-northwest-1)	View AMI ID			
Europe (Frankfurt) (eu-central-1)	View AMI ID			
Europe (Zurich) (eu-central-2)	View AMI ID			
Europe (Ireland) (eu-west-1)	View AMI ID			
Europe (London) (eu-west-2)	View AMI ID			
Europe (Milan) (eu-south-1)	View AMI ID			
Europe (Spain) (eu-south-2)	View AMI ID			
Europe (Paris) (eu-west-3)	View AMI ID			
Europe (Stockholm) (eu-north-1)	View AMI ID			
Israel (Tel Aviv) (il-central-1)	View AMI ID			

AWS Region	Windows Server 2022 Core	Windows Server 2022 Full	Windows Server 2019 Core	Windows Server 2019 Full
Middle East (Bahrain) (me-south-1)	View AMI ID			
Middle East (UAE) (me-central-1)	View AMI ID			
South America (São Paulo) (sa-east-1)	View AMI ID			
AWS GovCloud (US-East) (us-gov-east-1)	View AMI ID			
AWS GovCloud (US-West) (us-gov-west-1)	View AMI ID			

Creating custom Amazon EKS optimized Windows AMIs

You can use EC2 Image Builder to create custom Amazon EKS optimized Windows AMIs with one of the following options:

- [Using an Amazon EKS optimized Windows AMI as a base \(p. 225\)](#)
- [Using the Amazon-managed build component \(p. 226\)](#)

With both methods, you must create your own Image Builder recipe. For more information, see [Create a new version of an image recipe](#) in the Image Builder User Guide.

Important

The following **Amazon-managed** components for eks include patches for CVE-2023-3676, CVE-2023-3893, and CVE-2023-3955. All older **Amazon-managed** components are deprecated because of these CVEs.

- 1.23.3 and higher
- 1.24.2 and higher
- 1.25.1 and higher
- 1.26.1 and higher

Using an Amazon EKS optimized Windows AMI as a base

This option is the recommended way to build your custom Windows AMIs. The Amazon EKS optimized Windows AMIs we provide are more frequently updated than the Amazon-managed build component.

1. Start a new Image Builder recipe.
 - a. Open the EC2 Image Builder console at <https://console.aws.amazon.com/imagebuilder>.
 - b. In the left navigation pane, choose **Image recipes**.
 - c. Choose **Create image recipe**.
2. In the **Recipe details** section, enter a **Name** and **Version**.

3. Specify the ID of the Amazon EKS optimized Windows AMI in the **Base image** section.
 - a. Choose **Enter custom AMI ID**.
 - b. Retrieve the AMI ID for the Windows OS version that you require. For more information, see [Retrieving Amazon EKS optimized Windows AMI IDs \(p. 211\)](#).
 - c. Enter the custom **AMI ID**. If the AMI ID isn't found, make sure that the AWS Region for the AMI ID matches the AWS Region shown in the upper right of your console.
4. (Optional) To get the latest security updates, add the `update-windows` component in the **Build components** - section.
 - a. From the dropdown list to the right of the **Find components by name** search box, choose **Amazon-managed**.
 - b. In the **Find components by name** search box, enter **update-windows**.
 - c. Select the check box of the **update-windows** search result. This component includes the latest Windows patches for the operating system.
5. Complete the remaining image recipe inputs with your required configurations. For more information, see [Create a new image recipe version \(console\)](#) in the Image Builder User Guide.
6. Choose **Create recipe**.
7. Use the new image recipe in a new or existing image pipeline. Once your image pipeline runs successfully, your custom AMI will be listed as an output image and is ready for use. For more information, see [Create an image pipeline using the EC2 Image Builder console wizard](#).

Using the Amazon-managed build component

When using an Amazon EKS optimized Windows AMI as a base isn't viable, you can use the Amazon-managed build component instead. This option may lag behind the most recent supported Kubernetes versions.

1. Start a new Image Builder recipe.
 - a. Open the EC2 Image Builder console at <https://console.aws.amazon.com/imagebuilder>.
 - b. In the left navigation pane, choose **Image recipes**.
 - c. Choose **Create image recipe**.
2. In the **Recipe details** section, enter a **Name** and **Version**.
3. Determine which option you will be using to create your custom AMI in the **Base image** section:
 - **Select managed images** – Choose **Windows** for your **Image Operating System (OS)**. Then choose one of the following options for **Image origin**:
 - **Quick start (Amazon-managed)** – In the **Image name** dropdown, choose an Amazon EKS supported Windows Server version. For more information, see [Amazon EKS optimized Windows AMIs \(p. 184\)](#).
 - **Images owned by me** – For **Image name**, choose the ARN of your own image with your own license. The image that you provide can't already have Amazon EKS components installed.
 - **Enter custom AMI ID** – For AMI ID, enter the ID for your AMI with your own license. The image that you provide can't already have Amazon EKS components installed.
4. In the **Build components - Windows** section, do the following:
 - a. From the dropdown list to the right of the **Find components by name** search box, choose **Amazon-managed**.
 - b. In the **Find components by name** search box, enter `eks`.
 - c. Select the check box of the **eks-optimized-ami-windows** search result, even though the result returned may not be the version that you want.

- d. In the **Find components by name** search box, enter **update-windows**.
 - e. Select the check box of the **update-windows** search result. This component includes the latest Windows patches for the operating system.
5. In the **Selected components** section, do the following:
- a. Choose **Versioning options** for **eks-optimized-ami-windows**.
 - b. Choose **Specify component version**.
 - c. In the **Component Version** field, enter **version.x**, replacing **version** with a supported Kubernetes version. Entering an **x** for part of the version number indicates to use the latest component version that also aligns with the part of the version you explicitly define. Pay attention to the console output as it will advise you on whether your desired version is available as a managed component. Keep in mind that the most recent Kubernetes versions may not be available for the build component. For more information about available versions, see [Retrieving information about eks-optimized-ami-windows component versions \(p. 227\)](#).

Note

The following eks-optimized-ami-windows build component versions require eksctl version 0.129 or lower:

- 1.24.0
- 1.23.1 or lower

6. Complete the remaining image recipe inputs with your required configurations. For more information, see [Create a new image recipe version \(console\)](#) in the Image Builder User Guide.
7. Choose **Create recipe**.
8. Use the new image recipe in a new or existing image pipeline. Once your image pipeline runs successfully, your custom AMI will be listed as an output image and is ready for use. For more information, see [Create an image pipeline using the EC2 Image Builder console wizard](#).

Retrieving information about eks-optimized-ami-windows component versions

You can retrieve specific information regarding what is installed with each component. For example, you can verify what kubelet version is installed. The components go through functional testing on the Amazon EKS supported Windows operating systems versions. For more information, see [Release calendar \(p. 185\)](#). Any other Windows OS versions that aren't listed as supported or have reached end of support might not be compatible with the component.

1. Open the EC2 Image Builder console at <https://console.aws.amazon.com/imagebuilder>.
2. In the left navigation pane, choose **Components**.
3. From the dropdown list to the right of the **Find components by name** search box, change **Owned by me** to **Quick start (Amazon-managed)**.
4. In the **Find components by name** box, enter **eks**.
5. (Optional) If you are using a recent version, sort the **Version** column in descending order by choosing it twice.
6. Choose the **eks-optimized-ami-windows** link with a desired version.

The **Description** in the resulting page shows the specific information.

Storage

This chapter covers storage options for Amazon EKS clusters.

Topics

- [Amazon EBS CSI driver \(p. 228\)](#)
- [Amazon EFS CSI driver \(p. 244\)](#)
- [Amazon FSx for Lustre CSI driver \(p. 249\)](#)
- [Amazon FSx for NetApp ONTAP CSI driver \(p. 254\)](#)
- [Amazon FSx for OpenZFS CSI driver \(p. 254\)](#)
- [Amazon File Cache CSI driver \(p. 255\)](#)

Amazon EBS CSI driver

The Amazon Elastic Block Store (Amazon EBS) Container Storage Interface (CSI) driver manages the lifecycle of Amazon EBS volumes as storage for the *Kubernetes Volumes* that you create. The Amazon EBS CSI driver makes Amazon EBS volumes for these types of Kubernetes volumes: *generic ephemeral volumes* and *persistent volumes*

Here are some things to consider about using the Amazon EBS CSI driver.

- The Amazon EBS CSI plugin requires IAM permissions to make calls to AWS APIs on your behalf. For more information, see [Creating the Amazon EBS CSI driver IAM role \(p. 228\)](#).
- You can't mount Amazon EBS volumes to Fargate Pods.
- You can run the Amazon EBS CSI controller on Fargate nodes, but the Amazon EBS CSI node DaemonSet can only run on Amazon EC2 instances.
- Alpha features of the Amazon EBS CSI driver aren't supported on Amazon EKS clusters.

The Amazon EBS CSI driver isn't installed when you first create a cluster. To use the driver, you must add it as an Amazon EKS add-on or as a self-managed add-on.

- For instructions on how to add it as an Amazon EKS add-on, see [Managing the Amazon EBS CSI driver as an Amazon EKS add-on \(p. 234\)](#).
- For instructions on how to add it as a self-managed installation, see the [Amazon EBS Container Storage Interface \(CSI\) driver](#) project on GitHub.

After you installed the CSI driver with either method, you can test the functionality with a sample application. For more information, see [Deploy a sample application and verify that the CSI driver is working \(p. 239\)](#).

Creating the Amazon EBS CSI driver IAM role

The Amazon EBS CSI plugin requires IAM permissions to make calls to AWS APIs on your behalf. For more information, see [Set up driver permission](#) on GitHub.

Note

Pods will have access to the permissions that are assigned to the IAM role unless you block access to IMDS. For more information, see [Security best practices for Amazon EKS \(p. 522\)](#).

Prerequisites

- An existing cluster.
- An existing AWS Identity and Access Management (IAM) OpenID Connect (OIDC) provider for your cluster. To determine whether you already have one, or to create one, see [Creating an IAM OIDC provider for your cluster \(p. 465\)](#).

The following procedure shows you how to create an IAM role and attach the required AWS managed policy to it. You can use eksctl, the AWS Management Console, or the AWS CLI.

Note

The specific steps in this procedure are written for using the driver as an Amazon EKS add-on. Different steps are needed to use the driver as a self-managed add-on.

eksctl

To create your Amazon EBS CSI plugin IAM role with eksctl

1. Create an IAM role and attach the required AWS managed policy with the following command. Replace *my-cluster* with the name of your cluster. The command deploys an AWS CloudFormation stack that creates an IAM role and attaches the IAM policy to it. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov::`.

```
eksctl create iamserviceaccount \
--name ebs-csi-controller-sa \
--namespace kube-system \
--cluster my-cluster \
--role-name AmazonEKS_EBS_CSI_DriverRole \
--role-only \
--attach-policy-arn arn:aws:iam::aws:policy/service-role/
AmazonEBSCSIDriverPolicy \
--approve
```

2. If you use a custom [KMS key](#) for encryption on your Amazon EBS volumes, customize the IAM role as needed. For example, do the following:
 - a. Copy and paste the following code into a new `kms-key-for-encryption-on-ebs.json` file. Replace `custom-key-arn` with the custom [KMS key ARN](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms>CreateGrant",
        "kms>ListGrants",
        "kms>RevokeGrant"
      ],
      "Resource": ["custom-key-arn"],
      "Condition": {
        "Bool": {
          "kms>GrantIsForAWSResource": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms>Encrypt",
```

```
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": ["custom-key-arn"]
}
}
```

- b. Create the policy. You can change *KMS_Key_For_Encryption_On_EBS_Policy* to a different name. However, if you do, make sure to change it in later steps, too.

```
aws iam create-policy \
--policy-name KMS_Key_For_Encryption_On_EBS_Policy \
--policy-document file://kms-key-for-encryption-on-ebs.json
```

- c. Attach the IAM policy to the role with the following command. Replace *111122223333* with your account ID. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace arn:aws: with arn:aws-us-gov:.

```
aws iam attach-role-policy \
--policy-arn
arn:aws:iam::111122223333:policy/KMS_Key_For_Encryption_On_EBS_Policy \
--role-name AmazonEKS_EBS_CSI_DriverRole
```

AWS Management Console

To create your Amazon EBS CSI plugin IAM role with the AWS Management Console

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the left navigation pane, choose **Roles**.
3. On the **Roles** page, choose **Create role**.
4. On the **Select trusted entity** page, do the following:
 - a. In the **Trusted entity type** section, choose **Web identity**.
 - b. For **Identity provider**, choose the **OpenID Connect provider URL** for your cluster (as shown under **Overview** in Amazon EKS).
 - c. For **Audience**, choose `sts.amazonaws.com`.
 - d. Choose **Next**.
5. On the **Add permissions** page, do the following:
 - a. In the **Filter policies** box, enter `AmazonEBSCSIDriverPolicy`.
 - b. Select the check box to the left of the `AmazonEBSCSIDriverPolicy` returned in the search.
 - c. Choose **Next**.
6. On the **Name, review, and create** page, do the following:
 - a. For **Role name**, enter a unique name for your role, such as ***AmazonEKS_EBS_CSI_DriverRole***.
 - b. Under **Add tags (Optional)**, add metadata to the role by attaching tags as key-value pairs. For more information about using tags in IAM, see [Tagging IAM Entities](#) in the *IAM User Guide*.
 - c. Choose **Create role**.
7. After the role is created, choose the role in the console to open it for editing.

8. Choose the **Trust relationships** tab, and then choose **Edit trust policy**.
9. Find the line that looks similar to the following line:

```
"oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud":  
"sts.amazonaws.com"
```

Add a comma to the end of the previous line, and then add the following line after the previous line. Replace *region-code* with the AWS Region that your cluster is in. Replace *EXAMPLED539D4633E53DE1B71EXAMPLE* with your cluster's OIDC provider ID.

```
"oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub":  
"system:serviceaccount:kube-system:ebs-csi-controller-sa"
```

10. Choose **Update policy** to finish.
11. If you use a custom [KMS key](#) for encryption on your Amazon EBS volumes, customize the IAM role as needed. For example, do the following:
 - a. In the left navigation pane, choose **Policies**.
 - b. On the **Policies** page, choose **Create Policy**.
 - c. On the **Create policy** page, choose the **JSON** tab.
 - d. Copy and paste the following code into the editor, replacing *custom-key-arn* with the custom [KMS key ARN](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms>ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": ["custom-key-arn"],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": ["custom-key-arn"]
    }
  ]
}
```

- e. Choose **Next: Tags**.
- f. On the **Add tags (Optional)** page, choose **Next: Review**.
- g. For **Name**, enter a unique name for your policy (for example, [*KMS_Key_For_Encryption_On_EBS_Policy*](#)).

- h. Choose **Create policy**.
- i. In the left navigation pane, choose **Roles**.
- j. Choose the **AmazonEKS_EBS_CSI_DriverRole** in the console to open it for editing.
- k. From the **Add permissions** drop-down list, choose **Attach policies**.
- l. In the **Filter policies** box, enter **KMS_Key_For_Encryption_On_EBS_Policy**.
- m. Select the check box to the left of the **KMS_Key_For_Encryption_On_EBS_Policy** that was returned in the search.
- n. Choose **Attach policies**.

AWS CLI

To create your Amazon EBS CSI plugin IAM role with the AWS CLI

1. View your cluster's OIDC provider URL. Replace **my-cluster** with your cluster name. If the output from the command is None, review the **Prerequisites**.

```
aws eks describe-cluster --name my-cluster --query "cluster.identity.oidc.issuer" --output text
```

An example output is as follows.

```
https://oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE
```

2. Create the IAM role, granting the AssumeRoleWithWebIdentity action.
 - a. Copy the following contents to a file that's named **aws-ebs-csi-driver-trust-policy.json**. Replace **111122223333** with your account ID. Replace **EXAMPLED539D4633E53DE1B71EXAMPLE** and **region-code** with the values returned in the previous step. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace **arn:aws:** with **arn:aws-us-gov:**.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Federated": "arn:aws:iam::111122223333:oidc-provider/oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"  
            },  
            "Action": "sts:AssumeRoleWithWebIdentity",  
            "Condition": {  
                "StringEquals": {  
                    "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com",  
                    "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:kube-system:ebs-csi-controller-sa"  
                }  
            }  
        }  
    ]  
}
```

- b. Create the role. You can change **AmazonEKS_EBS_CSI_DriverRole** to a different name. If you change it, make sure to change it in later steps.

```
aws iam create-role \
--role-name AmazonEKS_EBS_CSI_DriverRole \
--assume-role-policy-document file:///"aws-ebs-csi-driver-trust-policy.json"
```

3. Attach the required AWS managed policy to the role with the following command. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy \
--role-name AmazonEKS_EBS_CSI_DriverRole
```

4. If you use a custom [KMS key](#) for encryption on your Amazon EBS volumes, customize the IAM role as needed. For example, do the following:

- a. Copy and paste the following code into a new `kms-key-for-encryption-on-ebs.json` file. Replace `custom-key-arn` with the custom [KMS key ARN](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms>CreateGrant",
        "kms>ListGrants",
        "kms>RevokeGrant"
      ],
      "Resource": ["custom-key-arn"],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": ["custom-key-arn"]
    }
  ]
}
```

- b. Create the policy. You can change `KMS_Key_For_Encryption_On_EBS_Policy` to a different name. However, if you do, make sure to change it in later steps, too.

```
aws iam create-policy \
--policy-name KMS_Key_For_Encryption_On_EBS_Policy \
--policy-document file:///"kms-key-for-encryption-on-ebs.json"
```

- c. Attach the IAM policy to the role with the following command. Replace `111122223333` with your account ID. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

```
aws iam attach-role-policy \
--policy-arn
arn:aws:iam::111122223333:policy/KMS_Key_For_Encryption_On_EBS_Policy \
--role-name AmazonEKS_EBS_CSI_DriverRole
```

Now that you have created the Amazon EBS CSI driver IAM role, you can continue to [Adding the Amazon EBS CSI driver add-on \(p. 235\)](#). When you deploy the plugin in that procedure, it creates and is configured to use a service account that's named ebs-csi-controller-sa. The service account is bound to a Kubernetes clusterrole that's assigned the required Kubernetes permissions.

Managing the Amazon EBS CSI driver as an Amazon EKS add-on

To improve security and reduce the amount of work, you can manage the Amazon EBS CSI driver as an Amazon EKS add-on. For information about Amazon EKS add-ons, see [Amazon EKS add-ons \(p. 385\)](#). You can add the Amazon EBS CSI add-on by following the steps in [Adding the Amazon EBS CSI driver add-on \(p. 235\)](#).

If you added the Amazon EBS CSI add-on, you can manage it by following the steps in the [Updating the Amazon EBS CSI driver as an Amazon EKS add-on \(p. 236\)](#) and [Removing the Amazon EBS CSI add-on \(p. 238\)](#) sections.

Prerequisites

- An existing cluster. To see the required platform version, run the following command.

```
aws eks describe-addon-versions --addon-name aws-ebs-csi-driver
```

- An existing AWS Identity and Access Management (IAM) OpenID Connect (OIDC) provider for your cluster. To determine whether you already have one, or to create one, see [Creating an IAM OIDC provider for your cluster \(p. 465\)](#).
- An Amazon EBS CSI driver IAM role. If you don't satisfy this prerequisite, attempting to install the add-on and running `kubectl describe pvc` will show failed to provision volume with StorageClass along with a could not create volume in EC2: UnauthorizedOperation error. For more information, see [Creating the Amazon EBS CSI driver IAM role \(p. 228\)](#).
- If you're using a cluster wide restricted [PodSecurityPolicy \(p. 522\)](#), make sure that the add-on is granted sufficient permissions to be deployed. For the permissions required by each add-on Pod, see the [relevant add-on manifest definition](#) on GitHub.

Important

To use the snapshot functionality of the Amazon EBS CSI driver, you must install the external snapshotter before the installation of the add-on. The external snapshotter components must be installed in the following order:

- [CustomResourceDefinition](#) (CRD) for `volumesnapshotclasses`, `volumesnapshots`, and `volumesnapshotcontents`
- [RBAC](#) (`ClusterRole`, `ClusterRoleBinding`, and so on)
- [controller deployment](#)

For more information, see [CSI Snapshotter](#) on GitHub.

Adding the Amazon EBS CSI driver add-on

Important

Before adding the Amazon EBS driver as an Amazon EKS add-on, confirm that you don't have a self-managed version of the driver installed on your cluster. If so, see [Uninstalling a self-managed Amazon EBS CSI driver](#) on GitHub.

You can use `eksctl`, the AWS Management Console, or the AWS CLI to add the Amazon EBS CSI add-on to your cluster.

`eksctl`

To add the Amazon EBS CSI add-on using `eksctl`

Run the following command. Replace `my-cluster` with the name of your cluster, `111122223333` with your account ID, and `AmazonEKS_EBS_CSI_DriverRole` with the name of the [IAM role created earlier \(p. 228\)](#). If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov::`.

```
eksctl create addon --name aws-ebs-csi-driver --cluster my-cluster --service-account-role-arn arn:aws:iam::111122223333:role/AmazonEKS_EBS_CSI_DriverRole --force
```

If you remove the `--force` option and any of the Amazon EKS add-on settings conflict with your existing settings, then updating the Amazon EKS add-on fails, and you receive an error message to help you resolve the conflict. Before specifying this option, make sure that the Amazon EKS add-on doesn't manage settings that you need to manage, because those settings are overwritten with this option. For more information about other options for this setting, see [Addons](#) in the `eksctl` documentation. For more information about Amazon EKS Kubernetes field management, see [Kubernetes field management \(p. 406\)](#).

AWS Management Console

To add the Amazon EBS CSI add-on using the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, choose **Clusters**.
3. Choose the name of the cluster that you want to configure the Amazon EBS CSI add-on for.
4. Choose the **Add-ons** tab.
5. Choose **Get more add-ons**.
6. On the **Select add-ons** page, do the following:
 - a. In the **Amazon EKS-addons** section, select the **Amazon EBS CSI Driver** check box.
 - b. Choose **Next**.
7. On the **Configure selected add-ons settings** page, do the following:
 - a. Select the **Version** you'd like to use.
 - b. For **Select IAM role**, select the name of an IAM role that you attached the Amazon EBS CSI driver IAM policy to.
 - c. (Optional) You can expand the **Optional configuration settings**. If you select **Override** for the **Conflict resolution method**, one or more of the settings for the existing add-on can be overwritten with the Amazon EKS add-on settings. If you don't enable this option and there's a conflict with your existing settings, the operation fails. You can use the resulting error message to troubleshoot the conflict. Before selecting this option, make sure that the Amazon EKS add-on doesn't manage settings that you need to self-manage.
 - d. Choose **Next**.

8. On the **Review and add** page, choose **Create**. After the add-on installation is complete, you see your installed add-on.

AWS CLI

To add the Amazon EBS CSI add-on using the AWS CLI

Run the following command. Replace *my-cluster* with the name of your cluster, **111122223333** with your account ID, and *AmazonEKS_EBS_CSI_DriverRole* with the name of the role that was created earlier. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

```
aws eks create-addon --cluster-name my-cluster --addon-name aws-ebs-csi-driver \
--service-account-role-arn
arn:aws:iam::111122223333:role/AmazonEKS_EBS_CSI_DriverRole
```

Now that you have added the Amazon EBS CSI driver as an Amazon EKS add-on, you can continue to [Deploy a sample application and verify that the CSI driver is working \(p. 239\)](#). That procedure includes setting up the storage class.

Updating the Amazon EBS CSI driver as an Amazon EKS add-on

Amazon EKS doesn't automatically update Amazon EBS CSI for your cluster when new versions are released or after you [update your cluster \(p. 34\)](#) to a new Kubernetes minor version. To update Amazon EBS CSI on an existing cluster, you must initiate the update and then Amazon EKS updates the add-on for you.

eksctl

To update the Amazon EBS CSI add-on using eksctl

1. Check the current version of your Amazon EBS CSI add-on. Replace *my-cluster* with your cluster name.

```
eksctl get addon --name aws-ebs-csi-driver --cluster my-cluster
```

An example output is as follows.

NAME	VERSION	STATUS	ISSUES	IAMROLE	UPDATE
AVAILABLE aws-ebs-csi-driver <i>eksbuild.1</i>	<i>v1.11.2-eksbuild.1</i>	ACTIVE	0		<i>v1.11.4-</i>

2. Update the add-on to the version returned under UPDATE AVAILABLE in the output of the previous step.

```
eksctl update addon --name aws-ebs-csi-driver --version v1.11.4-eksbuild.1 --
cluster my-cluster --force
```

If you remove the `--force` option and any of the Amazon EKS add-on settings conflict with your existing settings, then updating the Amazon EKS add-on fails, and you receive an error message to help you resolve the conflict. Before specifying this option, make sure that the Amazon EKS add-on doesn't manage settings that you need to manage, because those settings are overwritten with this option. For more information about other options for this setting, see

[Addons](#) in the `eksctl` documentation. For more information about Amazon EKS Kubernetes field management, see [Kubernetes field management \(p. 406\)](#).

AWS Management Console

To update the Amazon EBS CSI add-on using the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, choose **Clusters**.
3. Choose the name of the cluster that you want to update the Amazon EBS CSI add-on for.
4. Choose the **Add-ons** tab.
5. Choose **Amazon EBS CSI Driver**.
6. Choose **Edit**.
7. On the **Configure Amazon EBS CSI Driver** page, do the following:
 - a. Select the **Version** you'd like to use.
 - b. For **Select IAM role**, select the name of an IAM role that you attached the Amazon EBS CSI driver IAM policy to.
 - c. (Optional) You can expand the **Optional configuration settings** and modify as needed.
 - d. Choose **Save changes**.

AWS CLI

To update the Amazon EBS CSI add-on using the AWS CLI

1. Check the current version of your Amazon EBS CSI add-on. Replace `my-cluster` with your cluster name.

```
aws eks describe-addon --cluster-name my-cluster --addon-name aws-ebs-csi-driver --query "addon.addonVersion" --output text
```

An example output is as follows.

```
v1.11.2-eksbuild.1
```

2. Determine which versions of the Amazon EBS CSI add-on are available for your cluster version.

```
aws eks describe-addon-versions --addon-name aws-ebs-csi-driver --kubernetes-version 1.23 \
--query "addons[].addonVersions[].[addonVersion, compatibilities[].defaultVersion]" --output text
```

An example output is as follows.

```
v1.11.4-eksbuild.1
True
v1.11.2-eksbuild.1
False
```

The version with `True` underneath is the default version deployed when the add-on is created. The version deployed when the add-on is created might not be the latest available version. In the previous output, the latest version is deployed when the add-on is created.

3. Update the add-on to the version with True that was returned in the output of the previous step. If it was returned in the output, you can also update to a later version.

```
aws eks update-addon --cluster-name my-cluster --addon-name aws-ebs-csi-driver --  
addon-version v1.11.4-eksbuild.1 \  
--resolve-conflicts PRESERVE
```

The *PRESERVE* option preserves any custom settings that you've set for the add-on. For more information about other options for this setting, see [update-addon](#) in the Amazon EKS Command Line Reference. For more information about Amazon EKS add-on configuration management, see [Kubernetes field management \(p. 406\)](#).

Removing the Amazon EBS CSI add-on

You have two options for removing an Amazon EKS add-on.

- **Preserve add-on software on your cluster** – This option removes Amazon EKS management of any settings. It also removes the ability for Amazon EKS to notify you of updates and automatically update the Amazon EKS add-on after you initiate an update. However, it preserves the add-on software on your cluster. This option makes the add-on a self-managed installation, rather than an Amazon EKS add-on. With this option, there's no downtime for the add-on. The commands in this procedure use this option.
- **Remove add-on software entirely from your cluster** – We recommend that you remove the Amazon EKS add-on from your cluster only if there are no resources on your cluster that are dependent on it. To do this option, delete `--preserve` from the command you use in this procedure.

If the add-on has an IAM account associated with it, the IAM account isn't removed.

You can use `eksctl`, the AWS Management Console, or the AWS CLI to remove the Amazon EBS CSI add-on.

`eksctl`

To remove the Amazon EBS CSI add-on using `eksctl`

Replace *my-cluster* with the name of your cluster, and then run the following command.

```
eksctl delete addon --cluster my-cluster --name aws-ebs-csi-driver --preserve
```

AWS Management Console

To remove the Amazon EBS CSI add-on using the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, choose **Clusters**.
3. Choose the name of the cluster that you want to remove the Amazon EBS CSI add-on for.
4. Choose the **Add-ons** tab.
5. Choose **Amazon EBS CSI Driver**.
6. Choose **Remove**.
7. In the **Remove: aws-ebs-csi-driver** confirmation dialog box, do the following:
 - a. If you want Amazon EKS to stop managing settings for the add-on, select **Preserve on cluster**. Do this if you want to retain the add-on software on your cluster. This is so that you can manage all of the settings of the add-on on your own.

- b. Enter **aws-ebs-csi-driver**.
- c. Select **Remove**.

AWS CLI

To remove the Amazon EBS CSI add-on using the AWS CLI

Replace *my-cluster* with the name of your cluster, and then run the following command.

```
aws eks delete-addon --cluster-name my-cluster --addon-name aws-ebs-csi-driver --preserve
```

Deploy a sample application and verify that the CSI driver is working

You can test the CSI driver functionality with a sample application. This topic shows one example, but you can also do the following:

- Deploy a sample application that uses the external snapshotter to create volume snapshots. For more information, see [Volume Snapshots](#) on GitHub.
- Deploy a sample application that uses volume resizing. For more information, see [Volume Resizing](#) on GitHub.

This procedure uses the [Dynamic volume provisioning](#) example from the [Amazon EBS Container Storage Interface \(CSI\) driver](#) GitHub repository to consume a dynamically provisioned Amazon EBS volume.

1. Clone the [Amazon EBS Container Storage Interface \(CSI\) driver](#) GitHub repository to your local system.

```
git clone https://github.com/kubernetes-sigs/aws-ebs-csi-driver.git
```

2. Navigate to the dynamic-provisioning example directory.

```
cd aws-ebs-csi-driver/examples/kubernetes/dynamic-provisioning/
```

3. (Optional) The manifests/storageclass.yaml file provisions gp2 Amazon EBS volumes by default. To use gp3 volumes instead, add type: gp3 to manifests/storageclass.yaml.

```
echo "parameters:
  type: gp3" >> manifests/storageclass.yaml
```

4. Deploy the ebs-sc storage class, ebs-claim persistent volume claim, and app sample application from the manifests directory.

```
kubectl apply -f manifests/
```

5. Describe the ebs-sc storage class.

```
kubectl describe storageclass ebs-sc
```

An example output is as follows.

```
Name: ebs-sc
IsDefaultClass: No
Annotations: kubectl.kubernetes.io/last-applied-configuration={"apiVersion":"storage.k8s.io/v1","kind":"StorageClass","metadata":{"annotations":{},"name":"ebs-sc"},"provisioner":"ebs.csi.aws.com","volumeBindingMode":"WaitForFirstConsumer"}

Provisioner: ebs.csi.aws.com
Parameters: <none>
AllowVolumeExpansion: <unset>
MountOptions: <none>
ReclaimPolicy: Delete
VolumeBindingMode: WaitForFirstConsumer
Events: <none>
```

Note

The storage class uses the `WaitForFirstConsumer` volume binding mode. This means that volumes aren't dynamically provisioned until a Pod makes a persistent volume claim. For more information, see [Volume Binding Mode](#) in the Kubernetes documentation.

6. Watch the Pods in the default namespace. After a few minutes, the app Pod's status changes to `Running`.

```
kubectl get pods --watch
```

Enter `Ctrl+C` to return to a shell prompt.

7. List the persistent volumes in the default namespace. Look for a persistent volume with the `default/ebs-claim` claim.

```
kubectl get pv
```

An example output is as follows.

NAME	STATUS	CLAIM	STORAGECLASS	CAPACITY	ACCESS MODES	RECLAIM POLICY
pvc-37717cd6-d0dc-11e9-b17f-06fad4858a5a	Bound	default/ebs-claim	ebs-sc	4Gi	RWO 30s	Delete

8. Describe the persistent volume. Replace `pvc-37717cd6-d0dc-11e9-b17f-06fad4858a5a` with the value from the output in the previous step.

```
kubectl describe pv pvc-37717cd6-d0dc-11e9-b17f-06fad4858a5a
```

An example output is as follows.

```
Name: pvc-37717cd6-d0dc-11e9-b17f-06fad4858a5a
Labels: <none>
Annotations: pv.kubernetes.io/provisioned-by: ebs.csi.aws.com
Finalizers: [kubernetes.io/pv-protection external-attacher/ebs-csi-aws-com]
StorageClass: ebs-sc
Status: Bound
Claim: default/ebs-claim
Reclaim Policy: Delete
Access Modes: RWO
VolumeMode: Filesystem
Capacity: 4Gi
Node Affinity:
```

```
Required Terms:  
Term 0: topology.ebs.csi.aws.com/zone in [region-code]  
Message:  
Source:  
  Type:           CSI (a Container Storage Interface (CSI) volume source)  
  Driver:         ebs.csi.aws.com  
  VolumeHandle:  vol-0d651e157c6d93445  
  ReadOnly:       false  
  VolumeAttributes: storage.kubernetes.io/  
  csiProvisionerIdentity=1567792483192-8081-ebs.csi.aws.com  
Events:          <none>
```

The Amazon EBS volume ID is the value for VolumeHandle in the previous output.

- Verify that the Pod is writing data to the volume.

```
kubectl exec -it app -- cat /data/out.txt
```

An example output is as follows.

```
Wed May 5 16:17:03 UTC 2021  
Wed May 5 16:17:08 UTC 2021  
Wed May 5 16:17:13 UTC 2021  
Wed May 5 16:17:18 UTC 2021  
[...]
```

- After you're done, delete the resources for this sample application.

```
kubectl delete -f manifests/
```

Amazon EBS CSI migration frequently asked questions

Important

If you have Pods running on a version 1.22 or earlier cluster, then you must install the [Amazon EBS CSI driver \(p. 228\)](#) before updating your cluster to version 1.23 to avoid service interruption.

The Amazon EBS container storage interface (CSI) migration feature moves responsibility for handling storage operations from the Amazon EBS in-tree EBS storage provisioner to the [Amazon EBS CSI driver \(p. 228\)](#).

What are CSI drivers?

CSI drivers:

- replace the Kubernetes "in-tree" storage drivers that exist in the Kubernetes project source code.
- work with storage providers, such as Amazon EBS.
- provide a simplified plugin model that make it easier for storage providers like AWS to release features and maintain support without depending on the Kubernetes release cycle.

For more information, see [Introduction](#) in the Kubernetes CSI documentation.

What is CSI migration?

The Kubernetes CSI Migration feature moves responsibility for handling storage operations from the existing in-tree storage plugins, such as `kubernetes.io/aws-ebs`, to corresponding CSI drivers. Existing `StorageClass`, `PersistentVolume` and `PersistentVolumeClaim` (PVC) objects continue to work, as long as the corresponding CSI driver is installed. When the feature is enabled:

- Existing workloads that utilize PVCs continue to function as they always have.
- Kubernetes passes control of all storage management operations to CSI drivers.

For more information, see [Kubernetes 1.23: Kubernetes In-Tree to CSI Volume Migration Status Update](#) on the Kubernetes blog.

To help you migrate from the in-tree plugin to CSI drivers, the `CSIMigration` and `CSIMigrationAWS` flags are enabled by default on Amazon EKS version 1.23 and later clusters. These flags enable your cluster to translate the in-tree APIs to their equivalent CSI APIs. These flags are set on the Kubernetes control plane managed by Amazon EKS and in the `kubelet` settings configured in Amazon EKS optimized AMIs. **If you have Pods using Amazon EBS volumes in your cluster, you must install the Amazon EBS CSI driver before updating your cluster to version 1.23.** If you don't, volume operations such as provisioning and mounting might not work as expected. For more information, see [Amazon EBS CSI driver \(p. 228\)](#).

Note

The in-tree `StorageClass` provisioner is named `kubernetes.io/aws-ebs`. The Amazon EBS `StorageClass` provisioner is named `ebs.csi.aws.com`.

Can I mount `kubernetes.io/aws-ebs` `StorageClass` volumes in version 1.23 and later clusters?

Yes, as long as the [Amazon EBS CSI driver \(p. 228\)](#) is installed. For newly created version 1.23 and later clusters, we recommend installing the Amazon EBS CSI driver as part of your cluster creation process. We also recommend only using `StorageClasses` based on the `ebs.csi.aws.com` provisioner.

If you've updated your cluster control plane to version 1.23 and haven't yet updated your nodes to 1.23, then the `CSIMigration` and `CSIMigrationAWS` `kubelet` flags aren't enabled. In this case, the in-tree driver is used to mount `kubernetes.io/aws-ebs` based volumes. The Amazon EBS CSI driver must still be installed however, to ensure that Pods using `kubernetes.io/aws-ebs` based volumes can be scheduled. The driver is also required for other volume operations to succeed.

Can I provision `kubernetes.io/aws-ebs` `StorageClass` volumes on Amazon EKS 1.23 and later clusters?

Yes, as long as the [Amazon EBS CSI driver \(p. 228\)](#) is installed.

Will the `kubernetes.io/aws-ebs` `StorageClass` provisioner ever be removed from Amazon EKS?

The `kubernetes.io/aws-ebs` `StorageClass` provisioner and `awsElasticBlockStore` volume type are no longer supported, but there are no plans to remove them. These resources are treated as a part of the Kubernetes API.

How do I install the Amazon EBS CSI driver?

If you want to manage the driver yourself, you can install it using the open source [Helm chart](#). Alternatively, you can install the [Amazon EBS CSI driver Amazon EKS add-on \(p. 228\)](#). When an update

is required to the Amazon EKS add-on, you initiate the update and Amazon EKS updates the add-on for you.

Important

The Kubernetes in-tree Amazon EBS driver runs on the Kubernetes control plane. It uses IAM permissions assigned to the [the section called “Cluster IAM role” \(p. 499\)](#) to provision Amazon EBS volumes. The Amazon EBS CSI driver runs on nodes. The driver needs IAM permissions to provision volumes. For more information, see [the section called “Create an IAM role” \(p. 228\)](#).

How can I check whether the Amazon EBS CSI driver is installed in my cluster?

Use `helm list -A` to determine whether the open source Helm chart is installed. Use `aws eks list-addons --cluster-name my-cluster` to determine whether the Amazon EKS add-on is installed.

Will Amazon EKS prevent a cluster update to version 1.23 if I haven't already installed the Amazon EBS CSI driver?

No.

What if I forget to install the Amazon EBS CSI driver before I update my cluster to version 1.23? Can I install the driver after updating my cluster?

Yes, but volume operations requiring the Amazon EBS CSI driver will fail after your cluster update until the driver is installed.

What is the default StorageClass applied in newly created Amazon EKS version 1.23 and later clusters?

The default StorageClass behavior remains unchanged. With each new cluster, Amazon EKS applies a `kubernetes.io/aws-ebs` based StorageClass named `gp2`. We don't plan to ever remove this StorageClass from newly created clusters. Though subject to change, we are currently targeting version 1.25 to remove the default annotation from the StorageClass applied to newly created clusters. Separate from the cluster default StorageClass, if you create an `ebs.csi.aws.com` based StorageClass without specifying a volume type, the Amazon EBS CSI driver will default to using `gp3`.

Will Amazon EKS make any changes to StorageClasses already present in my existing cluster when I update my cluster to version 1.23?

No.

How do I migrate a persistent volume from the `kubernetes.io/aws-ebsStorageClass` to `ebs.csi.aws.com` using snapshots?

To migrate a persistent volume, see [Migrating Amazon EKS clusters from gp2 to gp3 EBS volumes](#) on the AWS blog.

How do I modify an Amazon EBS volume using annotations?

Starting with `aws-ebs-csi-driver v1.19.0-eksbuild.2`, you can modify Amazon EBS volumes using annotations within their PersistentVolumeClaims (PVC). The new [volume modification](#) feature is implemented as an additional sidecar, called `volumemodifier`. For more information, see [Simplifying Amazon EBS volume migration and modification on Kubernetes using the EBS CSI Driver](#) on the AWS blog.

Is migration supported for Windows workloads?

Yes. If you're installing the Amazon EBS CSI driver using the open source Helm chart, set `node.enableWindows` to `true`. This is set by default if installing the Amazon EBS CSI driver as an Amazon EKS add-on. When creating StorageClasses, set the `fsType` to a Windows file system, such as `ntfs`. Volume operations for Windows workloads are then migrated to the Amazon EBS CSI driver the same as they are for Linux workloads. An exception is file system resize operations, which are not supported for `kubernetes.io/aws-ebs` persistent volumes using Windows file systems.

Amazon EFS CSI driver

[Amazon Elastic File System](#) (Amazon EFS) provides serverless, fully elastic file storage so that you can share file data without provisioning or managing storage capacity and performance. The [Amazon EFS Container Storage Interface \(CSI\) driver](#) provides a CSI interface that allows Kubernetes clusters running on AWS to manage the lifecycle of Amazon EFS file systems. This topic shows you how to deploy the Amazon EFS CSI driver to your Amazon EKS cluster.

Considerations

- The Amazon EFS CSI driver isn't compatible with Windows-based container images.
- You can't use dynamic persistent volume provisioning with Fargate nodes, but you can use static provisioning.
- Dynamic provisioning requires 1.2 or later of the driver. You can statically provision persistent volumes using version 1.1 of the driver on any [supported Amazon EKS cluster version \(p. 60\)](#).
- Version 1.3.2 or later of this driver supports the Arm64 architecture, including Amazon EC2 Graviton-based instances.
- Version 1.4.2 or later of this driver supports using FIPS for mounting file systems.
- Take note of the resource quotas for Amazon EFS. For example, there's a quota of 1000 access points that can be created for each Amazon EFS file system. For more information, see [Amazon EFS resource quotas that you cannot change](#).

Prerequisites

- An existing AWS Identity and Access Management (IAM) OpenID Connect (OIDC) provider for your cluster. To determine whether you already have one, or to create one, see [Creating an IAM OIDC provider for your cluster \(p. 465\)](#).
- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such `yum`, `apt-get`, or `Homebrew` for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.

- The `kubectl` command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use `kubectl` version 1.26, 1.27, or 1.28 with it. To install or upgrade `kubectl`, see [Installing or updating kubectl \(p. 6\)](#).

Note

A Pod running on AWS Fargate automatically mounts an Amazon EFS file system.

Creating an IAM role

The Amazon EFS CSI driver requires IAM permissions to interact with your file system. For more information, see [Set up driver permission](#) on GitHub.

Create an IAM role and attach the required AWS managed policy to it. Annotate the Kubernetes service account with the IAM role ARN and the IAM role with the Kubernetes service account name. You can use `eksctl`, the AWS Management Console, or the AWS CLI.

`eksctl`

To create your Amazon EFS CSI driver IAM role with `eksctl`

Run the following commands to create the IAM role and Kubernetes service account. The commands also attach the policy to the role, annotate the Kubernetes service accounts (`efs-csi-controller-sa` and `efs-csi-node-sa`) with the IAM role ARN, and add the Kubernetes service account name to the trust policy for the IAM role. Replace `my-cluster` with your cluster name and `AmazonEKS_EFS_CSI_DriverRole` with the name for your role.

```
export cluster_name=my-cluster
export role_name=AmazonEKS_EFS_CSI_DriverRole
eksctl create iamserviceaccount \
    --name efs-csi-controller-sa \
    --namespace kube-system \
    --cluster $cluster_name \
    --role-name $role_name \
    --role-only \
    --attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy \
    --approve
eksctl create iamserviceaccount \
    --name efs-csi-node-sa \
    --namespace kube-system \
    --cluster $cluster_name \
    --role-name $role_name \
    --role-only \
    --attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy \
    --approve
TRUST_POLICY=$(aws iam get-role --role-name $role_name --query
'Role.AssumeRolePolicyDocument' | \
    sed -e 's/efs-csi-controller-sa/efs-csi-*/' -e 's/StringEquals/StringLike/'')
aws iam update-assume-role-policy --role-name $role_name --policy-document
"$TRUST_POLICY"
```

AWS Management Console

To create your Amazon EFS CSI driver IAM role with the AWS Management Console

- Open the IAM console at <https://console.aws.amazon.com/iam/>.
- In the left navigation pane, choose **Roles**.
- On the **Roles** page, choose **Create role**.
- On the **Select trusted entity** page, do the following:

- a. In the **Trusted entity type** section, choose **Web identity**.
 - b. For **Identity provider**, choose the **OpenID Connect provider URL** for your cluster (as shown under **Overview** in Amazon EKS).
 - c. For **Audience**, choose `sts.amazonaws.com`.
 - d. Choose **Next**.
5. On the **Add permissions** page, do the following:
 - a. In the **Filter policies** box, enter `AmazonEFSCSIDriverPolicy`.
 - b. Select the check box to the left of the `AmazonEFSCSIDriverPolicy` returned in the search.
 - c. Choose **Next**.
 6. On the **Name, review, and create** page, do the following:
 - a. For **Role name**, enter a unique name for your role, such as `AmazonEKS_EFS_CSI_DriverRole`.
 - b. Under **Add tags (Optional)**, add metadata to the role by attaching tags as key–value pairs. For more information about using tags in IAM, see [Tagging IAM Entities](#) in the *IAM User Guide*.
 - c. Choose **Create role**.
 7. After the role is created, choose the role in the console to open it for editing.
 8. Choose the **Trust relationships** tab, and then choose **Edit trust policy**.
 9. Find the line that looks similar to the following line:

```
"oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud":  
"sts.amazonaws.com"
```

Add the following line above the previous line. Replace `region-code` with the AWS Region that your cluster is in. Replace `EXAMPLED539D4633E53DE1B71EXAMPLE` with your cluster's OIDC provider ID.

```
"oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub":  
"system:serviceaccount:kube-system:efs-csi-*",
```

10. Modify the Condition operator from "StringEquals" to "StringLike".
11. Choose **Update policy** to finish.
12. For self-managed installations of the driver, create Kubernetes service accounts that are annotated with the ARN of the IAM role that you created. This step isn't required if you are installing the driver as an Amazon EKS add-on.
 - a. Save the following contents to a file named `efs-service-account.yaml`. Replace `111122223333` with your account ID. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

```
---  
apiVersion: v1  
kind: ServiceAccount  
metadata:  
  labels:  
    app.kubernetes.io/name: aws-efs-csi-driver  
    name: efs-csi-controller-sa  
    namespace: kube-system  
  annotations:  
    eks.amazonaws.com/role-arn:  
    arn:aws:iam::111122223333:role/AmazonEKS_EFS_CSI_DriverRole
```

```
---
apiVersion: v1
kind: ServiceAccount
metadata:
  labels:
    app.kubernetes.io/name: aws-efs-csi-driver
  name: efs-csi-node-sa
  namespace: kube-system
  annotations:
    eks.amazonaws.com/role-arn:
      arn:aws:iam::111122223333:role/AmazonEKS_EFS_CSI_DriverRole
```

- b. Create the Kubernetes service account on your cluster. The Kubernetes service accounts (efs-csi-controller-sa and efs-csi-node-sa) are annotated with the IAM role that you created named *AmazonEKS_EFS_CSI_DriverRole*.

```
kubectl apply -f efs-service-account.yaml
```

AWS CLI

To create your Amazon EFS CSI driver IAM role with the AWS CLI

1. View your cluster's OIDC provider URL. Replace *my-cluster* with your cluster name. If the output from the command is None, review the [Prerequisites](#).

```
aws eks describe-cluster --name my-cluster --query "cluster.identity.oidc.issuer" --output text
```

An example output is as follows.

```
https://oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE
```

2. Create the IAM role, granting the Kubernetes service account the AssumeRoleWithWebIdentity action.
 - a. Copy the following contents to a file named *aws-efs-csi-driver-trust-policy.json*. Replace *111122223333* with your account ID. Replace *EXAMPLED539D4633E53DE1B71EXAMPLE* and *region-code* with the values returned in the previous step. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::111122223333:oidc-provider/oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringLike": {
          "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:kube-system:efs-csi-*",
          "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com"
        }
      }
    }
  ]
}
```

```
        }  
    }  
}
```

- b. Create the role. You can change `AmazonEKS_EFS_CSI_DriverRole` to a different name, but if you do, make sure to change it in later steps too.

```
aws iam create-role \  
  --role-name AmazonEKS_EFS_CSI_DriverRole \  
  --assume-role-policy-document file://"aws-efs-csi-driver-trust-policy.json"
```

3. Attach the required AWS managed policy to the role with the following command. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov::`.

```
aws iam attach-role-policy \  
  --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy \  
  --role-name AmazonEKS_EFS_CSI_DriverRole
```

4. For self-managed installations of the driver, create Kubernetes service accounts that are annotated with the ARN of the IAM role that you created. This step isn't required if you are installing the driver as an Amazon EKS add-on.
- a. Save the following contents to a file named `efs-service-account.yaml`. Replace `111122223333` with your account ID. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov::`.

```
---  
apiVersion: v1  
kind: ServiceAccount  
metadata:  
  labels:  
    app.kubernetes.io/name: aws-efs-csi-driver  
  name: efs-csi-controller-sa  
  namespace: kube-system  
  annotations:  
    eks.amazonaws.com/role-arn:  
    arn:aws:iam::111122223333:role/AmazonEKS_EFS_CSI_DriverRole  
---  
apiVersion: v1  
kind: ServiceAccount  
metadata:  
  labels:  
    app.kubernetes.io/name: aws-efs-csi-driver  
  name: efs-csi-node-sa  
  namespace: kube-system  
  annotations:  
    eks.amazonaws.com/role-arn:  
    arn:aws:iam::111122223333:role/AmazonEKS_EFS_CSI_DriverRole
```

- b. Create the Kubernetes service account on your cluster. The Kubernetes service accounts (`efs-csi-controller-sa` and `efs-csi-node-sa`) are annotated with the IAM role that you created named `AmazonEKS_EFS_CSI_DriverRole`.

```
kubectl apply -f efs-service-account.yaml
```

Installing the Amazon EFS CSI driver

We recommend that you install the Amazon EFS CSI driver through the Amazon EKS add-on. To add an Amazon EKS add-on to your cluster, see [the section called "Creating an add-on" \(p. 393\)](#). For more information about add-ons, see [the section called "Amazon EKS add-ons" \(p. 385\)](#). If you're unable to use the Amazon EKS add-on, we encourage you to submit an issue about why you can't to the [Containers roadmap GitHub repository](#).

Alternatively, if you want a self-managed installation of the Amazon EFS CSI driver, see [Installation](#) on GitHub.

Creating an Amazon EFS file system

To create an Amazon EFS file system, see [Create an Amazon EFS file system for Amazon EKS](#) on GitHub.

Deploying a sample application

You can deploy a variety of sample apps and modify them as needed. For more information, see [Examples](#) on GitHub.

Amazon FSx for Lustre CSI driver

The [FSx for Lustre Container Storage Interface \(CSI\) driver](#) provides a CSI interface that allows Amazon EKS clusters to manage the lifecycle of FSx for Lustre file systems. For more information, see the [FSx for Lustre User Guide](#).

This topic shows you how to deploy the FSx for Lustre CSI driver to your Amazon EKS cluster and verify that it works. We recommend using the latest version of the driver. For available versions, see [CSI Specification Compatibility Matrix](#) on GitHub.

Note

The driver isn't supported on Fargate.

For detailed descriptions of the available parameters and complete examples that demonstrate the driver's features, see the [FSx for Lustre Container Storage Interface \(CSI\) driver](#) project on GitHub.

Prerequisites

You must have:

- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.
- Version 0.160.0 or later of the eksctl command line tool installed on your device or AWS CloudShell. To install or update eksctl, see [Installing or updating eksctl \(p. 13\)](#).
- The kubectl command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use kubectl version 1.26, 1.27, or 1.28 with it. To install or upgrade kubectl, see [Installing or updating kubectl \(p. 6\)](#).

The following procedures help you create a simple test cluster with the FSx for Lustre CSI driver so that you can see how it works. We don't recommend using the testing cluster for production workloads. For this tutorial, we recommend using the *example values*, except where it's noted to replace them. You can replace any *example value* when completing the steps for your production cluster. We recommend completing all steps in the same terminal because variables are set and used throughout the steps and won't exist in different terminals.

To deploy the FSx for Lustre CSI driver to an Amazon EKS cluster

1. Set a few variables to use in the remaining steps. Replace *my-csi-fsx-cluster* with the name of the test cluster you want to create and *region-code* with the AWS Region that you want to create your test cluster in.

```
export cluster_name=my-csi-fsx-cluster
export region_code=region-code
```

2. Create a test cluster.

```
eksctl create cluster \
--name $cluster_name \
--region $region_code \
--with-oidc \
--ssh-access \
--ssh-public-key my-key
```

Cluster provisioning takes several minutes. During cluster creation, you'll see several lines of output. The last line of output is similar to the following example line.

```
[#] EKS cluster "my-csi-fsx-cluster" in "region-code" region is ready
```

3. Create a Kubernetes service account for the driver and attach the AmazonFSxFullAccess AWS-managed policy to the service account with the following command. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

```
eksctl create iamserviceaccount \
--name fsx-csi-controller-sa \
--namespace kube-system \
--cluster $cluster_name \
--attach-policy-arn arn:aws:iam::aws:policy/AmazonFSxFullAccess \
--approve \
--role-name AmazonEKSFsxEstoreCSIControllerFullAccess \
--region $region_code
```

An example output is as follows.

You'll see several lines of output as the service account is created. The last lines of output are similar to the following.

```
[#] 1 task: {
  2 sequential sub-tasks: {
    create IAM role for serviceaccount "kube-system/fsx-csi-controller-sa", 
    create serviceaccount "kube-system/fsx-csi-controller-sa",
  } }
[#] building iamserviceaccount stack "eksctl-my-csi-fsx-cluster-addon-
iamserviceaccount-kube-system-fsx-csi-controller-sa"
[#] deploying stack "eksctl-my-csi-fsx-cluster-addon-iamserviceaccount-kube-
system-fsx-csi-controller-sa"
```

```
[#] waiting for CloudFormation stack "eksctl-my-csi-fsx-cluster-addon-iamserviceaccount-kube-system-fsx-csi-controller-sa"  
[#] created serviceaccount "kube-system/fsx-csi-controller-sa"
```

Note the name of the AWS CloudFormation stack that was deployed. In the previous example output, the stack is named eksctl-*my-csi-fsx-cluster*-addon-iamserviceaccount-kube-system-*fsx-csi-controller-sa*.

4. Deploy the driver with the following command. Replace *release-X.XX* with your desired branch. The master branch isn't supported because it may contain upcoming features incompatible with the currently released stable version of the driver. We recommend using the latest released version. For a list of active branches, see [aws-fsx-csi-driver](#) on GitHub.

Note

You can view the content being applied in [aws-fsx-csi-driver](#) on GitHub.

```
kubectl apply -k "github.com/kubernetes-sigs/aws-fsx-csi-driver/deploy/kubernetes/overlays/stable/?ref=release-X.XX"
```

An example output is as follows.

```
serviceaccount/fsx-csi-controller-sa created  
serviceaccount/fsx-csi-node-sa created  
clusterrole.rbac.authorization.k8s.io/fsx-csi-external-provisioner-role created  
clusterrole.rbac.authorization.k8s.io/fsx-external-resizer-role created  
clusterrolebinding.rbac.authorization.k8s.io/fsx-csi-external-provisioner-binding created  
clusterrolebinding.rbac.authorization.k8s.io/fsx-csi-resizer-binding created  
deployment.apps/fsx-csi-controller created  
daemonset.apps/fsx-csi-node created  
csidriver.storage.k8s.io/fsx.csi.aws.com created
```

5. Note the ARN for the role that was created. If you didn't note it earlier and don't have it available anymore in the AWS CLI output, you can do the following to see it in the AWS Management Console.
 - a. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
 - b. Ensure that the console is set to the AWS Region that you created your IAM role in and then select **Stacks**.
 - c. Select the stack named eksctl-*my-csi-fsx-cluster*-addon-iamserviceaccount-kube-system-*fsx-csi-controller-sa*.
 - d. Select the **Outputs** tab. The **Role1** ARN is listed on the **Outputs (1)** page.
6. Patch the driver deployment to add the service account that you created earlier with the following command. Replace the ARN with the ARN that you noted. Replace *111122223333* with your account ID. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

```
kubectl annotate serviceaccount -n kube-system fsx-csi-controller-sa \ eks.amazonaws.com/role- arn=arn:aws:iam::111122223333:role/AmazonEKSFSxLustreCSIDriverFullAccess -- overwrite=true
```

An example output is as follows.

```
serviceaccount/fsx-csi-controller-sa annotated
```

To deploy a Kubernetes storage class, persistent volume claim, and sample application to verify that the CSI driver is working

This procedure uses the [FSx for Lustre Container Storage Interface \(CSI\) driver](#) GitHub repository to consume a dynamically-provisioned FSx for Lustre volume.

1. Note the security group for your cluster. You can see it in the AWS Management Console under the **Networking** section or by using the following AWS CLI command.

```
aws eks describe-cluster --name $cluster_name --query
cluster.resourcesVpcConfig.clusterSecurityGroupId
```

2. Create a security group for your Amazon FSx file system according to the criteria shown in [Amazon VPC Security Groups](#) in the Amazon FSx for Lustre User Guide. For the **VPC**, select the VPC of your cluster as shown under the **Networking** section. For "the security groups associated with your Lustre clients", use your cluster security group. You can leave the outbound rules alone to allow **All traffic**.
3. Download the storage class manifest with the following command.

```
curl -0 https://raw.githubusercontent.com/kubernetes-sigs/aws-fsx-csi-driver/master/
examples/kubernetes/dynamic_provisioning/specs/storageclass.yaml
```

4. Edit the parameters section of the `storageclass.yaml` file. Replace every *example value* with your own values.

```
parameters:
  subnetId: subnet-0eabfaa81fb22bcf
  securityGroupIds: sg-068000ccf82dfba88
  deploymentType: PERSISTENT_1
  automaticBackupRetentionDays: "1"
  dailyAutomaticBackupStartTime: "00:00"
  copyTagsToBackups: "true"
  perUnitStorageThroughput: "200"
  dataCompressionType: "NONE"
  weeklyMaintenanceStartTime: "7:09:00"
  fileSystemTypeVersion: "2.12"
```

- **subnetId** – The subnet ID that the Amazon FSx for Lustre file system should be created in. Amazon FSx for Lustre isn't supported in all Availability Zones. Open the Amazon FSx for Lustre console at <https://console.aws.amazon.com/fsx/> to confirm that the subnet that you want to use is in a supported Availability Zone. The subnet can include your nodes, or can be a different subnet or VPC:
 - You can check for the node subnets in the AWS Management Console by selecting the node group under the **Compute** section.
 - If the subnet that you specify isn't the same subnet that you have nodes in, then your VPCs must be [connected](#), and you must ensure that you have the necessary ports open in your security groups.
- **securityGroupIds** – The ID of the security group you created for the file system.
- **deploymentType (optional)** – The file system deployment type. Valid values are SCRATCH_1, SCRATCH_2, PERSISTENT_1, and PERSISTENT_2. For more information about deployment types, see [Create your Amazon FSx for Lustre file system](#).
- **other parameters (optional)** – For information about the other parameters, see [Edit StorageClass](#) on GitHub.

5. Create the storage class manifest.

```
kubectl apply -f storageclass.yaml
```

An example output is as follows.

```
storageclass.storage.k8s.io/fsx-sc created
```

6. Download the persistent volume claim manifest.

```
curl -0 https://raw.githubusercontent.com/kubernetes-sigs/aws-fsx-csi-driver/master/examples/kubernetes/dynamic_provisioning/specs/claim.yaml
```

7. (Optional) Edit the `claim.yaml` file. Change `1200Gi` to one of the following increment values, based on your storage requirements and the `deploymentType` that you selected in a previous step.

```
storage: 1200Gi
```

- SCRATCH_2 and PERSISTENT – **1.2 TiB, 2.4 TiB**, or increments of 2.4 TiB over 2.4 TiB.
- SCRATCH_1 – **1.2 TiB, 2.4 TiB, 3.6 TiB**, or increments of 3.6 TiB over 3.6 TiB.

8. Create the persistent volume claim.

```
kubectl apply -f claim.yaml
```

An example output is as follows.

```
persistentvolumeclaim/fsx-claim created
```

9. Confirm that the file system is provisioned.

```
kubectl describe pvc
```

An example output is as follows.

```
Name:           fsx-claim
Namespace:      default
StorageClass:   fsx-sc
Status:         Bound
[...]
```

Note

The Status may show as Pending for 5-10 minutes, before changing to Bound. Don't continue with the next step until the Status is Bound. If the Status shows Pending for more than 10 minutes, use warning messages in the Events as reference for addressing any problems.

10. Deploy the sample application.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/aws-fsx-csi-driver/master/examples/kubernetes/dynamic_provisioning/specs/pod.yaml
```

11. Verify that the sample application is running.

```
kubectl get pods
```

An example output is as follows.

NAME	READY	STATUS	RESTARTS	AGE
------	-------	--------	----------	-----

fsx-app	1/1	Running	0	8s
---------	-----	---------	---	----

12. Verify that the file system is mounted correctly by the application.

<code>kubectl exec -ti fsx-app -- df -h</code>
--

An example output is as follows.

Filesystem	Size	Used	Avail	Use%	Mounted on
overlay	80G	4.0G	77G	5%	/
tmpfs	64M	0	64M	0%	/dev
tmpfs	3.8G	0	3.8G	0%	/sys/fs/cgroup
192.0.2.0@tcp:/abcdef01	1.1T	7.8M	1.1T	1%	/data
/dev/nvme0n1p1	80G	4.0G	77G	5%	/etc/hosts
shm	64M	0	64M	0%	/dev/shm
tmpfs	6.9G	12K	6.9G	1%	/run/secrets/kubernetes.io/serviceaccount
tmpfs	3.8G	0	3.8G	0%	/proc/acpi
tmpfs	3.8G	0	3.8G	0%	/sys/firmware

13. Verify that data was written to the FSx for Lustre file system by the sample app.

<code>kubectl exec -it fsx-app -- ls /data</code>

An example output is as follows.

out.txt

This example output shows that the sample app successfully wrote the `out.txt` file to the file system.

Note

Before deleting the cluster, make sure to delete the FSx for Lustre file system. For more information, see [Clean up resources](#) in the *FSx for Lustre User Guide*.

Amazon FSx for NetApp ONTAP CSI driver

NetApp's Astra Trident provides dynamic storage orchestration using a Container Storage Interface (CSI) compliant driver. This allows Amazon EKS clusters to manage the lifecycle of persistent volumes (PVs) backed by Amazon FSx for NetApp ONTAP file systems. To get started, see [Use Astra Trident with Amazon FSx for NetApp ONTAP](#) in the Astra Trident documentation.

Amazon FSx for NetApp ONTAP is a storage service that allows you to launch and run fully managed ONTAP file systems in the cloud. ONTAP is NetApp's file system technology that provides a widely adopted set of data access and data management capabilities. Amazon FSx for NetApp ONTAP provides the features, performance, and APIs of on-premises NetApp file systems with the agility, scalability, and simplicity of a fully managed AWS service. For more information, see the [FSx for ONTAP User Guide](#).

Amazon FSx for OpenZFS CSI driver

Amazon FSx for OpenZFS is a fully managed file storage service that makes it easy to move data to AWS from on-premises ZFS or other Linux-based file servers. You can do this without changing your

application code or how you manage data. It offers highly reliable, scalable, efficient, and feature-rich file storage built on the open-source OpenZFS file system. It combines these capabilities with the agility, scalability, and simplicity of a fully managed AWS service. For more information, see the [Amazon FSx for OpenZFS User Guide](#).

The Amazon FSx for OpenZFS Container Storage Interface (CSI) driver provides a CSI interface that allows Amazon EKS clusters to manage the life cycle of Amazon FSx for OpenZFS volumes. To deploy the Amazon FSx for OpenZFS CSI driver to your Amazon EKS cluster, see [aws-fsx-openzfs-csi-driver](#) on GitHub.

Amazon File Cache CSI driver

Amazon File Cache is a fully managed, high-speed cache on AWS that's used to process file data, regardless of where the data is stored. Amazon File Cache automatically loads data into the cache when it's accessed for the first time and releases data when it's not used. For more information, see the [Amazon File Cache User Guide](#).

The Amazon File Cache Container Storage Interface (CSI) driver provides a CSI interface that allows Amazon EKS clusters to manage the life cycle of Amazon file caches. To deploy the Amazon File Cache CSI driver to your Amazon EKS cluster, see [aws-file-cache-csi-driver](#) on GitHub.

Amazon EKS networking

Your Amazon EKS cluster is created in a VPC. Pod networking is provided by the Amazon VPC Container Network Interface (CNI) plugin. This chapter includes the following topics for learning more about networking for your cluster.

Topics

- [Amazon EKS VPC and subnet requirements and considerations \(p. 256\)](#)
- [Creating a VPC for your Amazon EKS cluster \(p. 259\)](#)
- [Amazon EKS security group requirements and considerations \(p. 263\)](#)
- [Amazon EKS networking add-ons \(p. 265\)](#)
- [Access the Amazon Elastic Kubernetes Service using an interface endpoint \(AWS PrivateLink\) \(p. 353\)](#)

Amazon EKS VPC and subnet requirements and considerations

When you create a cluster, you specify a [VPC](#) and at least two subnets that are in different Availability Zones. This topic provides an overview of Amazon EKS specific requirements and considerations for the VPC and subnets that you use with your cluster. If you don't have a VPC to use with Amazon EKS, you can [create one using an Amazon EKS provided AWS CloudFormation template \(p. 259\)](#). If you're creating a local or extended cluster on AWS Outposts, see [the section called "VPC and subnet requirements" \(p. 601\)](#) instead of this topic.

VPC requirements and considerations

When you create a cluster, the VPC that you specify must meet the following requirements and considerations:

- The VPC must have a sufficient number of IP addresses available for the cluster, any nodes, and other Kubernetes resources that you want to create. If the VPC that you want to use doesn't have a sufficient number of IP addresses, try to increase the number of available IP addresses. You can do this by [associating additional Classless Inter-Domain Routing \(CIDR\) blocks](#) with your VPC. You can associate private (RFC 1918) and public (non-RFC 1918) CIDR blocks to your VPC either before or after you create your cluster. It can take a cluster up to five hours for a CIDR block that you associated with a VPC to be recognized.

You can conserve IP address utilization by using a transit gateway with a shared services VPC. For more information, see [Isolated VPCs with shared services](#) and [Amazon EKS VPC routable IP address conservation patterns in a hybrid network](#).

- If you want Kubernetes to assign IPv6 addresses to Pods and services, associate an IPv6 CIDR block with your VPC. For more information, see [Associate an IPv6 CIDR block with your VPC](#) in the Amazon VPC User Guide.
- The VPC must have DNS hostname and DNS resolution support. Otherwise, nodes can't register to your cluster. For more information, see [DNS attributes for your VPC](#) in the Amazon VPC User Guide.
- The VPC might require VPC endpoints using AWS PrivateLink. For more information, see [the section called "Subnet requirements and considerations" \(p. 257\)](#).

If you created a cluster with Kubernetes 1.14 or earlier, Amazon EKS added the following tag to your VPC:

Key	Value
kubernetes.io/cluster/ <i>my-cluster</i>	owned

This tag was only used by Amazon EKS. You can remove the tag without impacting your services. It's not used with clusters that are version 1.15 or later.

Subnet requirements and considerations

When you create a cluster, Amazon EKS creates 2–4 [elastic network interfaces](#) in the subnets that you specify. These network interfaces enable communication between your cluster and your VPC. These network interfaces also enable Kubernetes features such as `kubectl exec` and `kubectl logs`. Each Amazon EKS created network interface has the text Amazon EKS *cluster-name* in its description.

Amazon EKS can create its network interfaces in any subnet that you specify when you create a cluster. You can't change which subnets Amazon EKS creates its network interfaces in after your cluster is created. When you update the Kubernetes version of a cluster, Amazon EKS deletes the original network interfaces that it created, and creates new network interfaces. These network interfaces might be created in the same subnets as the original network interfaces or in different subnets than the original network interfaces. To control which subnets network interfaces are created in, you can limit the number of subnets you specify to only two when you create a cluster.

The [subnets](#) that you specify when you create a cluster must meet the following requirements:

- The subnets must each have at least six IP addresses for use by Amazon EKS. However, we recommend at least 16 IP addresses.
- The subnets can't reside in AWS Outposts, AWS Wavelength, or an AWS Local Zone. However, if you have them in your VPC, you can deploy [self-managed nodes \(p. 108\)](#) and Kubernetes resources to these types of subnets.
- The subnets can be a public or private. However, we recommend that you specify private subnets, if possible. A public subnet is a subnet with a route table that includes a route to an [internet gateway](#), whereas a private subnet is a subnet with a route table that doesn't include a route to an internet gateway.

You can deploy nodes and Kubernetes resources to the same subnets that you specify when you create your cluster. However, this isn't necessary. This is because you can also deploy nodes and Kubernetes resources to subnets that you didn't specify when you created the cluster. If you deploy nodes to different subnets, Amazon EKS doesn't create cluster network interfaces in those subnets. Any subnet that you deploy nodes and Kubernetes resources to must meet the following requirements:

- The subnets must have enough available IP addresses to deploy all of your nodes and Kubernetes resources to.
- If you want Kubernetes to assign IPv6 addresses to Pods and services, then you must have one IPv6 CIDR block and one IPv4 CIDR block that are associated with your subnet. For more information, see [Associate an IPv6 CIDR block with your subnet](#) in the Amazon VPC User Guide. The route tables that are associated with the subnets must include routes to IPv4 and IPv6 addresses. For more information, see [Routes](#) in the Amazon VPC User Guide. Pods are assigned only an IPv6 address. However the network interfaces that Amazon EKS creates for your cluster and your nodes are assigned an IPv4 and an IPv6 address.
- If you need inbound access from the internet to your Pods, make sure to have at least one public subnet with enough available IP addresses to deploy load balancers and ingresses to. You can deploy

load balancers to public subnets. Load balancers can load balance to Pods in private or public subnets. We recommend deploying your nodes to private subnets, if possible.

- If you plan to deploy nodes to a public subnet, the subnet must auto-assign IPv4 public addresses or IPv6 addresses. If you deploy nodes to a private subnet that has an associated IPv6 CIDR block, the private subnet must also auto-assign IPv6 addresses. If you used an [Amazon EKS AWS CloudFormation template \(p. 259\)](#) to deploy your VPC after March 26, 2020, this setting is enabled. If you used the templates to deploy your VPC before this date or you use your own VPC, you must enable this setting manually. For more information, see [Modify the public IPv4 addressing attribute for your subnet](#) and [Modify the IPv6 addressing attribute for your subnet](#) in the [Amazon VPC User Guide](#).
- If the subnet that you deploy a node to is a private subnet and its route table doesn't include a route to a network address translation ([NAT device](#)) (IPv4) or an [egress-only gateway](#) (IPv6), add VPC endpoints using AWS PrivateLink to your VPC. VPC endpoints are needed for all the AWS services that your nodes and Pods need to communicate with. Examples include Amazon ECR, Elastic Load Balancing, Amazon CloudWatch, AWS Security Token Service, and Amazon Simple Storage Service (Amazon S3). The endpoint must include the subnet that the nodes are in. Not all AWS services support VPC endpoints. For more information, see [What is AWS PrivateLink?](#) and [AWS services that integrate with AWS PrivateLink](#). For a list of more Amazon EKS requirements, see the section called ["Private cluster requirements" \(p. 58\)](#).
- If you want to deploy load balancers to a subnet, the subnet must have the following tag:
 - Private subnets

Key	Value
kubernetes.io/role/internal-elb	1

- Public subnets

Key	Value
kubernetes.io/role/elb	1

When a Kubernetes cluster that's version 1.18 and earlier was created, Amazon EKS added the following tag to all of the subnets that were specified.

Key	Value
kubernetes.io/cluster/ <i>my-cluster</i>	shared

When you create a new Kubernetes cluster now, Amazon EKS doesn't add the tag to your subnets. If the tag was on subnets that were used by a cluster that was previously a version earlier than 1.19, the tag wasn't automatically removed from the subnets when the cluster was updated to a newer version. Version 2.1.1 or earlier of the [AWS Load Balancer Controller \(p. 333\)](#) requires this tag. If you are using a newer version of the Load Balancer Controller, you can remove the tag without interrupting your services.

If you deployed a VPC by using `eksctl` or any of the Amazon EKS AWS CloudFormation VPC templates, the following applies:

- **On or after March 26, 2020** – Public IPv4 addresses are automatically assigned by public subnets to new nodes that are deployed to public subnets.
- **Before March 26, 2020** – Public IPv4 addresses aren't automatically assigned by public subnets to new nodes that are deployed to public subnets.

This change impacts new node groups that are deployed to public subnets in the following ways:

- **Managed node groups (p. 85)** – If the node group is deployed to a public subnet on or after April 22, 2020, automatic assignment of public IP addresses must be enabled for the public subnet. For more information, see [Modifying the public IPv4 addressing attribute for your subnet](#).
- **Linux (p. 108), Windows (p. 117), or Arm (p. 160) self-managed node groups** – If the node group is deployed to a public subnet on or after March 26, 2020, automatic assignment of public IP addresses must be enabled for the public subnet. Otherwise, the nodes must be launched with a public IP address instead. For more information, see [Modifying the public IPv4 addressing attribute for your subnet](#) or [Assigning a public IPv4 address during instance launch](#).

Shared subnet requirements and considerations

You can use *VPC sharing* to share subnets with other AWS accounts within the same AWS Organizations. You can create Amazon EKS clusters in shared subnets, with the following considerations:

- The owner of the VPC subnet must share a subnet with a participant account before that account can create an Amazon EKS cluster in it.
- You can't launch resources using the default security group for the VPC because it belongs to the owner. Additionally, participants can't launch resources using security groups that are owned by other participants or the owner.
- In a shared subnet, the participant and the owner separately controls the security groups within each respective account. The subnet owner can see security groups that are created by the participants but cannot perform any actions on them. If the subnet owner wants to remove or modify these security groups, the participant that created the security group must take the action.
- If a cluster is created by a participant, the following considerations apply:
 - Cluster IAM role and Node IAM roles must be created in that account. For more information, see [Amazon EKS cluster IAM role \(p. 499\)](#) and [Amazon EKS node IAM role \(p. 501\)](#).
 - All nodes must be made by the same participant, including managed node groups.
- The shared VPC owner cannot view, update or delete a cluster that a participant creates in the shared subnet. This is in addition to the VPC resources that each account has different access to. For more information, see [Responsibilities and permissions for owners and participants](#) in the *Amazon VPC User Guide*.
- If you use the *custom networking* feature of the Amazon VPC CNI plugin for Kubernetes, you need to use the Availability Zone ID mappings listed in the owner account to create each ENIConfig. For more information, see [Custom networking for pods \(p. 306\)](#).

For more information about VPC subnet sharing, see [Share your VPC with other accounts](#) in the *Amazon VPC User Guide*.

Creating a VPC for your Amazon EKS cluster

You can use Amazon Virtual Private Cloud (Amazon VPC) to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you might operate in your own data center. However, it comes with the benefits of using the scalable infrastructure of Amazon Web Services. We recommend that you have a thorough understanding of the Amazon VPC service before deploying production Amazon EKS clusters. For more information, see the [Amazon VPC User Guide](#).

An Amazon EKS cluster, nodes, and Kubernetes resources are deployed to a VPC. If you want to use an existing VPC with Amazon EKS, that VPC must meet the requirements that are described in [the section called "VPC and subnet requirements" \(p. 256\)](#). This topic describes how to create a VPC that meets

Amazon EKS requirements using an Amazon EKS provided AWS CloudFormation template. Once you've deployed a template, you can view the resources created by the template to know exactly what resources it created, and the configuration of those resources.

Prerequisite

To create a VPC for Amazon EKS, you must have the necessary IAM permissions to create Amazon VPC resources. These resources are VPCs, subnets, security groups, route tables and routes, and internet and NAT gateways. For more information, see [Create a VPC with a public subnet example policy](#) in the Amazon VPC User Guide and the full list of [Actions, resources, and condition keys for Amazon EC2](#) in the [Service Authorization Reference](#).

You can create a VPC with public and private subnets, only public subnets, or only private subnets.

Public and private subnets

This VPC has two public and two private subnets. A public subnet's associated route table has a route to an internet gateway. However, the route table of a private subnet doesn't have a route to an internet gateway. One public and one private subnet are deployed to the same Availability Zone. The other public and private subnets are deployed to a second Availability Zone in the same AWS Region. We recommend this option for most deployments.

With this option, you can deploy your nodes to private subnets. This option allows Kubernetes to deploy load balancers to the public subnets that can load balance traffic to Pods that run on nodes in the private subnets. Public IPv4 addresses are automatically assigned to nodes that are deployed to public subnets, but public IPv4 addresses aren't assigned to nodes deployed to private subnets.

You can also assign IPv6 addresses to nodes in public and private subnets. The nodes in private subnets can communicate with the cluster and other AWS services. Pods can communicate to the internet through a NAT gateway using IPv4 addresses or outbound-only Internet gateway using IPv6 addresses deployed in each Availability Zone. A security group is deployed that has rules that deny all inbound traffic from sources other than the cluster or nodes but allows all outbound traffic. The subnets are tagged so that Kubernetes can deploy load balancers to them.

To create your VPC

1. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
2. From the navigation bar, select an AWS Region that supports Amazon EKS.
3. Choose **Create stack, With new resources (standard)**.
4. Under **Prerequisite - Prepare template**, make sure that **Template is ready** is selected and then under **Specify template**, select **Amazon S3 URL**.
5. You can create a VPC that supports only IPv4, or a VPC that supports IPv4 and IPv6. Paste one of the following URLs into the text area under **Amazon S3 URL** and choose **Next**:
 - IPv4

`https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/amazon-eks-vpc-private-subnets.yaml`
 - IPv4 and IPv6

`https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/amazon-eks-ipv6-vpc-public-private-subnets.yaml`
6. On the **Specify stack details** page, enter the parameters, and then choose **Next**.
 - **Stack name:** Choose a stack name for your AWS CloudFormation stack. For example, you can use the template name you used in the previous step. The name can contain only

alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters.

- **VpcBlock:** Choose an IPv4 CIDR range for your VPC. Each node, Pod, and load balancer that you deploy is assigned an IPv4 address from this block. The default IPv4 values provide enough IP addresses for most implementations, but if it doesn't, then you can change it. For more information, see [VPC and subnet sizing](#) in the Amazon VPC User Guide. You can also add additional CIDR blocks to the VPC once it's created. If you're creating an IPv6 VPC, IPv6 CIDR ranges are automatically assigned for you from Amazon's Global Unicast Address space.
 - **PublicSubnet01Block:** Specify an IPv4 CIDR block for public subnet 1. The default value provides enough IP addresses for most implementations, but if it doesn't, then you can change it. If you're creating an IPv6 VPC, this block is specified for you within the template.
 - **PublicSubnet02Block:** Specify an IPv4 CIDR block for public subnet 2. The default value provides enough IP addresses for most implementations, but if it doesn't, then you can change it. If you're creating an IPv6 VPC, this block is specified for you within the template.
 - **PrivateSubnet01Block:** Specify an IPv4 CIDR block for private subnet 1. The default value provides enough IP addresses for most implementations, but if it doesn't, then you can change it. If you're creating an IPv6 VPC, this block is specified for you within the template.
 - **PrivateSubnet02Block:** Specify an IPv4 CIDR block for private subnet 2. The default value provides enough IP addresses for most implementations, but if it doesn't, then you can change it. If you're creating an IPv6 VPC, this block is specified for you within the template.
7. (Optional) On the **Configure stack options** page, tag your stack resources and then choose **Next**.
 8. On the **Review** page, choose **Create stack**.
 9. When your stack is created, select it in the console and choose **Outputs**.
 10. Record the **VpcId** for the VPC that was created. You need this when you create your cluster and nodes.
 11. Record the **SubnetIds** for the subnets that were created and whether you created them as public or private subnets. You need at least two of these when you create your cluster and nodes.
 12. If you created an IPv4 VPC, skip this step. If you created an IPv6 VPC, you must enable the auto-assign IPv6 address option for the public subnets that were created by the template. That setting is already enabled for the private subnets. To enable the setting, complete the following steps:
 - a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. In the left navigation pane, choose **Subnets**
 - c. Select one of your public subnets (**stack-name/SubnetPublic01** or **stack-name/SubnetPublic02** contains the word **public**) and choose **Actions, Edit subnet settings**.
 - d. Choose the **Enable auto-assign IPv6 address** check box and then choose **Save**.
 - e. Complete the previous steps again for your other public subnet.

Only public subnets

This VPC has three public subnets that are deployed into different Availability Zones in an AWS Region. All nodes are automatically assigned public IPv4 addresses and can send and receive internet traffic through an [internet gateway](#). A [security group](#) is deployed that denies all inbound traffic and allows all outbound traffic. The subnets are tagged so that Kubernetes can deploy load balancers to them.

To create your VPC

1. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.

2. From the navigation bar, select an AWS Region that supports Amazon EKS.
3. Choose **Create stack, With new resources (standard)**.
4. Under **Prepare template**, make sure that **Template is ready** is selected and then under **Template source**, select **Amazon S3 URL**.
5. Paste the following URL into the text area under **Amazon S3 URL** and choose **Next**:

```
https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/amazon-eks-vpc-sample.yaml
```

6. On the **Specify Details** page, enter the parameters, and then choose **Next**.
 - **Stack name:** Choose a stack name for your AWS CloudFormation stack. For example, you can call it **amazon-eks-vpc-sample**. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters.
 - **VpcBlock:** Choose a CIDR block for your VPC. Each node, Pod, and load balancer that you deploy is assigned an IPv4 address from this block. The default IPv4 values provide enough IP addresses for most implementations, but if it doesn't, then you can change it. For more information, see [VPC and subnet sizing](#) in the Amazon VPC User Guide. You can also add additional CIDR blocks to the VPC once it's created.
 - **Subnet01Block:** Specify a CIDR block for subnet 1. The default value provides enough IP addresses for most implementations, but if it doesn't, then you can change it.
 - **Subnet02Block:** Specify a CIDR block for subnet 2. The default value provides enough IP addresses for most implementations, but if it doesn't, then you can change it.
 - **Subnet03Block:** Specify a CIDR block for subnet 3. The default value provides enough IP addresses for most implementations, but if it doesn't, then you can change it.
7. (Optional) On the **Options** page, tag your stack resources. Choose **Next**.
8. On the **Review** page, choose **Create**.
9. When your stack is created, select it in the console and choose **Outputs**.
10. Record the **VpcId** for the VPC that was created. You need this when you create your cluster and nodes.
11. Record the **SubnetIds** for the subnets that were created. You need at least two of these when you create your cluster and nodes.
12. (Optional) Any cluster that you deploy to this VPC can assign private IPv4 addresses to your Pods and services. If you want to deploy clusters to this VPC to assign private IPv6 addresses to your Pods and services, make updates to your VPC, subnet, route tables, and security groups. For more information, see [Migrate existing VPCs from IPv4 to IPv6](#) in the Amazon VPC User Guide. Amazon EKS requires that your subnets have the Auto-assign IPv6 addresses option enabled. By default, it's disabled.

Only private subnets

This VPC has three private subnets that are deployed into different Availability Zones in the AWS Region. Resources that are deployed to the subnets can't access the internet, nor can the internet access resources in the subnets. The template creates [VPC endpoints](#) using AWS PrivateLink for several AWS services that nodes typically need to access. If your nodes need outbound internet access, you can add a public [NAT gateway](#) in the Availability Zone of each subnet after the VPC is created. A [security group](#) is created that denies all inbound traffic, except from resources deployed into the subnets. A security group also allows all outbound traffic. The subnets are tagged so that Kubernetes can deploy internal load balancers to them. If you're creating a VPC with this configuration, see the section called ["Private cluster requirements" \(p. 58\)](#) for additional requirements and considerations.

To create your VPC

1. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
2. From the navigation bar, select an AWS Region that supports Amazon EKS.
3. Choose **Create stack, With new resources (standard)**.
4. Under **Prepare template**, make sure that **Template is ready** is selected and then under **Template source**, select **Amazon S3 URL**.
5. Paste the following URL into the text area under **Amazon S3 URL** and choose **Next**:

`https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/amazon-eks-fully-private-vpc.yaml`
6. On the **Specify Details** page, enter the parameters and then choose **Next**.
 - **Stack name:** Choose a stack name for your AWS CloudFormation stack. For example, you can call it **amazon-eks-fully-private-vpc**. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters.
 - **VpcBlock:** Choose a CIDR block for your VPC. Each node, Pod, and load balancer that you deploy is assigned an IPv4 address from this block. The default IPv4 values provide enough IP addresses for most implementations, but if it doesn't, then you can change it. For more information, see [VPC and subnet sizing](#) in the Amazon VPC User Guide. You can also add additional CIDR blocks to the VPC once it's created.
 - **PrivateSubnet01Block:** Specify a CIDR block for subnet 1. The default value provides enough IP addresses for most implementations, but if it doesn't, then you can change it.
 - **PrivateSubnet02Block:** Specify a CIDR block for subnet 2. The default value provides enough IP addresses for most implementations, but if it doesn't, then you can change it.
 - **PrivateSubnet03Block:** Specify a CIDR block for subnet 3. The default value provides enough IP addresses for most implementations, but if it doesn't, then you can change it.
7. (Optional) On the **Options** page, tag your stack resources. Choose **Next**.
8. On the **Review** page, choose **Create**.
9. When your stack is created, select it in the console and choose **Outputs**.
10. Record the **VpcId** for the VPC that was created. You need this when you create your cluster and nodes.
11. Record the **SubnetIds** for the subnets that were created. You need at least two of these when you create your cluster and nodes.
12. (Optional) Any cluster that you deploy to this VPC can assign private IPv4 addresses to your Pods and services. If you want deploy clusters to this VPC to assign private IPv6 addresses to your Pods and services, make updates to your VPC, subnet, route tables, and security groups. For more information, see [Migrate existing VPCs from IPv4 to IPv6](#) in the Amazon VPC User Guide. Amazon EKS requires that your subnets have the Auto-assign IPv6 addresses option enabled (it's disabled by default).

Amazon EKS security group requirements and considerations

This topic describes the security group requirements of an Amazon EKS cluster.

When you create a cluster, Amazon EKS creates a security group that's named `eks-cluster-sg-my-cluster-uniqueID`. This security group has the following default rules:

Rule type	Protocol	Ports	Source	Destination
Inbound	All	All	Self	
Outbound	All	All		0.0.0.0/0 (IPv4) or ::/0 (IPv6)

Important

If your cluster doesn't need the outbound rule, you can remove it. If you remove it, you must still have the minimum rules listed in [Restricting cluster traffic \(p. 264\)](#). If you remove the inbound rule, Amazon EKS recreates it whenever the cluster is updated.

Amazon EKS adds the following tags to the security group. If you remove the tags, Amazon EKS adds them back to the security group whenever your cluster is updated.

Key	Value
kubernetes.io/cluster/ <i>my-cluster</i>	owned
aws:eks:cluster-name	<i>my-cluster</i>
Name	eks-cluster-sg- <i>my-cluster-uniqueid</i>

Amazon EKS automatically associates this security group to the following resources that it also creates:

- 2–4 elastic network interfaces (referred to for the rest of this document as *network interface*) that are created when you create your cluster.
- Network interfaces of the nodes in any managed node group that you create.

The default rules allow all traffic to flow freely between your cluster and nodes, and allows all outbound traffic to any destination. When you create a cluster, you can (optionally) specify your own security groups. If you do, then Amazon EKS also associates the security groups that you specify to the network interfaces that it creates for your cluster. However, it doesn't associate them to any node groups that you create.

You can determine the ID of your cluster security group in the AWS Management Console under the cluster's **Networking** section. Or, you can do so by running the following AWS CLI command.

```
aws eks describe-cluster --name my-cluster --query
cluster.resourcesVpcConfig.clusterSecurityGroupId
```

Restricting cluster traffic

If you need to limit the open ports between the cluster and nodes, you can remove the [default outbound rule \(p. 263\)](#) and add the following minimum rules that are required for the cluster. If you remove the [default inbound rule \(p. 263\)](#), Amazon EKS recreates it whenever the cluster is updated.

Rule type	Protocol	Port	Destination
Outbound	TCP	443	Cluster security group
Outbound	TCP	10250	Cluster security group

Rule type	Protocol	Port	Destination
Outbound (DNS)	TCP and UDP	53	Cluster security group

You must also add rules for the following traffic:

- Any protocol and ports that you expect your nodes to use for inter-node communication.
- Outbound internet access so that nodes can access the Amazon EKS APIs for cluster introspection and node registration at launch time. If your nodes don't have internet access, review [Private cluster requirements \(p. 58\)](#) for additional considerations.
- Node access to pull container images from Amazon ECR or other container registries APIs that they need to pull images from, such as DockerHub. For more information, see [AWS IP address ranges](#) in the AWS General Reference.
- Node access to Amazon S3.
- Separate rules are required for IPv4 and IPv6 addresses.

If you're considering limiting the rules, we recommend that you thoroughly test all of your Pods before you apply your changed rules to a production cluster.

If you originally deployed a cluster with Kubernetes 1.14 and a platform version of eks .3 or earlier, then consider the following:

- You might also have control plane and node security groups. When these groups were created, they included the restricted rules listed in the previous table. These security groups are no longer required and can be removed. However, you need to make sure your cluster security group contains the rules that those groups contain.
- If you deployed the cluster using the API directly or you used a tool such as the AWS CLI or AWS CloudFormation to create the cluster and you didn't specify a security group at cluster creation, then the default security group for the VPC was applied to the cluster network interfaces that Amazon EKS created.

Amazon EKS networking add-ons

Several networking add-ons are available for your Amazon EKS cluster.

Built-in add-ons

Note

If you create clusters in any way except by using the console, each cluster comes with the self-managed versions of the built-in add-ons. The self-managed versions can't be managed from the AWS Management Console, AWS Command Line Interface, or SDKs. You manage the configuration and upgrades of self-managed add-ons.

We recommend adding the Amazon EKS type of the add-on to your cluster instead of using the self-managed type of the add-on. If you create clusters in the console, the Amazon EKS type of these add-ons is installed.

Amazon VPC CNI plugin for Kubernetes

This CNI add-on creates elastic network interfaces and attaches them to your Amazon EC2 nodes. The add-on also assigns a private IPv4 or IPv6 address from your VPC to each Pod and service. This add-on is installed, by default, on your cluster. For more information, see [the section called "Amazon VPC CNI plugin for Kubernetes" \(p. 266\)](#).

CoreDNS

CoreDNS is a flexible, extensible DNS server that can serve as the Kubernetes cluster DNS. CoreDNS provides name resolution for all Pods in the cluster. This add-on is installed, by default, on your cluster. For more information, see [the section called "CoreDNS" \(p. 341\)](#).

kube-proxy

This add-on maintains network rules on your Amazon EC2 nodes and enables network communication to your Pods. This add-on is installed, by default, on your cluster. For more information, see [Updating the Kubernetes kube-proxy self-managed add-on \(p. 347\)](#).

Optional AWS networking add-ons

AWS Load Balancer Controller

When you deploy Kubernetes service objects of type `loadbalancer`, the controller creates AWS Network Load Balancers. When you create Kubernetes ingress objects, the controller creates AWS Application Load Balancers. We recommend using this controller to provision Network Load Balancers, rather than using the [legacy Cloud Provider](#) controller built-in to Kubernetes. For more information, see the [AWS Load Balancer Controller](#) documentation.

AWS Gateway API Controller

This controller lets you connect services across multiple Kubernetes clusters using the [Kubernetes gateway API](#). The controller connects Kubernetes services running on Amazon EC2 instances, containers, and serverless functions by using the [Amazon VPC Lattice](#) service. For more information, see the [AWS Gateway API Controller](#) documentation.

Additional networking add-ons

Calico network policy engine

This add-on is a network policy engine for Kubernetes. With Calico network policy enforcement, you can implement network segmentation and tenant isolation. This is useful in multi-tenant environments where you must isolate tenants from each other or when you want to create separate environments for development, staging, and production. For more information, see [the section called "Calico network policy engine" \(p. 350\)](#).

For more information about add-ons, see [Amazon EKS add-ons \(p. 385\)](#).

Working with the Amazon VPC CNI plugin for Kubernetes Amazon EKS add-on

The Amazon VPC CNI plugin for Kubernetes add-on is deployed on each Amazon EC2 node in your Amazon EKS cluster. The add-on creates [elastic network interfaces](#) and attaches them to your Amazon EC2 nodes. The add-on also assigns a private IPv4 or IPv6 address from your VPC to each Pod and service.

A version of the add-on is deployed with each Fargate node in your cluster, but you don't update it on Fargate nodes. [Other compatible CNI plugins \(p. 332\)](#) are available for use on Amazon EKS clusters, but this is the only CNI plugin supported by Amazon EKS.

The following table lists the latest available version of the Amazon EKS add-on type for each Kubernetes version.

Kubernetes version	1.28	1.27	1.26	1.25	1.24	1.23
Amazon EKS type of VPC CNI version	v1.15.0-eksbuild.2	v1.15.0-eksbuild.2	v1.15.0-eksbuild.2	v1.15.0-eksbuild.2	v1.15.0-eksbuild.2	v1.15.0-eksbuild.2

Important

If you're self-managing this add-on, the versions in the table might not be the same as the available self-managed versions. For more information about updating the self-managed type of this add-on, see [the section called "Updating the self-managed add-on" \(p. 270\)](#).

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Getting started with Amazon EKS \(p. 6\)](#).
- An existing AWS Identity and Access Management (IAM) OpenID Connect (OIDC) provider for your cluster. To determine whether you already have one, or to create one, see [Creating an IAM OIDC provider for your cluster \(p. 465\)](#).
- An IAM role with the [AmazonEKS_CNI_Policy](#) IAM policy (if your cluster uses the IPv4 family) or an [IPv6 policy \(p. 276\)](#) (if your cluster uses the IPv6 family) attached to it. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).
- If you're using version 1.7.0 or later of the Amazon VPC CNI plugin for Kubernetes and you use custom Pod security policies, see [the section called "Delete default policy" \(p. 523\)Pod security policy \(p. 522\)](#).

Considerations

- Versions are specified as major-version.minor-version.patch-version-eksbuild.build-number.
- You can only update the Amazon EKS type of this add-on one *minor* version at a time. For example, if your current version is v1.13.4-eksbuild.1 and you want to update to v1.15.0-eksbuild.2, then you need to update to v1.14.1-eksbuild.1 first, and then update to v1.15.0-eksbuild.2. If you're updating the self-managed type of this add-on, we recommend updating to the same major.minor.patch version listed in the [latest available versions table \(p. 267\)](#), even if later versions are available on GitHub..
- **Check version compatibility for each feature**

All versions of this add-on work with all Amazon EKS supported Kubernetes versions, though not all features of each release work with all Kubernetes versions. When using different Amazon EKS features, if a specific version of the add-on is required, then it's noted in the feature documentation. Unless you have a specific reason for running an earlier version, we recommend running the latest version.

Creating the Amazon EKS add-on

Create the Amazon EKS type of the add-on.

1. See which version of the add-on is installed on your cluster.

```
kubectl describe daemonset aws-node --namespace kube-system | grep amazon-k8s-cni: |
cut -d : -f 3
```

An example output is as follows.

v1.12.6-eksbuild.2

2. See which type of the add-on is installed on your cluster. Depending on the tool that you created your cluster with, you might not currently have the Amazon EKS add-on type installed on your cluster. Replace *my-cluster* with the name of your cluster.

```
$ aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni --query addon.addonVersion --output text
```

If a version number is returned, you have the Amazon EKS type of the add-on installed on your cluster and don't need to complete the remaining steps in this procedure. If an error is returned, you don't have the Amazon EKS type of the add-on installed on your cluster. Complete the remaining steps of this procedure to install it.

3. Save the configuration of your currently installed add-on.

```
kubectl get daemonset aws-node -n kube-system -o yaml > aws-k8s-cni-old.yaml
```

4. Create the add-on using the AWS CLI. If you want to use the AWS Management Console or eksctl to create the add-on, see [the section called "Creating an add-on" \(p. 393\)](#) and specify vpc-cni for the add-on name. Copy the command that follows to your device. Make the following modifications to the command, as needed, and then run the modified command.
 - Replace *my-cluster* with the name of your cluster.
 - Replace *v1.15.0-eksbuild.2* with the latest version listed in the [latest version table \(p. 267\)](#) for your cluster version.
 - Replace *111122223333* with your account ID and *AmazonEKSVPCCNIRole* with the name of an [existing IAM role \(p. 272\)](#) that you've created. Specifying a role requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one for your cluster, or to create one, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#).

```
aws eks create-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version v1.15.0-eksbuild.2 \
    --service-account-role-arn arn:aws:iam::111122223333:role/AmazonEKSVPCCNIRole
```

If you've applied custom settings to your current add-on that conflict with the default settings of the Amazon EKS add-on, creation might fail. If creation fails, you receive an error that can help you resolve the issue. Alternatively, you can add **--resolve-conflicts OVERWRITE** to the previous command. This allows the add-on to overwrite any existing custom settings. Once you've created the add-on, you can update it with your custom settings.

5. Confirm that the latest version of the add-on for your cluster's Kubernetes version was added to your cluster. Replace *my-cluster* with the name of your cluster.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni --query addon.addonVersion --output text
```

It might take several seconds for add-on creation to complete.

An example output is as follows.

v1.15.0-eksbuild.2

6. If you made custom settings to your original add-on, before you created the Amazon EKS add-on, use the configuration that you saved in a previous step to [update \(p. 269\)](#) the Amazon EKS add-on with your custom settings.
7. (Optional) Install the `cni-metrics-helper` to your cluster. It scrapes elastic network interface and IP address information, aggregates it at a cluster level, and publishes the metrics to Amazon CloudWatch. For more information, see [cni-metrics-helper](#) on GitHub.

Updating the Amazon EKS add-on

Update the Amazon EKS type of the add-on. If you haven't added the Amazon EKS type of the add-on to your cluster, either [add it \(p. 267\)](#) or see [the section called "Updating the self-managed add-on" \(p. 270\)](#), instead of completing this procedure.

1. See which version of the add-on is installed on your cluster. Replace `my-cluster` with your cluster name.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni --query "addon.addonVersion" --output text
```

An example output is as follows.

```
v1.12.6-eksbuild.2
```

If the version returned is the same as the version for your cluster's Kubernetes version in the [latest version table \(p. 267\)](#), then you already have the latest version installed on your cluster and don't need to complete the rest of this procedure. If you receive an error, instead of a version number in your output, then you don't have the Amazon EKS type of the add-on installed on your cluster. You need to [create the add-on \(p. 267\)](#) before you can update it with this procedure.

2. Save the configuration of your currently installed add-on.

```
kubectl get daemonset aws-node -n kube-system -o yaml > aws-k8s-cni-old.yaml
```

3. Update your add-on using the AWS CLI. If you want to use the AWS Management Console or eksctl to update the add-on, see [the section called "Updating an add-on" \(p. 400\)](#). Copy the command that follows to your device. Make the following modifications to the command, as needed, and then run the modified command.

- Replace `my-cluster` with the name of your cluster.
- Replace `v1.15.0-eksbuild.2` with the latest version listed in the [latest version table \(p. 267\)](#) for your cluster version.
- Replace `111122223333` with your account ID and `AmazonEKSVPCNIRole` with the name of an [existing IAM role \(p. 272\)](#) that you've created. Specifying a role requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one for your cluster, or to create one, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#).
- The `--resolve-conflicts PRESERVE` option preserves existing configuration values for the add-on. If you've set custom values for add-on settings, and you don't use this option, Amazon EKS overwrites your values with its default values. If you use this option, then we recommend testing any field and value changes on a non-production cluster before updating the add-on on your production cluster. If you change this value to OVERWRITE, all settings are changed to Amazon EKS default values. If you've set custom values for any settings, they might be overwritten with Amazon EKS default values. If you change this value to none, Amazon EKS doesn't change the value of any settings, but the update might fail. If the update fails, you receive an error message to help you resolve the conflict.

- If you're not updating a configuration setting, remove `--configuration-values '{"env": {"AWS_VPC_K8S_CNI_EXTERNALSNAT": "true"}}'` from the command. If you're updating a configuration setting, replace `"env": {"AWS_VPC_K8S_CNI_EXTERNALSNAT": "true"}` with the setting that you want to set. In this example, the AWS_VPC_K8S_CNI_EXTERNALSNAT environment variable is set to true. The value that you specify must be valid for the configuration schema. If you don't know the configuration schema, run `aws eks describe-addon-configuration --addon-name vpc-cni --addon-version v1.15.0-eksbuild.2`, replacing `v1.15.0-eksbuild.2` with the version number of the add-on that you want to see the configuration for. The schema is returned in the output. If you have any existing custom configuration, want to remove it all, and set the values for all settings back to Amazon EKS defaults, remove `"env": {"AWS_VPC_K8S_CNI_EXTERNALSNAT": "true"}` from the command, so that you have empty `{}`. For an explanation of each setting, see [CNI Configuration Variables](#) on GitHub.

```
aws eks update-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version v1.15.0-eksbuild.2 \
    --service-account-role-arn arn:aws:iam::111122223333:role/AmazonEKSVPCCNIRole \
    --resolve-conflicts PRESERVE --configuration-values '{"env": {"AWS_VPC_K8S_CNI_EXTERNALSNAT": "true"}}'
```

It might take several seconds for the update to complete.

4. Confirm that the add-on version was updated. Replace `my-cluster` with the name of your cluster.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni
```

It might take several seconds for the update to complete.

An example output is as follows.

```
{
  "addon": {
    "addonName": "vpc-cni",
    "clusterName": "my-cluster",
    "status": "ACTIVE",
    "addonVersion": "v1.15.0-eksbuild.2",
    "health": {
      "issues": []
    },
    "addonArn": "arn:aws:eks:region:111122223333:addon/my-cluster/vpc-cni/74c33d2f-b4dc-8718-56e7-9fdfa65d14a9",
    "createdAt": "2023-04-12T18:25:19.319000+00:00",
    "modifiedAt": "2023-04-12T18:40:28.683000+00:00",
    "serviceAccountRoleArn": "arn:aws:iam::111122223333:role/AmazonEKSVPCCNIRole",
    "tags": {},
    "configurationValues": "{\"env\":{\"AWS_VPC_K8S_CNI_EXTERNALSNAT\":\"true\"}}"
  }
}
```

Updating the self-managed add-on

Important

We recommend adding the Amazon EKS type of the add-on to your cluster instead of using the self-managed type of the add-on. If you're not familiar with the difference between the types, see [the section called “Amazon EKS add-ons” \(p. 385\)](#). For more information about adding an Amazon EKS add-on to your cluster, see [the section called “Creating an add-on” \(p. 393\)](#). If you're unable to use the Amazon EKS add-on, we encourage you to submit an issue about why you can't to the [Containers roadmap GitHub repository](#).

1. Confirm that you don't have the Amazon EKS type of the add-on installed on your cluster. Replace *my-cluster* with the name of your cluster.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni --query  
addon.addonVersion --output text
```

If an error message is returned, you don't have the Amazon EKS type of the add-on installed on your cluster. To self-manage the add-on, complete the remaining steps in this procedure to update the add-on. If a version number is returned, you have the Amazon EKS type of the add-on installed on your cluster. To update it, use the procedure in [the section called "Updating an add-on" \(p. 400\)](#), rather than using this procedure. If you're not familiar with the differences between the add-on types, see [the section called "Amazon EKS add-ons" \(p. 385\)](#).

2. See which version of the container image is currently installed on your cluster.

```
kubectl describe daemonset aws-node --namespace kube-system | grep amazon-k8s-cni: |  
cut -d : -f 3
```

An example output is as follows.

```
v1.12.6-eksbuild.2
```

Your output might not include the build number.

3. Backup your current settings so you can configure the same settings once you've updated your version.

```
kubectl get daemonset aws-node -n kube-system -o yaml > aws-k8s-cni-old.yaml
```

4. To review the available versions and familiarize yourself with the changes in the version that you want to update to, see [releases](#) on GitHub. Note that we recommend updating to the same major.minor.patch version listed in the [latest available versions table \(p. 267\)](#), even if later versions are available on GitHub.. The build versions listed in the table aren't specified in the self-managed versions listed on GitHub. Update your version by completing the tasks in one of the following options:

- If you don't have any custom settings for the add-on, then run the command under the `To apply this release:` heading on GitHub for the [release](#) that you're updating to.
- If you have custom settings, download the manifest file with the following command. Change <https://raw.githubusercontent.com/aws/amazon-vpc-cni-k8s/v1.15.0/config/master/aws-k8s-cni.yaml> to the URL for the release on GitHub that you're updating to.

```
curl -o https://raw.githubusercontent.com/aws/amazon-vpc-cni-k8s/v1.15.0/config/master/aws-k8s-cni.yaml
```

If necessary, modify the manifest with the custom settings from the backup you made in a previous step and then apply the modified manifest to your cluster. If your nodes don't have access to the private Amazon EKS Amazon ECR repositories that the images are pulled from (see the lines that start with `image:` in the manifest), then you'll have to download the images, copy them to your own repository, and modify the manifest to pull the images from your repository. For more information, see [the section called "Copy an image to a repository" \(p. 381\)](#).

```
kubectl apply -f aws-k8s-cni.yaml
```

5. Confirm that the new version is now installed on your cluster.

```
kubectl describe daemonset aws-node --namespace kube-system | grep amazon-k8s-cni: |  
cut -d : -f 3
```

An example output is as follows.

```
v1.15.0
```

6. (Optional) Install the `cni-metrics-helper` to your cluster. It scrapes elastic network interface and IP address information, aggregates it at a cluster level, and publishes the metrics to Amazon CloudWatch. For more information, see [cni-metrics-helper](#) on GitHub.

Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts

The [Amazon VPC CNI plugin for Kubernetes](#) is the networking plugin for Pod networking in Amazon EKS clusters. The plugin is responsible for allocating VPC IP addresses to Kubernetes nodes and configuring the necessary networking for Pods on each node. The plugin:

- Requires AWS Identity and Access Management (IAM) permissions. If your cluster uses the IPv4 family, the permissions are specified in the [AmazonEKS_CNI_Policy](#) AWS managed policy. If your cluster uses the IPv6 family, then the permissions must be added to an [IAM policy that you create \(p. 276\)](#). You can attach the policy to the [Amazon EKS node IAM role \(p. 501\)](#), or to a separate IAM role. We recommend that you assign it to a separate role, as detailed in this topic.
- Creates and is configured to use a Kubernetes service account named `aws-node` when it's deployed. The service account is bound to a Kubernetes `clusterrole` named `aws-node`, which is assigned the required Kubernetes permissions.

Note

The Pods for the Amazon VPC CNI plugin for Kubernetes have access to the permissions assigned to the [Amazon EKS node IAM role \(p. 501\)](#), unless you block access to IMDS. For more information, see [Restrict access to the instance profile assigned to the worker node](#).

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Getting started with Amazon EKS \(p. 6\)](#).
- An existing AWS Identity and Access Management (IAM) OpenID Connect (OIDC) provider for your cluster. To determine whether you already have one, or to create one, see [Creating an IAM OIDC provider for your cluster \(p. 465\)](#).

Step 1: Create the Amazon VPC CNI plugin for Kubernetes IAM role

To create the IAM role

1. Determine the IP family of your cluster.

```
aws eks describe-cluster --name my-cluster | grep ipFamily
```

An example output is as follows.

```
"ipFamily": "ipv4"
```

The output may return ipv6 instead.

2. Create the IAM role. You can use eksctl or kubectl and the AWS CLI to create your IAM role.

eksctl

Create an IAM role and attach the IAM policy to the role with the command that matches the IP family of your cluster. The command creates and deploys an AWS CloudFormation stack that creates an IAM role, attaches the policy that you specify to it, and annotates the existing aws-node Kubernetes service account with the ARN of the IAM role that is created.

- IPv4

Replace *my-cluster* with your own value.

```
eksctl create iamserviceaccount \
--name aws-node \
--namespace kube-system \
--cluster my-cluster \
--role-name AmazonEKSVPCCNIRole \
--attach-policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy \
--override-existing-serviceaccounts \
--approve
```

- IPv6

Replace *my-cluster* with your own value. Replace *111122223333* with your account ID and replace *AmazonEKS_CNI_IPv6_Policy* with the name of your IPv6 policy. If you don't have an IPv6 policy, see [Create IAM policy for clusters that use the IPv6 family \(p. 276\)](#) to create one. To use IPv6 with your cluster, it must meet several requirements. For more information, see [Tutorial: Assigning IPv6 addresses to Pods and services \(p. 278\)](#).

```
eksctl create iamserviceaccount \
--name aws-node \
--namespace kube-system \
--cluster my-cluster \
--role-name AmazonEKSVPCCNIRole \
--attach-policy-arn
arn:aws:iam::111122223333:policy/AmazonEKS_CNI_IPv6_Policy \
--override-existing-serviceaccounts \
--approve
```

kubectl and the AWS CLI

1. View your cluster's OIDC provider URL.

```
aws eks describe-cluster --name my-cluster --query "cluster.identity.oidc.issuer"
--output text
```

An example output is as follows.

```
https://oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE
```

If no output is returned, then you must [create an IAM OIDC provider for your cluster \(p. 465\)](#).

2. Copy the following contents to a file named *vpc-cni-trust-policy.json*. Replace *111122223333* with your account ID and *EXAMPLED539D4633E53DE1B71EXAMPLE* with the

output returned in the previous step. Replace *region-code* with the AWS Region that your cluster is in.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::111122223333:oidc-provider/
oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringEquals": {
                    "oidc.eks.region-code.amazonaws.com/
id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com",
                    "oidc.eks.region-code.amazonaws.com/
id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:kube-system:aws-
node"
                }
            }
        }
    ]
}
```

3. Create the role. You can replace *AmazonEKSVPCCNIRole* with any name that you choose.

```
aws iam create-role \
--role-name AmazonEKSVPCCNIRole \
--assume-role-policy-document file:///"vpc-cni-trust-policy.json"
```

4. Attach the required IAM policy to the role. Run the command that matches the IP family of your cluster.

- IPv4

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy \
--role-name AmazonEKSVPCCNIRole
```

- IPv6

Replace *111122223333* with your account ID and *AmazonEKS_CNI_IPv6_Policy* with the name of your IPv6 policy. If you don't have an IPv6 policy, see [Create IAM policy for clusters that use the IPv6 family \(p. 276\)](#) to create one. To use IPv6 with your cluster, it must meet several requirements. For more information, see [Tutorial: Assigning IPv6 addresses to Pods and services \(p. 278\)](#).

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::111122223333:policy/AmazonEKS_CNI_IPv6_Policy \
--role-name AmazonEKSVPCCNIRole
```

5. Run the following command to annotate the aws-node service account with the ARN of the IAM role that you created previously. Replace the *example values* with your own values.

```
kubectl annotate serviceaccount \
-n kube-system aws-node \
eks.amazonaws.com/role-arn=arn:aws:iam::111122223333:role/AmazonEKSVPCCNIRole
```

3. (Optional) Configure the AWS Security Token Service endpoint type used by your Kubernetes service account. For more information, see [Configuring the AWS Security Token Service endpoint for a service account \(p. 474\)](#).

Step 2: Re-deploy Amazon VPC CNI plugin for KubernetesPods

1. Delete and re-create any existing Pods that are associated with the service account to apply the credential environment variables. The annotation is not applied to Pods that are currently running without the annotation. The following command deletes the existing aws-node DaemonSet Pods and deploys them with the service account annotation.

```
kubectl delete Pods -n kube-system -l k8s-app=aws-node
```

2. Confirm that the Pods all restarted.

```
kubectl get pods -n kube-system -l k8s-app=aws-node
```

3. Describe one of the Pods and verify that the AWS_WEB_IDENTITY_TOKEN_FILE and AWS_ROLE_ARN environment variables exist. Replace *cpjw7* with the name of one of your Pods returned in the output of the previous step.

```
kubectl describe pod -n kube-system aws-node-cpjw7 | grep 'AWS_ROLE_ARN:\|AWS_WEB_IDENTITY_TOKEN_FILE:'
```

An example output is as follows.

```
AWS_ROLE_ARN:           arn:aws:iam::111122223333:role/AmazonEKSVPCCNIRole
AWS_WEB_IDENTITY_TOKEN_FILE: /var/run/secrets/eks.amazonaws.com/serviceaccount/
token
AWS_ROLE_ARN:
arn:aws:iam::111122223333:role/AmazonEKSVPCCNIRole
AWS_WEB_IDENTITY_TOKEN_FILE:           /var/run/secrets/eks.amazonaws.com/
serviceaccount/token
```

Two sets of duplicate results are returned because the Pod contains two containers. Both containers have the same values.

If your Pod is using the AWS Regional endpoint, then the following line is also returned in the previous output.

```
AWS_STS_REGIONAL_ENDPOINTS=regional
```

Step 3: Remove the CNI policy from the node IAM role

If your [Amazon EKS node IAM role \(p. 501\)](#) currently has the AmazonEKS_CNI_Policy IAM (IPv4) policy or an [IPv6 policy \(p. 276\)](#) attached to it, and you've created a separate IAM role, attached the policy to it instead, and assigned it to the aws-node Kubernetes service account, then we recommend that you remove the policy from your node role with the AWS CLI command that matches the IP family of your cluster. Replace *AmazonEKSNodeRole* with the name of your node role.

- IPv4

```
aws iam detach-role-policy --role-name AmazonEKSNodeRole --policy-arn
arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
```

- IPv6

Replace **111122223333** with your account ID and **AmazonEKS_CNI_IPv6_Policy** with the name of your IPv6 policy.

```
aws iam detach-role-policy --role-name AmazonEKSNodeRole --policy-arn
arn:aws:iam::111122223333:policy/AmazonEKS_CNI_IPv6_Policy
```

Create IAM policy for clusters that use the IPv6 family

If you created a cluster that uses the IPv6 family and the cluster has version 1.10.1 or later of the Amazon VPC CNI plugin for Kubernetes add-on configured, then you need to create an IAM policy that you can assign to an IAM role. If you have an existing cluster that you didn't configure with the IPv6 family when you created it, then to use IPv6, you must create a new cluster. For more information about using IPv6 with your cluster, see [the section called "IPv6" \(p. 278\)](#).

1. Copy the following text and save it to a file named **vpc-cni-ipv6-policy.json**.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeInstances",
                "ec2:DescribeTags",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstanceTypes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ]
        }
    ]
}
```

2. Create the IAM policy.

```
aws iam create-policy --policy-name AmazonEKS_CNI_IPv6_Policy --policy-document file://
vpc-cni-ipv6-policy.json
```

Choosing Pod networking use cases

The Amazon VPC CNI plugin for Kubernetes provides networking for Pods. The following table helps you understand which networking use cases you can use together and the capabilities and Amazon VPC CNI plugin for Kubernetes settings that you can use with different Amazon EKS node types. All information in the table applies to Linux IPv4 nodes only.

<u>Amazon EKS node type (p. 77)</u>	<u>Amazon EC2</u>			<u>Fargate</u>
<u>Custom networking for pods (p. 306)</u> – Assign IP addresses from a different subnet than the node's subnet	Yes	Yes	Yes	Yes (subnets controlled through Fargate profile)
<u>SNAT for Pods (p. 289)</u>	Yes (default is false)	Yes (default is false)	Yes (true only)	Yes (true only)
Capabilities				
<u>Security group scope</u>	Node	Node POD_SECURITY_GROUP_ENFORCING_MODE=standard and AWS_VPC_K8S_CNI_EXTERNALSNAT=false, traffic destined for endpoints outside the VPC use the node's security groups, not the Pod's security groups)	Pod (If you've set POD_SECURITY_GROUP_ENFORCING_MODE=standard and AWS_VPC_K8S_CNI_EXTERNALSNAT=false, traffic destined for endpoints outside the VPC use the node's security groups, not the Pod's security groups)	Pod
<u>Amazon VPC subnet types</u>	Private and public	Private and public	Private only	Private only
<u>Network policy (VPC CNI)</u>	Compatible	Compatible	Compatible Only with version 1.14.0 or later of the Amazon VPC CNI plugin	Not supported
Pod density per node	Medium	High	Low	One
Pod launch time	Better	Best	Good	Moderate
Amazon VPC CNI plugin settings (for more information about each setting, see amazon-vpc-cni-k8s on GitHub)				
WARM_ENI_TARGET	Yes	Not applicable	Not applicable	Not applicable
WARM_IP_TARGET	Yes	Yes	Not applicable	Not applicable
MINIMUM_IP_TARGET	Yes	Yes	Not applicable	Not applicable
WARM_PREFIX_TARGET	Not applicable	Yes	Not applicable	Not applicable

Note

- You can't use IPv6 with custom networking.
- IPv6 addresses are not translated, so SNAT doesn't apply.
- You can use Calico network policy with IPv6.
- Traffic flow to and from Pods with associated security groups are not subjected to Calico network policy enforcement and are limited to Amazon VPC security group enforcement only.
- IP prefixes and IP addresses are associated with standard Amazon EC2 elastic network interfaces. Pods requiring specific security groups are assigned the primary IP address of a branch network interface. You can mix Pods getting IP addresses, or IP addresses from IP prefixes with Pods getting branch network interfaces on the same node.

Windows nodes

Each node only supports one network interface. You can use secondary IPv4 addresses and IPv4 prefixes. By default, the number of available IPv4 addresses on the node is equal to the number of secondary IPv4 addresses that you can assign to each elastic network interface, minus one. However, you can increase the available IPv4 addresses and Pod density on the node by enabling IP prefixes. For more information, see [the section called "Increase available IP addresses" \(p. 318\)](#).

Calico network policies are supported on Windows. For more information, see [Open Source Calico for Windows Containers on Amazon EKS](#). You can't use [security groups for Pods \(p. 324\)](#) or [custom networking \(p. 306\)](#) on Windows.

Tutorial: Assigning IPv6 addresses to Pods and services

By default, Kubernetes assigns IPv4 addresses to your Pods and services. Instead of assigning IPv4 addresses to your Pods and services, you can configure your cluster to assign IPv6 addresses to them. Amazon EKS doesn't support dual-stacked Pods or services, even though Kubernetes does in version 1.23 and later. As a result, you can't assign both IPv4 and IPv6 addresses to your Pods and services.

You select which IP family you want to use for your cluster when you create it. You can't change the family after you create the cluster.

Considerations for using the IPv6 family for your cluster:

- You must create a new cluster and specify that you want to use the IPv6 family for that cluster. You can't enable the IPv6 family for a cluster that you updated from a previous version. For instructions on how to create a new cluster, see [Creating an Amazon EKS cluster \(p. 25\)](#).
- The version of the Amazon VPC CNI add-on that you deploy to your cluster must be version 1.10.1 or later. This version or later is deployed by default. After you deploy the add-on, you can't downgrade your Amazon VPC CNI add-on to a version lower than 1.10.1 without first removing all nodes in all node groups in your cluster.
- Windows Pods and services aren't supported.
- If you use Amazon EC2 nodes, you must configure the Amazon VPC CNI add-on with IP prefix delegation and IPv6. If you choose the IPv6 family when creating your cluster, the 1.10.1 version of the add-on defaults to this configuration. This is the case for both a self-managed or Amazon EKS add-on. For more information about IP prefix delegation, see [Increase the amount of available IP addresses for your Amazon EC2 nodes \(p. 318\)](#).
- When you create a cluster, the VPC and subnets that you specify must have an IPv6 CIDR block that's assigned to the VPC and subnets that you specify. They must also have an IPv4 CIDR block assigned to them. This is because, even if you only want to use IPv6, a VPC still requires an IPv4 CIDR block to function. For more information, see [Associate an IPv6 CIDR block with your VPC](#) in the Amazon VPC User Guide.

- When you create your cluster and nodes, you must specify subnets that are configured to auto-assign IPv6 addresses. Otherwise, you can't deploy your cluster and nodes. By default, this configuration is disabled. For more information, see [Modify the IPv6 addressing attribute for your subnet](#) in the Amazon VPC User Guide.
- The route tables that are assigned to your subnets must have routes for IPv6 addresses. For more information, see [Migrate to IPv6](#) in the Amazon VPC User Guide.
- Your security groups must allow IPv6 addresses. For more information, see [Migrate to IPv6](#) in the Amazon VPC User Guide.
- You can only use IPv6 with AWS Nitro-based Amazon EC2 or Fargate nodes.
- You can't use IPv6 with [Tutorial: Security groups for Pods \(p. 324\)](#) with Amazon EC2 nodes. However, you can use it with Fargate nodes. If you need separate security groups for individual Pods, continue using the IPv4 family with Amazon EC2 nodes, or use Fargate nodes instead.
- If you previously used [custom networking \(p. 306\)](#) to help alleviate IP address exhaustion, you can use IPv6 instead. You can't use custom networking with IPv6. If you use custom networking for network isolation, then you might need to continue to use custom networking and the IPv4 family for your clusters.
- You can't use IPv6 with [AWS Outposts \(p. 588\)](#).
- Pods and services are only assigned an IPv6 address. They aren't assigned an IPv4 address. Because Pods are able to communicate to IPv4 endpoints through NAT on the instance itself, [DNS64 and NAT64](#) aren't needed. If the traffic needs a public IP address, the traffic is then source network address translated to a public IP.
- The source IPv6 address of a Pod isn't source network address translated to the IPv6 address of the node when communicating outside of the VPC. It is routed using an internet gateway or egress-only internet gateway.
- All nodes are assigned an IPv4 and IPv6 address.
- The [Amazon FSx for Lustre CSI driver \(p. 249\)](#) is not supported.
- You can use version 2.3.1 or later of the AWS Load Balancer Controller to load balance [application \(p. 375\)](#) or [network \(p. 369\)](#) traffic to IPv6 Pods in IP mode, but not instance mode. For more information, see [Installing the AWS Load Balancer Controller add-on \(p. 333\)](#).
- You must attach an IPv6 IAM policy to your node IAM or CNI IAM role. Between the two, we recommend that you attach it to a CNI IAM role. For more information, see [Create IAM policy for clusters that use the IPv6 family \(p. 276\)](#) and [Step 1: Create the Amazon VPC CNI plugin for Kubernetes IAM role \(p. 272\)](#).
- Each Fargate Pod receives an IPv6 address from the CIDR that's specified for the subnet that it's deployed in. The underlying hardware unit that runs Fargate Pods gets a unique IPv4 and IPv6 address from the CIDRs that are assigned to the subnet that the hardware unit is deployed in.
- We recommend that you perform a thorough evaluation of your applications, Amazon EKS add-ons, and AWS services that you integrate with before deploying IPv6 clusters. This is to ensure that everything works as expected with IPv6.
- Use of the Amazon EC2 [Instance Metadata Service](#) IPv6 endpoint is not supported with Amazon EKS.
- When creating a self-managed node group in a cluster that uses the IPv6 family, user-data must include the following BootstrapArguments for the [bootstrap.sh](#) file that runs at node start up. Replace `your-cidr` with the IPv6 CIDR range of your cluster's VPC.

```
--ip-family ipv6 --service-ipv6-cidr your-cidr
```

If you don't know the IPv6 CIDR range for your cluster, you can see it with the following command (requires the AWS CLI version 2.4.9 or later).

```
aws eks describe-cluster --name my-cluster --query
cluster.kubernetesNetworkConfig.serviceIpv6Cidr --output text
```

Deploy an IPv6 cluster and managed Amazon Linux nodes

In this tutorial, you deploy an IPv6 Amazon VPC, an Amazon EKS cluster with the IPv6 family, and a managed node group with Amazon EC2 Amazon Linux nodes. You can't deploy Amazon EC2 Windows nodes in an IPv6 cluster. You can also deploy Fargate nodes to your cluster, though those instructions aren't provided in this topic for simplicity.

Before creating a cluster for production use, we recommend that you familiarize yourself with all settings and deploy a cluster with the settings that meet your requirements. For more information, see [Creating an Amazon EKS cluster \(p. 25\)](#), [Managed node groups \(p. 81\)](#) and the [considerations \(p. 278\)](#) for this topic. You can only enable some settings when creating your cluster.

Prerequisites

Before starting this tutorial, you must install and configure the following tools and resources that you need to create and manage an Amazon EKS cluster.

- The `kubectl` command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use `kubectl` version 1.26, 1.27, or 1.28 with it. To install or upgrade `kubectl`, see [Installing or updating kubectl \(p. 6\)](#).
- The IAM security principal that you're using must have permissions to work with Amazon EKS IAM roles, service linked roles, AWS CloudFormation, a VPC, and related resources. For more information, see [Actions, resources, and condition keys for Amazon Elastic Kubernetes Service](#) and [Using service-linked roles](#) in the IAM User Guide.

Procedures are provided to create the resources with either `eksctl` or the AWS CLI. You can also deploy the resources using the AWS Management Console, but those instructions aren't provided in this topic for simplicity.

`eksctl`

Prerequisite

`eksctl` version 0.160.0 or later installed on your computer. To install or update to it, see [the section called "Installing eksctl" \(p. 13\)](#).

To deploy an IPv6 cluster with `eksctl`

1. Create the `ipv6-cluster.yaml` file. Copy the command that follows to your device. Make the following modifications to the command as needed and then run the modified command:
 - Replace `my-cluster` with a name for your cluster. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters.
 - Replace `region-code` with any AWS Region that is supported by Amazon EKS. For a list of AWS Regions, see [Amazon EKS endpoints and quotas](#) in the AWS General Reference guide.
 - The value for `version` with the version of your cluster. For more information, see [supported Amazon EKS Kubernetes version \(p. 60\)](#).
 - Replace `my-nodegroup` with a name for your node group. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters.
 - Replace `t3.medium` with any [AWS Nitro System instance type](#).

```
cat >ipv6-cluster.yaml <<EOF
---
```

```

apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-cluster
  region: region-code
  version: "X.XX"

kubernetesNetworkConfig:
  ipFamily: IPv6

addons:
  - name: vpc-cni
    version: latest
  - name: coredns
    version: latest
  - name: kube-proxy
    version: latest

iam:
  withOIDC: true

managedNodeGroups:
  - name: my-nodegroup
    instanceType: t3.medium
EOF

```

2. Create your cluster.

```
eksctl create cluster -f ipv6-cluster.yaml
```

Cluster creation takes several minutes. Don't proceed until you see the last line of output, which looks similar to the following output.

```
[...]
[#] EKS cluster "my-cluster" in "region-code" region is ready
```

3. Confirm that default Pods are assigned IPv6 addresses.

```
kubectl get pods -n kube-system -o wide
```

An example output is as follows.

NAME	NODE	READY	STATUS	RESTARTS	AGE	IP	NOMINATED
	NODE	READY	STATUS	RESTARTS	AGE	IP	NOMINATED
aws-node- <i>rs1ts</i>		1/1	Running	1	5m36s		
	2600:1f13:b66:8200:11a5:ade0:c590:6ac8		ip-192-168-34-75.region-				
aws-node- <i>t74jh</i>		1/1	Running	0	5m32s		
	2600:1f13:b66:8203:4516:2080:8ced:1ca9		ip-192-168-253-70.region-				
coredns- <i>85d5b4454c-cw7w2</i>		1/1	Running	0	56m		
	2600:1f13:b66:8203:34e5::		ip-192-168-253-70.region-				
coredns- <i>85d5b4454c-tx6n8</i>		1/1	Running	0	56m		
	2600:1f13:b66:8203:34e5::1		ip-192-168-253-70.region-				
kube-proxy- <i>btpbk</i>		1/1	Running	0	5m36s		
	2600:1f13:b66:8200:11a5:ade0:c590:6ac8		ip-192-168-34-75.region-				
coredns- <i>compute.internal</i>		<none>	<none>				

```
kube-proxy-jjk2g      1/1     Running   0          5m33s
  2600:1f13:b66:8203:4516:2080:8ced:1ca9 ip-192-168-253-70.region-
code.compute.internal <none>           <none>
```

4. Confirm that default services are assigned IPv6 addresses.

```
kubectl get services -n kube-system -o wide
```

An example output is as follows.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
SELECTOR					
kube-dns	ClusterIP	fd30:3087:b6c2::a	<none>	53/UDP, 53/TCP	57m k8s-
app=kube-dns					

5. (Optional) [Deploy a sample application \(p. 356\)](#) or deploy the [AWS Load Balancer Controller \(p. 333\)](#) and a sample application to load balance [application \(p. 375\)](#) or [network \(p. 369\)](#) traffic to IPv6 Pods.
6. After you've finished with the cluster and nodes that you created for this tutorial, you should clean up the resources that you created with the following command.

```
eksctl delete cluster my-cluster
```

AWS CLI

Prerequisite

Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide. If you use the AWS CloudShell, you may need to [install version 2.12.3 or later or 1.27.160 or later of the AWS CLI](#), because the default AWS CLI version installed in the AWS CloudShell may be an earlier version.

Important

- You must complete all steps in this procedure as the same user. To check the current user, run the following command:

```
aws sts get-caller-identity
```

- You must complete all steps in this procedure in the same shell. Several steps use variables set in previous steps. Steps that use variables won't function properly if the variable values are set in a different shell. If you use the [AWS CloudShell](#) to complete the following procedure, remember that if you don't interact with it using your keyboard or pointer for approximately 20–30 minutes, your shell session ends. Running processes do not count as interactions.
- The instructions are written for the Bash shell, and may need adjusting in other shells.

To create your cluster with the AWS CLI

Replace all *example values* in the steps of this procedure with your own values.

- Run the following commands to set some variables used in later steps. Replace `region-code` with the AWS Region that you want to deploy your resources in. The value can be any AWS Region that is supported by Amazon EKS. For a list of AWS Regions, see [Amazon EKS endpoints and quotas](#) in the AWS General Reference guide. Replace `my-cluster` with a name for your cluster. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters. Replace `my-nodegroup` with a name for your node group. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters. Replace `111122223333` with your account ID.

```
export region_code=region-code
export cluster_name=my-cluster
export nodegroup_name=my-nodegroup
export account_id=111122223333
```

- Create an Amazon VPC with public and private subnets that meets Amazon EKS and IPv6 requirements.
 - Run the following command to set a variable for your AWS CloudFormation stack name. You can replace `my-eks-ipv6-vpc` with any name you choose.

```
export vpc_stack_name=my-eks-ipv6-vpc
```

- Create an IPv6 VPC using an AWS CloudFormation template.

```
aws cloudformation create-stack --region $region_code --stack-name
$vpc_stack_name \
--template-url https://s3.us-west-2.amazonaws.com/amazon-
eks/cloudformation/2020-10-29/amazon-eks-ipv6-vpc-public-private-subnets.yaml
```

The stack takes a few minutes to create. Run the following command. Don't continue to the next step until the output of the command is CREATE_COMPLETE.

```
aws cloudformation describe-stacks --region $region_code --stack-name
$vpc_stack_name --query Stacks[].StackStatus --output text
```

- Retrieve the IDs of the public subnets that were created.

```
aws cloudformation describe-stacks --region $region_code --stack-name
$vpc_stack_name \
--query='Stacks[].Outputs[?OutputKey==`SubnetsPublic`].OutputValue' --
output text
```

An example output is as follows.

```
subnet-0a1a56c486EXAMPLE,subnet-099e6ca77aEXAMPLE
```

- Enable the auto-assign IPv6 address option for the public subnets that were created.

```
aws ec2 modify-subnet-attribute --region $region_code --
subnet-id subnet-0a1a56c486EXAMPLE --assign-ipv6-address-on-
creation
aws ec2 modify-subnet-attribute --region $region_code --subnet-id
subnet-099e6ca77aEXAMPLE --assign-ipv6-address-on-creation
```

- Retrieve the names of the subnets and security groups created by the template from the deployed AWS CloudFormation stack and store them in variables for use in a later step.

```

security_groups=$(aws cloudformation describe-stacks --region $region_code --
stack-name $vpc_stack_name \
--query='Stacks[].Outputs[?OutputKey==`SecurityGroups`].OutputValue' --
output text)

public_subnets=$(aws cloudformation describe-stacks --region $region_code --
stack-name $vpc_stack_name \
--query='Stacks[].Outputs[?OutputKey==`SubnetsPublic`].OutputValue' --
output text)

private_subnets=$(aws cloudformation describe-stacks --region $region_code --
stack-name $vpc_stack_name \
--query='Stacks[].Outputs[?OutputKey==`SubnetsPrivate`].OutputValue' --
output text)

subnets=${public_subnets},${private_subnets}

```

3. Create a cluster IAM role and attach the required Amazon EKS IAM managed policy to it. Kubernetes clusters managed by Amazon EKS make calls to other AWS services on your behalf to manage the resources that you use with the service.
 - a. Run the following command to create the `eks-cluster-role-trust-policy.json` file.

```

cat >eks-cluster-role-trust-policy.json <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "eks.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF

```

- b. Run the following command to set a variable for your role name. You can replace `myAmazonEKSClusterRole` with any name you choose.

```
export cluster_role_name=myAmazonEKSClusterRole
```

- c. Create the role.

```
aws iam create-role --role-name $cluster_role_name --assume-role-policy-
document file:///"eks-cluster-role-trust-policy.json"
```

- d. Retrieve the ARN of the IAM role and store it in a variable for a later step.

```
cluster_iam_role=$(aws iam get-role --role-name $cluster_role_name --
query="Role.Arn" --output text)
```

- e. Attach the required Amazon EKS managed IAM policy to the role.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/
AmazonEKSClusterPolicy --role-name $cluster_role_name
```

4. Create your cluster.

```
aws eks create-cluster --region $region_code --name $cluster_name --kubernetes-
version 1.XX \
--role-arn $cluster_iam_role --resources-vpc-config subnetIds=
$subnets,securityGroupIds=$security_groups \
--kubernetes-network-config ipFamily=ipv6
```

- **Note**

You might receive an error that one of the Availability Zones in your request doesn't have sufficient capacity to create an Amazon EKS cluster. If this happens, the error output contains the Availability Zones that can support a new cluster. Retry creating your cluster with at least two subnets that are located in the supported Availability Zones for your account. For more information, see [Insufficient capacity \(p. 562\)](#).

The cluster takes several minutes to create. Run the following command. Don't continue to the next step until the output from the command is ACTIVE.

```
aws eks describe-cluster --region $region_code --name $cluster_name --query
cluster.status
```

5. Create or update a kubeconfig file for your cluster so that you can communicate with your cluster.

```
aws eks update-kubeconfig --region $region_code --name $cluster_name
```

By default, the config file is created in `~/.kube` or the new cluster's configuration is added to an existing config file in `~/.kube`.

6. Create a node IAM role.

- a. Run the following command to create the `vpc-cni-ipv6-policy.json` file.

```
cat >vpc-cni-ipv6-policy <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeInstances",
                "ec2:DescribeTags",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstanceTypes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*.*:network-interface/*"
            ]
        }
    ]
}
EOF
```

- b. Create the IAM policy.

```
aws iam create-policy --policy-name AmazonEKS_CNT_IPv6_Policy --policy-document  
file://vpc-cni-ipv6-policy.json
```

- c. Run the following command to create the node-role-trust-relationship.json file.

```
cat >node-role-trust-relationship.json <<EOF  
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "ec2.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}  
EOF
```

- d. Run the following command to set a variable for your role name. You can replace *AmazonEKSNODERole* with any name you choose.

```
export node_role_name=AmazonEKSNODERole
```

- e. Create the IAM role.

```
aws iam create-role --role-name $node_role_name --assume-role-policy-document  
file://"node-role-trust-relationship.json"
```

- f. Attach the IAM policy to the IAM role.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::  
$account_id:policy/AmazonEKS_CNI_IPv6_Policy \  
--role-name $node_role_name
```

Important

For simplicity in this tutorial, the policy is attached to this IAM role. In a production cluster however, we recommend attaching the policy to a separate IAM role. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).

- g. Attach two required IAM managed policies to the IAM role.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/  
AmazonEKSWorkerNodePolicy \  
--role-name $node_role_name  
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/  
AmazonEC2ContainerRegistryReadOnly \  
--role-name $node_role_name
```

- h. Retrieve the ARN of the IAM role and store it in a variable for a later step.

```
node_iam_role=$(aws iam get-role --role-name $node_role_name --query="Role.Arn"  
--output text)
```

7. Create a managed node group.

- a. View the IDs of the subnets that you created in a previous step.

```
echo $subnets
```

An example output is as follows.

```
subnet-0a1a56c486EXAMPLE, subnet-099e6ca77aEXAMPLE, subnet-
0377963d69EXAMPLE, subnet-0c05f819d5EXAMPLE
```

- b. Create the node group. Replace `0a1a56c486EXAMPLE`, `099e6ca77aEXAMPLE`, `0377963d69EXAMPLE`, and `0c05f819d5EXAMPLE` with the values returned in the output of the previous step. Be sure to remove the commas between subnet IDs from the previous output in the following command. You can replace `t3.medium` with any [AWS Nitro System instance type](#).

```
aws eks create-nodegroup --region $region_code --cluster-name $cluster_name --
nodegroup-name $nodegroup_name \
--subnets subnet-0a1a56c486EXAMPLE subnet-099e6ca77aEXAMPLE
subnet-0377963d69EXAMPLE subnet-0c05f819d5EXAMPLE \
--instance-types t3.medium --node-role $node_iam_role
```

The node group takes a few minutes to create. Run the following command. Don't proceed to the next step until the output returned is ACTIVE.

```
aws eks describe-nodegroup --region $region_code --cluster-name $cluster_name
--nodegroup-name $nodegroup_name \
--query nodegroup.status --output text
```

8. Confirm that the default Pods are assigned IPv6 addresses in the IP column.

```
kubectl get pods -n kube-system -o wide
```

An example output is as follows.

NAME	READY	STATUS	RESTARTS	AGE	IP	NOMINATED
NODE	READINESS	GATES				
aws-node-rs1ts	1/1	Running	1	5m36s		
2600:1f13:b66:8200:11a5:ade0:c590:6ac8		ip-192-168-34-75.region-				
code.compute.internal	<none>	<none>				
aws-node-t74jh	1/1	Running	0	5m32s		
2600:1f13:b66:8203:4516:2080:8ced:1ca9		ip-192-168-253-70.region-				
code.compute.internal	<none>	<none>				
coredns-85d5b4454c-cw7w2	1/1	Running	0	56m		
2600:1f13:b66:8203:34e5::		ip-192-168-253-70.region-				
code.compute.internal	<none>	<none>				
coredns-85d5b4454c-tx6n8	1/1	Running	0	56m		
2600:1f13:b66:8203:34e5::1		ip-192-168-253-70.region-				
code.compute.internal	<none>	<none>				
kube-proxy-btpbk	1/1	Running	0	5m36s		
2600:1f13:b66:8200:11a5:ade0:c590:6ac8		ip-192-168-34-75.region-				
code.compute.internal	<none>	<none>				
kube-proxy-jjk2g	1/1	Running	0	5m33s		
2600:1f13:b66:8203:4516:2080:8ced:1ca9		ip-192-168-253-70.region-				
code.compute.internal	<none>	<none>				

9. Confirm that the default services are assigned IPv6 addresses in the IP column.

```
kubectl get services -n kube-system -o wide
```

An example output is as follows.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
SELECTOR kube-dns app=kube-dns	ClusterIP	<i>fd30:3087:b6c2::a</i>	<none>	53/UDP, 53/TCP	57m k8s-

10. (Optional) [Deploy a sample application \(p. 356\)](#) or deploy the [AWS Load Balancer Controller \(p. 333\)](#) and a sample application to load balance [application \(p. 375\)](#) or [network \(p. 369\)](#) traffic to IPv6 Pods.
11. After you've finished with the cluster and nodes that you created for this tutorial, you should clean up the resources that you created with the following commands. Make sure that you're not using any of the resources outside of this tutorial before deleting them.
 - a. If you're completing this step in a different shell than you completed the previous steps in, set the values of all the variables used in previous steps, replacing the *example values* with the values you specified when you completed the previous steps. If you're completing this step in the same shell that you completed the previous steps in, skip to the next step.

```
export region_code=region-code
export vpc_stack_name=my-eks-ipv6-vpc
export cluster_name=my-cluster
export nodegroup_name=my-nodegroup
export account_id=111122223333
export node_role_name=AmazonEKSNodeRole
export cluster_role_name=myAmazonEKSClusterRole
```

- b. Delete your node group.

```
aws eks delete-nodegroup --region $region_code --cluster-name $cluster_name --
nodegroup-name $nodegroup_name
```

Deletion takes a few minutes. Run the following command. Don't proceed to the next step if any output is returned.

```
aws eks list-nodegroups --region $region_code --cluster-name $cluster_name --
query nodegroups --output text
```

- c. Delete the cluster.

```
aws eks delete-cluster --region $region_code --name $cluster_name
```

The cluster takes a few minutes to delete. Before continuing make sure that the cluster is deleted with the following command.

```
aws eks describe-cluster --region $region_code --name $cluster_name
```

Don't proceed to the next step until your output is similar to the following output.

```
An error occurred (ResourceNotFoundException) when calling the DescribeCluster
operation: No cluster found for name: my-cluster.
```

- d. Delete the IAM resources that you created. Replace *AmazonEKS_CNI_IPv6_Policy* with the name you chose, if you chose a different name than the one used in previous steps.

```
aws iam detach-role-policy --role-name $cluster_role_name --policy-arn
    arn:aws:iam::aws:policy/AmazonEKSClusterPolicy
aws iam detach-role-policy --role-name $node_role_name --policy-arn
    arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
aws iam detach-role-policy --role-name $node_role_name --policy-arn
    arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
aws iam detach-role-policy --role-name $node_role_name --policy-arn
    arn:aws:iam::$account_id:policy/AmazonEKS_CNI_IPv6_Policy
aws iam delete-policy --policy-arn arn:aws:iam::$account_id:policy/AmazonEKS_CNI_IPv6_Policy
aws iam delete-role --role-name $cluster_role_name
aws iam delete-role --role-name $node_role_name
```

- e. Delete the AWS CloudFormation stack that created the VPC.

```
aws cloudformation delete-stack --region $region_code --stack-name
    $vpc_stack_name
```

SNAT for Pods

If you deployed your cluster using the IPv6 family, then the information in this topic isn't applicable to your cluster, because IPv6 addresses are not network translated. For more information about using IPv6 with your cluster, see [the section called "IPv6" \(p. 278\)](#).

By default, each Pod in your cluster is assigned a [private](#) IPv4 address from a classless inter-domain routing (CIDR) block that is associated with the VPC that the Pod is deployed in. Pods in the same VPC communicate with each other using these private IP addresses as end points. When a Pod communicates to any IPv4 address that isn't within a CIDR block that's associated to your VPC, the Amazon VPC CNI plugin (for both [Linux](#) or [Windows](#)) translates the Pod's IPv4 address to the primary private IPv4 address of the primary [elastic network interface](#) of the node that the Pod is running on, by default [* \(p. 290\)](#).

Note

For Windows nodes, there are additional details to consider. By default, the [VPC CNI plugin for Windows](#) is defined with a networking configuration in which the traffic to a destination within the same VPC is excluded for SNAT. This means that internal VPC communication has SNAT disabled and the IP address allocated to a Pod is routable inside the VPC. But traffic to a destination outside of the VPC has the source Pod IP SNAT'ed to the instance ENI's primary IP address. This default configuration for Windows ensures that the pod can access networks outside of your VPC in the same way as the host instance.

Due to this behavior:

- Your Pods can communicate with internet resources only if the node that they're running on has a [public](#) or [elastic](#) IP address assigned to it and is in a [public subnet](#). A public subnet's associated [route table](#) has a route to an internet gateway. We recommend deploying nodes to private subnets, whenever possible.
- For versions of the plugin earlier than 1.8.0, resources that are in networks or VPCs that are connected to your cluster VPC using [VPC peering](#), a [transit VPC](#), or [AWS Direct Connect](#) can't initiate communication to your Pods behind secondary elastic network interfaces. Your Pods can initiate communication to those resources and receive responses from them, though.

If either of the following statements are true in your environment, then change the default configuration with the command that follows.

- You have resources in networks or VPCs that are connected to your cluster VPC using [VPC peering](#), a [transit VPC](#), or [AWS Direct Connect](#) that need to initiate communication with your Pods using an IPv4 address and your plugin version is earlier than 1.8.0.
- Your Pods are in a [private subnet](#) and need to communicate outbound to the internet. The subnet has a route to a [NAT gateway](#).

```
kubectl set env daemonset -n kube-system aws-node AWS_VPC_K8S_CNI_EXTERNALSNAT=true
```

Note

The AWS_VPC_K8S_CNI_EXTERNALSNAT and AWS_VPC_K8S_CNI_EXCLUDE_SNAT_CIDRS CNI configuration variables aren't applicable to Windows nodes. Disabling SNAT isn't supported for Windows. As for excluding a list of IPv4 CIDRs from SNAT, you can define this by specifying the ExcludedSnatCIDRs parameter in the Windows bootstrap script. For more information on using this parameter, see [Bootstrap script configuration parameters \(p. 186\)](#).

* If a Pod's spec contains hostNetwork=true (default is false), then its IP address isn't translated to a different address. This is the case for the kube-proxy and Amazon VPC CNI plugin for Kubernetes Pods that run on your cluster, by default. For these Pods, the IP address is the same as the node's primary IP address, so the Pod's IP address isn't translated. For more information about a Pod's hostNetwork setting, see [PodSpec v1 core](#) in the Kubernetes API reference.

Configure your cluster for Kubernetes network policies

By default, there are no restrictions in Kubernetes for IP addresses, ports, or connections between any Pods in your cluster or between your Pods and resources in any other network. You can use Kubernetes *network policy* to restrict network traffic to and from your Pods. For more information, see [Network Policies](#) in the Kubernetes documentation.

If you have version 1.13 or earlier of the Amazon VPC CNI plugin for Kubernetes on your cluster, you need to implement a third party solution to apply Kubernetes network policies to your cluster. Version 1.14 or later of the plugin can implement network policies, so you don't need to use a third party solution. In this topic, you learn how to configure your cluster to use Kubernetes network policy on your cluster without using a third party add-on.

Network policies in the Amazon VPC CNI plugin for Kubernetes are supported in the following configurations.

- Amazon EKS clusters of version 1.25 and later.
- Version 1.14 or later of the Amazon VPC CNI plugin for Kubernetes on your cluster.
- Cluster configured for IPv4 or IPv6 addresses.
- You can use network policies with [security groups for Pods \(p. 324\)](#). With network policies, you can control all in-cluster communication. With security groups for Pods, you can control access to AWS services from applications within a Pod.
- You can use network policies with *custom networking and prefix delegation*.

Considerations

- When applying Amazon VPC CNI plugin for Kubernetes network policies to your cluster with the Amazon VPC CNI plugin for Kubernetes, you can apply the policies to Amazon EC2 Linux nodes only. You can't apply the policies to Fargate or Windows nodes.
- If your cluster is currently using a third party solution to manage Kubernetes network policies, you can use those same policies with the Amazon VPC CNI plugin for Kubernetes. However you must remove your existing solution so that it isn't managing the same policies.
- You can apply multiple network policies to the same Pod. When two or more policies that select the same Pod are configured, all policies are applied to the Pod.

- The maximum number of unique combinations of ports for each protocol in each `ingress:` or `egress:` selector in a network policy is 8.
- For any of your Kubernetes services, the service port must be the same as the container port. If you're using named ports, use the same name in the service spec too.
- The Amazon VPC CNI plugin for Kubernetes configures network policies for pods in parallel with the pod provisioning. Until all of the policies are configured for the new pod, containers in the new pod will start with a default allow policy. All ingress and egress traffic is allowed to and from the new pods unless they are resolved against the existing policies.
- The network policy feature creates and requires a `PolicyEndpoint` Custom Resource Definition (CRD) called `policyendpoints.networking.k8s.aws`. `PolicyEndpoint` objects of the Custom Resource are managed by Amazon EKS. You shouldn't modify or delete these resources.
- If you run pods that use the instance role IAM credentials or connect to the EC2 IMDS, be careful to check for network policies that would block access to the EC2 IMDS. You may need to add a network policy to allow access to EC2 IMDS. For more information, see [Instance metadata and user data](#) in the Amazon EC2 User Guide for Linux Instances.

Pods that use IAM roles for service accounts don't access EC2 IMDS.

- The network policy feature uses port 8162 on the node for metrics by default. Also, the feature used port 8163 for health probes. If you run another application on the nodes or inside pods that needs to use these ports, the app fails to run. In VPC CNI version v1.14.1 or later, you can change these ports port in the following places:

AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, select **Clusters**, and then select the name of the cluster that you want to configure the Amazon VPC CNI add-on for.
3. Choose the **Add-ons** tab.
4. Select the box in the top right of the add-on box and then choose **Edit**.
5. On the **Configure name of addon** page:
 - a. Select a v1.14.0-eksbuild.3 or later version in the **Version** dropdown list.
 - b. Expand the **Optional configuration settings**.
 - c. Enter the JSON key "enableNetworkPolicy": and value "true" in **Configuration values**. The resulting text must be a valid JSON object. If this key and value are the only data in the text box, surround the key and value with curly braces {}.

The following example has network policy feature enabled, the network policy logs sent to Amazon CloudWatch Logs, and the metrics and health probes are set to the default port numbers:

```
{
  "enableNetworkPolicy": "true",
  "nodeAgent": {
    "enableCloudWatchLogs": "true",
    "healthProbeBindAddr": "8163",
    "metricsBindAddr": "8162"
  }
}
```

Helm

If you have installed the Amazon VPC CNI plugin for Kubernetes through `helm`, you can update the configuration to change the ports.

- Run the following command to change the ports. Set the port number in the value for either key `nodeAgent.metricsBindAddr` or key `nodeAgent.healthProbeBindAddr`, respectively.

```
helm upgrade --set nodeAgent.metricsBindAddr=8162 --set
  nodeAgent.healthProbeBindAddr=8163 aws-vpc-cni --namespace kube-system eks/aws-
vpc-cni
```

kubectl

- Open the `aws-node` DaemonSet in your editor.

```
kubectl edit daemonset -n kube-system aws-node
```

- Replace the port numbers in the following command arguments in the `args:` in the `aws-network-policy-agent` container in the VPC CNI `aws-node` daemonset manifest.

```
- args:
  - --metrics-bind-addr=:8162
  - --health-probe-bind-addr=:8163
```

Prerequisites

- Minimum cluster version**

An existing Amazon EKS cluster. To deploy one, see [Getting started with Amazon EKS \(p. 6\)](#). The cluster must be Kubernetes version 1.25 or later. The cluster must be running one of the Kubernetes versions and platform versions listed in the following table. Note that any Kubernetes and platform versions later than those listed are also supported. You can check your current Kubernetes version by replacing `my-cluster` in the following command with the name of your cluster and then running the modified command:

```
aws eks describe-cluster
  --name my-cluster --query cluster.version --output
  text
```

Kubernetes version	Platform version
1.27.4	eks.5
1.26.7	eks.6
1.25.12	eks.7

- Minimum VPC CNI version**

Version 1.14 or later of the Amazon VPC CNI plugin for Kubernetes on your cluster. You can see which version that you currently have with the following command.

```
kubectl describe daemonset aws-node --namespace kube-system | grep amazon-k8s-cni: | cut
-d : -f 3
```

If your version is earlier than 1.14, see [the section called “Updating the Amazon EKS add-on” \(p. 269\)](#) to upgrade to version 1.14 or later.

- **Minimum Linux kernel version**

Your nodes must have Linux kernel version 5.10 or later. You can check your kernel version with `uname -r`. If you’re using the latest versions of the Amazon EKS optimized Amazon Linux and Bottlerocket AMIs, they already have the required kernel version.

The Amazon EKS optimized accelerated Amazon Linux AMIs have kernel 5.4, therefore these AMIs can’t be used with network policies.

To configure your cluster to use Kubernetes network policies

1. Mount the BPF filesystem

Note

If your cluster is version 1.27 or later, you can skip this step as all Amazon EKS optimized Amazon Linux and Bottlerocket AMIs for 1.27 or later have this feature already.

For all other cluster versions, if you upgrade the Amazon EKS optimized Amazon Linux to version v20230703 or later or you upgrade the Bottlerocket AMI to version v1.0.2 or later, you can skip this step.

- Mount the Berkeley Packet Filter (BPF) file system on each of your nodes.

```
sudo mount -t bpf bpffs /sys/fs/bpf
```

- Then, add the same command to your user data in your launch template for your Amazon EC2 Auto Scaling Groups.

2. Enable network policy in the VPC CNI

- See which type of the add-on is installed on your cluster. Depending on the tool that you created your cluster with, you might not currently have the Amazon EKS add-on type installed on your cluster. Replace `my-cluster` with the name of your cluster.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni --query addon.addonVersion --output text
```

If a version number is returned, you have the Amazon EKS type of the add-on installed on your cluster and don’t need to complete the remaining steps in this procedure. If an error is returned, you don’t have the Amazon EKS type of the add-on installed on your cluster.

- Amazon EKS add-on

AWS Management Console

- Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
- In the left navigation pane, select **Clusters**, and then select the name of the cluster that you want to configure the Amazon VPC CNI add-on for.
- Choose the **Add-ons** tab.
- Select the box in the top right of the add-on box and then choose **Edit**.
- On the **Configure name of addon** page:
 - Select a v1.14.0-eksbuild.3 or later version in the **Version** dropdown list.
 - Expand the **Optional configuration settings**.

- iii. Enter the JSON key "enableNetworkPolicy": and value "true" in **Configuration values**. The resulting text must be a valid JSON object. If this key and value are the only data in the text box, surround the key and value with curly braces {}. The following example shows both network policy and the network policy logs are enabled:

```
{
    "enableNetworkPolicy": "true",
    "nodeAgent": {
        "enableCloudWatchLogs": "true"
    }
}
```

The following screenshot shows an example of this scenario.

The screenshot shows the 'Configure Amazon VPC CNI' page in the EKS console. In the 'Optional configuration settings' section, there is a code editor containing the following JSON configuration:

```
{
    "enableNetworkPolicy": "true"
}
```

AWS CLI

- Run the following AWS CLI command. Replace `my-cluster` with the name of your cluster and the IAM role ARN with the role that you are using.

```
aws eks update-addon --cluster-name my-cluster --addon-name vpc-cni --
    --addon-version v1.14.0-eksbuild.3 \
    --service-account-role-arn arn:aws:iam::123456789012:role/AmazonEKSVPCCNIRole \
```

```
--resolve-conflicts PRESERVE --configuration-values  
'{"enableNetworkPolicy": "true"}'
```

- Self-managed add-on

Helm

If you have installed the Amazon VPC CNI plugin for Kubernetes through helm, you can update the configuration to enable network policy.

- Run the following command to enable network policy.

```
helm upgrade --set enableNetworkPolicy=true aws-vpc-cni --namespace  
kube-system eks/aws-vpc-cni
```

kubectl

- a. Open the amazon-vpc-cni ConfigMap in your editor.

```
kubectl edit configmap -n kube-system amazon-vpc-cni -o yaml
```

- b. Add the following line to the data in the ConfigMap.

```
enable-network-policy-controller: "true"
```

Once you've added the line, your ConfigMap should look like the following example.

```
apiVersion: v1  
kind: ConfigMap  
metadata:  
  name: amazon-vpc-cni  
  namespace: kube-system  
data:  
  enable-network-policy-controller: "true"
```

- c. Open the aws-node DaemonSet in your editor.

```
kubectl edit daemonset -n kube-system aws-node
```

- d. Replace the false with true in the command argument --enable-network-policy=false in the args: in the aws-network-policy-agent container in the VPC CNI aws-node daemonset manifest.

```
- args:  
  - --enable-network-policy=true
```

3. Confirm that the aws-node pods are running on your cluster.

```
kubectl get pods -n kube-system | grep 'aws-node\|amazon'
```

An example output is as follows.

aws-node- <i>gmqp7</i> 24h	2/2	Running	1 (24h ago)
-------------------------------	-----	---------	-------------

aws-node- <i>prnsh</i> 24h	2/2	Running	1 (24h ago)
-------------------------------	-----	---------	-------------

If network policy is enabled, there are 2 containers in the aws-node pods. In previous versions and if network policy is disabled, there is only a single container in the aws-node pods.

You can now deploy Kubernetes network policies to your cluster. For more information, see [the section called “Kubernetes network policies” \(p. 305\)](#).

Stars demo of network policy

This demo creates a front-end, back-end, and client service on your Amazon EKS cluster. The demo also creates a management graphical user interface that shows the available ingress and egress paths between each service. We recommend that you complete the demo on a cluster that you don't run production workloads on.

Before you create any network policies, all services can communicate bidirectionally. After you apply the network policies, you can see that the client can only communicate with the front-end service, and the back-end only accepts traffic from the front-end.

To run the Stars policy demo

1. Apply the front-end, back-end, client, and management user interface services:

```
kubectl apply -f https://eksworkshop.com/beginner/120_network-policies/calico/
stars_policy_demo/create_resources.files/namespace.yaml
kubectl apply -f https://eksworkshop.com/beginner/120_network-policies/calico/
stars_policy_demo/create_resources.files/management-ui.yaml
kubectl apply -f https://eksworkshop.com/beginner/120_network-policies/calico/
stars_policy_demo/create_resources.files/backend.yaml
kubectl apply -f https://eksworkshop.com/beginner/120_network-policies/calico/
stars_policy_demo/create_resources.files/frontend.yaml
kubectl apply -f https://eksworkshop.com/beginner/120_network-policies/calico/
stars_policy_demo/create_resources.files/client.yaml
```

2. View all Pods on the cluster.

```
kubectl get pods -A
```

An example output is as follows.

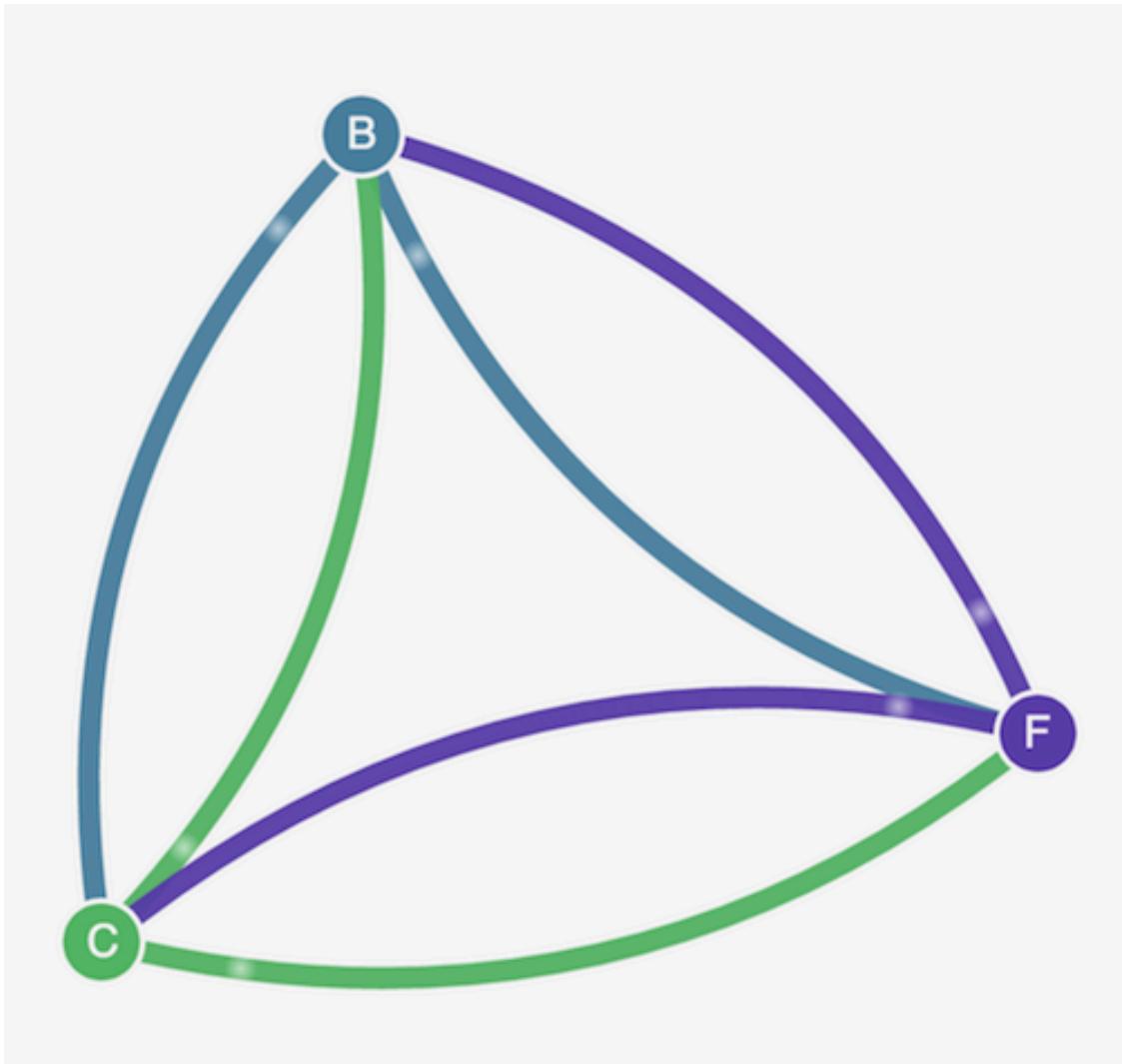
In your output, you should see pods in the namespaces shown in the following output. The **NAMES** of your pods and the number of pods in the READY column are different than those in the following output. Don't continue until you see pods with similar names and they all have Running in the STATUS column.

NAMESPACE AGE	NAME	READY	STATUS	RESTARTS
[...]				
client <i>5m19s</i>	client- <i>xlffc</i>	<i>1/1</i>	Running	0
[...]				
management-ui <i>5m24s</i>	management-ui- <i>qrb2g</i>	<i>1/1</i>	Running	0
stars <i>5m23s</i>	backend- <i>sz87q</i>	<i>1/1</i>	Running	0
stars <i>5m21s</i>	frontend- <i>cscnf</i>	<i>1/1</i>	Running	0
[...]				

3. To connect to the management user interface, connect to the EXTERNAL-IP of the service running on your cluster:

```
kubectl get service/management-ui -n management-ui
```

4. Open the a browser to the location from the previous step. You should see the management user interface. The **C** node is the client service, the **F** node is the front-end service, and the **B** node is the back-end service. Each node has full communication access to all other nodes, as indicated by the bold, colored lines.



5. Apply the following network policy in both the `stars` and `client` namespaces to isolate the services from each other:

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: default-deny
spec:
  podSelector:
    matchLabels: {}
```

You can use the following commands to apply the policy to both namespaces:

```
kubectl apply -n stars -f https://eksworkshop.com/beginner/120_network-policies/calico/stars_policy_demo/apply_network_policies.files/default-deny.yaml
kubectl apply -n client -f https://eksworkshop.com/beginner/120_network-policies/calico/stars_policy_demo/apply_network_policies.files/default-deny.yaml
```

6. Refresh your browser. You see that the management user interface can no longer reach any of the nodes, so they don't show up in the user interface.
7. Apply the following different network policies to allow the management user interface to access the services. Apply this policy to allow the UI:

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  namespace: stars
  name: allow-ui
spec:
  podSelector:
    matchLabels: {}
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              role: management-ui
```

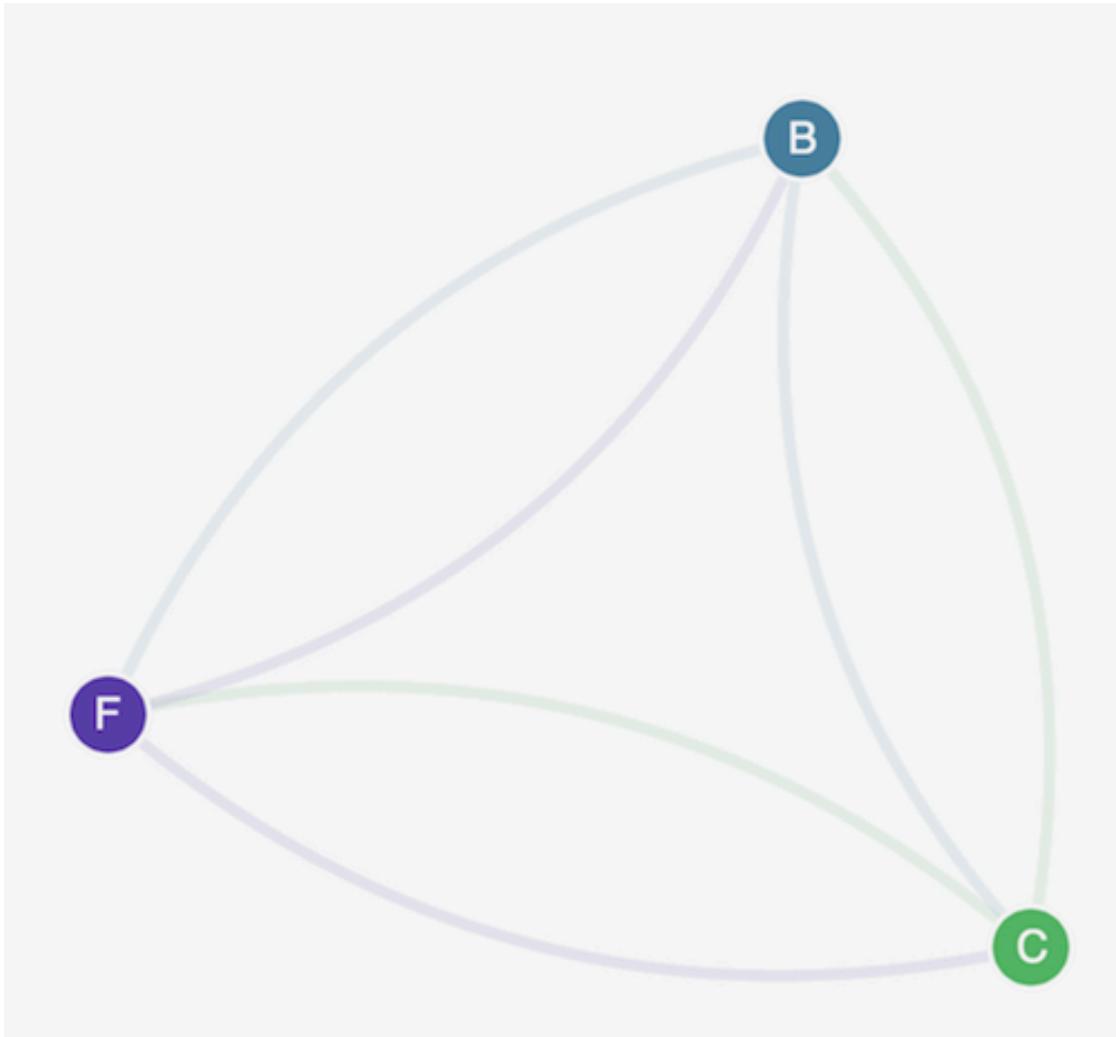
Apply this policy to allow the client:

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  namespace: client
  name: allow-ui
spec:
  podSelector:
    matchLabels: {}
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              role: management-ui
```

You can use the following commands to apply both policies:

```
kubectl apply -f https://eksworkshop.com/beginner/120_network-policies/calico/stars_policy_demo/apply_network_policies.files/allow-ui.yaml
kubectl apply -f https://eksworkshop.com/beginner/120_network-policies/calico/stars_policy_demo/apply_network_policies.files/allow-ui-client.yaml
```

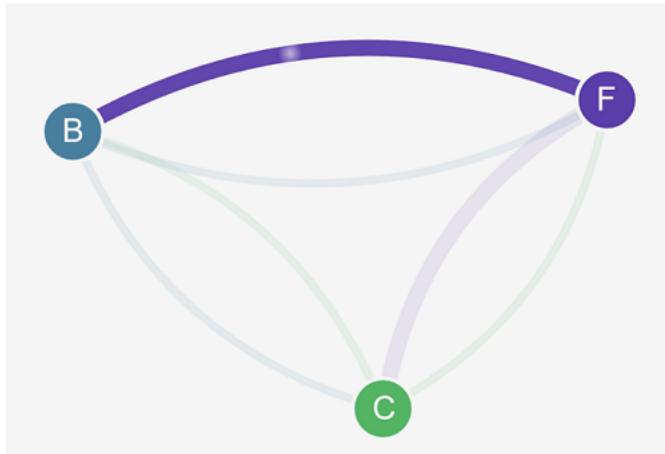
8. Refresh your browser. You see that the management user interface can reach the nodes again, but the nodes cannot communicate with each other.



9. Apply the following network policy to allow traffic from the front-end service to the back-end service:

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  namespace: stars
  name: backend-policy
spec:
  podSelector:
    matchLabels:
      role: backend
  ingress:
    - from:
        - podSelector:
            matchLabels:
              role: frontend
  ports:
    - protocol: TCP
      port: 6379
```

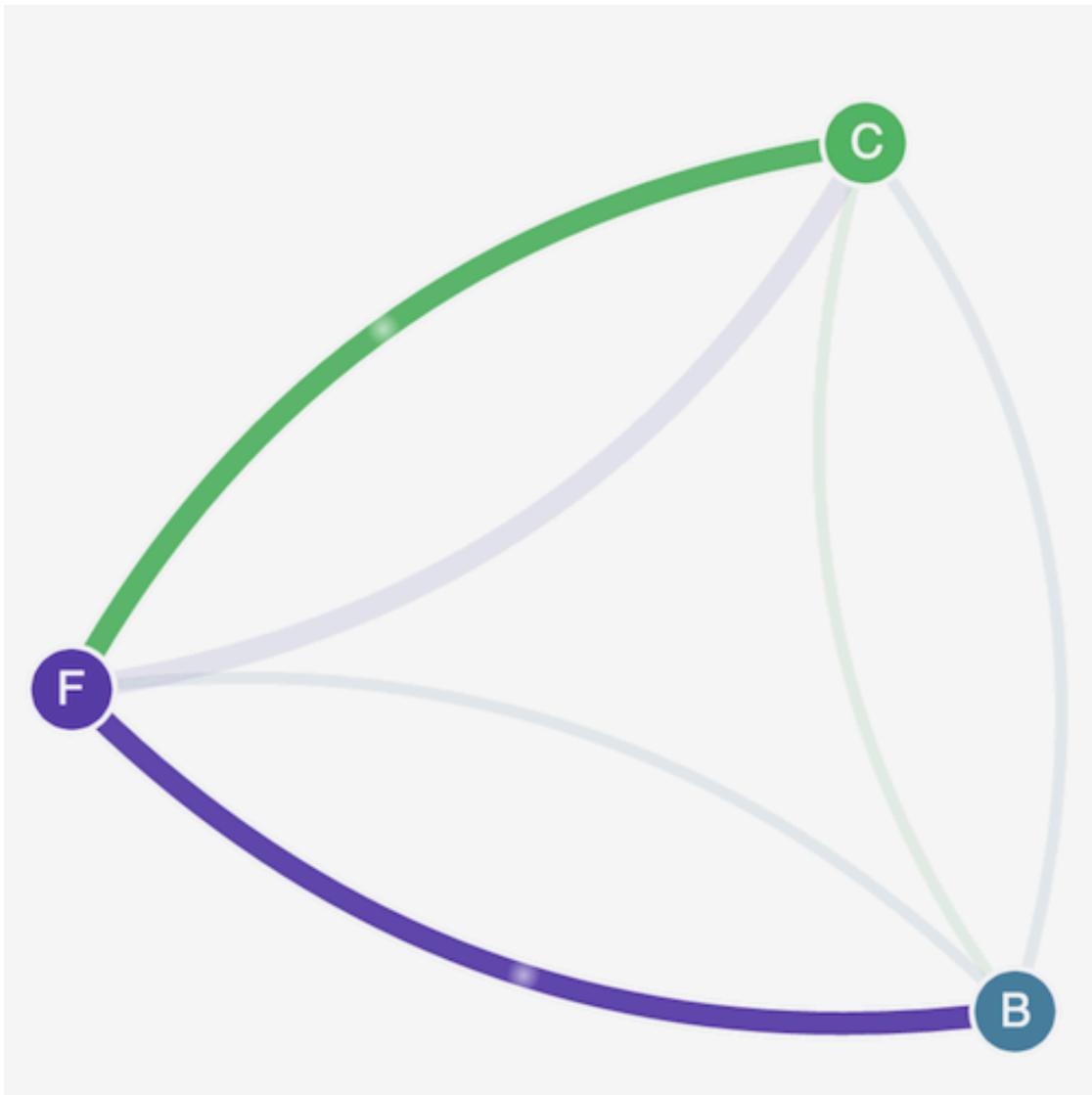
10. Refresh your browser. You see that the front-end can communicate with the back-end.



11. Apply the following network policy to allow traffic from the client to the front-end service:

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  namespace: stars
  name: frontend-policy
spec:
  podSelector:
    matchLabels:
      role: frontend
  ingress:
    - from:
        - namespaceSelector:
            matchLabels:
              role: client
      ports:
        - protocol: TCP
          port: 80
```

12. Refresh your browser. You see that the client can communicate to the front-end service. The front-end service can still communicate to the back-end service.



13. (Optional) When you are done with the demo, you can delete its resources.

```
kubectl delete -f https://eksworkshop.com/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/client.yaml
kubectl delete -f https://eksworkshop.com/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/frontend.yaml
kubectl delete -f https://eksworkshop.com/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/backend.yaml
kubectl delete -f https://eksworkshop.com/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/management-ui.yaml
kubectl delete -f https://eksworkshop.com/beginner/120_network-policies/calico/stars_policy_demo/create_resources.files/namespace.yaml
```

Even after deleting the resources, there can still be network policy endpoints on the nodes that might interfere in unexpected ways with networking in your cluster. The only sure way to remove these rules is to reboot the nodes or terminate all of the nodes and recycle them. To terminate all nodes, either set the Auto Scaling Group desired count to 0, then back up to the desired number, or just terminate the nodes.

Troubleshooting network policies

You can troubleshoot and investigate network connections that use network policies by reading the [Network policy logs \(p. 302\)](#) and by running tools from the [eBPF SDK \(p. 305\)](#).

Network policy logs

Whether connections are allowed or denied by a network policies is logged in *flow logs*. The network policy logs on each node include the flow logs for every pod that has a network policy. Network policy logs are stored at /var/log/aws-routed-eni/network-policy-agent.log. The following example is from a network-policy-agent.log file:

```
{"level": "info", "timestamp": "2023-05-30T16:05:32.573Z", "logger": "ebpf-client", "msg": "Flow Info: ", "Src IP": "192.168.87.155", "Src Port": 38971, "Dest IP": "64.6.160", "Dest Port": 53, "Proto": "UDP", "Verdict": "ACCEPT"}
```

Send network policy logs to Amazon CloudWatch Logs

You can monitor the network policy logs using services such as Amazon CloudWatch Logs. You can use the following methods to send the network policy logs to CloudWatch Logs.

For EKS clusters, the policy logs will be located under /aws/eks/*cluster-name*/cluster/ and for self-managed K8S clusters, the logs will be placed under /aws/k8s-cluster/cluster/.

Send network policy logs with Amazon VPC CNI plugin for Kubernetes

If you enable network policy, a second container is add to the aws-node pods for a *node agent*. This node agent can send the network policy logs to CloudWatch Logs.

Note

Only the network policy logs are sent by the node agent. Other logs made by the VPC CNI aren't included.

Prerequisites

- Add the following permissions as a stanza or separate policy to the IAM role that you are using for the VPC CNI.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "VisualEditor0",  
            "Effect": "Allow",  
            "Action": [  
                "logs:DescribeLogGroups",  
                "logs>CreateLogGroup",  
                "logs>CreateLogStream",  
                "logs:PutLogEvents"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Amazon EKS add-on

AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.

2. In the left navigation pane, select **Clusters**, and then select the name of the cluster that you want to configure the Amazon VPC CNI add-on for.
3. Choose the **Add-ons** tab.
4. Select the box in the top right of the add-on box and then choose **Edit**.
5. On the **Configure name of addon** page:
 - a. Select a v1.14.0-eksbuild.3 or later version in the **Version** dropdown list.
 - b. Expand the **Optional configuration settings**.
 - c. Enter the top-level JSON key "nodeAgent": and value is an object with a key "enableCloudWatchLogs": and value of "true" in **Configuration values**. The resulting text must be a valid JSON object. The following example shows both network policy and the network policy logs are enabled:

```
{  
    "enableNetworkPolicy": "true",  
    "nodeAgent": {  
        "enableCloudWatchLogs": "true"  
    }  
}
```

The following screenshot shows an example of this scenario.

The screenshot shows the 'Configure Amazon VPC CNI' page in the Amazon EKS console. At the top, there are navigation links: 'EKS > Clusters > Add-on: vpc-cni > Edit add-on'. The main title is 'Configure Amazon VPC CNI'. Below it, there's a section titled 'Amazon VPC CNI [Info](#)' with a table showing details: Listed by (Kubernetes icon), Category (networking), and Status (Active). A 'Version' dropdown is set to 'v1.14.0-eksbuild.3'. A 'Select IAM role' dropdown is shown with a placeholder 'Select an IAM role to use with this add-on. To create a new role, follow the instructions in the [Amazon EKS User Guide](#)'. Under 'Optional configuration settings', there's a 'Add-on configuration schema' section with a JSON schema code editor. The schema defines properties like 'init', 'livenessProbeTimeoutSeconds', 'nodeAgent', and 'readinessProbeTimeoutSeconds'. Below that is a 'Configuration values [Info](#)' section with a JSON code editor containing configuration values for the 'nodeAgent' property.

AWS CLI

- Run the following AWS CLI command. Replace `my-cluster` with the name of your cluster and replace the IAM role ARN with the role that you are using.

```
aws eks update-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version v1.14.0-eksbuild.3 \
--service-account-role-arn arn:aws:iam::123456789012:role/AmazonEKSVPCCNIRole \
--resolve-conflicts PRESERVE --configuration-values '{"nodeAgent": {"enableCloudWatchLogs": "true"}}'
```

Self-managed add-on

Helm

If you have installed the Amazon VPC CNI plugin for Kubernetes through helm, you can update the configuration to send network policy logs to CloudWatch Logs.

- Run the following command to enable network policy.

```
helm upgrade --set nodeAgent.enableCloudWatchLogs=true aws-vpc-cni --namespace kube-system eks/aws-vpc-cni
```

kubectl

- Open the aws-node DaemonSet in your editor.

```
kubectl edit daemonset -n kube-system aws-node
```

- Replace the false with true in the command argument --enable-cloudwatch-logs=false in the args: in the aws-network-policy-agent container in the VPC CNI aws-node daemonset manifest.

```
- args:  
  - --enable-cloudwatch-logs=true
```

Send network policy logs with a Fluent Bit daemonset

If you are using Fluent Bit in a daemonset to send logs from your nodes, you can add configuration to include the network policy logs from network policies. You can use the following example configuration:

```
[INPUT]  
Name          tail  
Tag           eksnp.*  
Path          /var/log/aws-routed-eni/network-policy-agent*.log  
Parser        json  
DB            /var/log/aws-routed-eni/flb_npagent.db  
Mem_Buf_Limit 5MB  
Skip_Long_Lines On  
Refresh_Interval 10
```

Included eBPF SDK

The Amazon VPC CNI plugin for Kubernetes installs eBPF SDK collection of tools on the nodes. You can use the eBPF SDK tools to identify issues with network policies. For example, the following command lists the programs that are running on the node.

```
sudo /opt/cni/bin/aws-eks-na-cli ebpf progs
```

To run this command, you can use any method to connect to the node.

Kubernetes network policies

To implement Kubernetes network policies you create Kubernetes NetworkPolicy objects and deploy them to your cluster. NetworkPolicy objects are scoped to a namespace. You implement policies to allow or deny traffic between Pods based on label selectors, namespaces, and IP address ranges. For

more information about creating NetworkPolicy objects, see [Network Policies](#) in the Kubernetes documentation.

Enforcement of Kubernetes NetworkPolicy objects is implemented using the Extended Berkeley Packet Filter (eBPF). Relative to iptables based implementations, it offers lower latency and performance characteristics, including reduced CPU utilization and avoiding sequential lookups. Additionally, eBPF probes provide access to context rich data that helps debug complex kernel level issues and improve observability. Amazon EKS supports an eBPF-based exporter that leverages the probes to log policy results on each node and export the data to external log collectors to aid in debugging. For more information, see the [eBPF documentation](#).

Custom networking for pods

By default, when the Amazon VPC CNI plugin for Kubernetes creates secondary [elastic network interfaces](#) (network interfaces) for your Amazon EC2 node, it creates them in the same subnet as the node's primary network interface. It also associates the same security groups to the secondary network interface that are associated to the primary network interface. For one or more of the following reasons, you might want the plugin to create secondary network interfaces in a different subnet or want to associate different security groups to the secondary network interfaces, or both:

- There's a limited number of IPv4 addresses that are available in the subnet that the primary network interface is in. This might limit the number of Pods that you can create in the subnet. By using a different subnet for secondary network interfaces, you can increase the number of available IPv4 addresses available for Pods.
- For security reasons, your Pods might need to use a different subnet or security groups than the node's primary network interface.
- The nodes are configured in public subnets, and you want to place the Pods in private subnets. The route table associated to a public subnet includes a route to an internet gateway. The route table associated to a private subnet doesn't include a route to an internet gateway.

Considerations

- With custom networking enabled, no IP addresses assigned to the primary network interface are assigned to Pods. Only IP addresses from secondary network interfaces are assigned to Pods.
- If your cluster uses the IPv6 family, you can't use custom networking.
- If you plan to use custom networking only to help alleviate IPv4 address exhaustion, you can create a cluster using the IPv6 family instead. For more information, see [Tutorial: Assigning IPv6 addresses to Pods and services \(p. 278\)](#).
- Even though Pods deployed to subnets specified for secondary network interfaces can use different subnet and security groups than the node's primary network interface, the subnets and security groups must be in the same VPC as the node.

Prerequisites

- Familiarity with how the Amazon VPC CNI plugin for Kubernetes creates secondary network interfaces and assigns IP addresses to Pods. For more information, see [ENI Allocation](#) on GitHub.
- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.

- The `kubectl` command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use `kubectl` version 1.26, 1.27, or 1.28 with it. To install or upgrade `kubectl`, see [Installing or updating kubectl \(p. 6\)](#).
- We recommend that you complete the steps in this topic in a Bash shell. If you aren't using a Bash shell, some script commands such as line continuation characters and the way variables are set and used require adjustment for your shell. Additionally, the quoting and escaping rules for your shell might be different. For more information, see [Using quotation marks with strings in the AWS CLI](#) in the AWS Command Line Interface User Guide.

For this tutorial, we recommend using the *example values*, except where it's noted to replace them. You can replace any *example value* when completing the steps for a production cluster. We recommend completing all steps in the same terminal. This is because variables are set and used throughout the steps and won't exist in different terminals.

The commands in this topic are formatted using the conventions listed in [Using the AWS CLI examples](#). If you're running commands from the command line against resources that are in a different AWS Region than the default AWS Region defined in the AWS CLI [profile](#) that you're using, then you need to add `--region region-code` to the commands.

When you want to deploy custom networking to your production cluster, skip to [the section called "Step 2: Configure your VPC" \(p. 309\)](#).

Step 1: Create a test VPC and cluster

To create a cluster

The following procedures help you create a test VPC and cluster and configure custom networking for that cluster. We don't recommend using the test cluster for production workloads because several unrelated features that you might use on your production cluster aren't covered in this topic. For more information, see [the section called "Creating a cluster" \(p. 25\)](#).

1. Define a few variables to use in the remaining steps.

```
export cluster_name=my-custom-networking-cluster
account_id=$(aws sts get-caller-identity --query Account --output text)
```

2. Create a VPC.

1. Create a VPC using an Amazon EKS AWS CloudFormation template.

```
aws cloudformation create-stack --stack-name my-eks-custom-networking-vpc \
    --template-url https://s3.us-west-2.amazonaws.com/amazon-
eks/cloudformation/2020-10-29/amazon-eks-vpc-private-subnets.yaml \
    --parameters ParameterKey=VpcBlock,ParameterValue=192.168.0.0/24 \
    ParameterKey=PrivateSubnet01Block,ParameterValue=192.168.0.64/27 \
    ParameterKey=PrivateSubnet02Block,ParameterValue=192.168.0.96/27 \
    ParameterKey=PublicSubnet01Block,ParameterValue=192.168.0.0/27 \
    ParameterKey=PublicSubnet02Block,ParameterValue=192.168.0.32/27
```

The AWS CloudFormation stack takes a few minutes to create. To check on the stack's deployment status, run the following command.

```
aws cloudformation describe-stacks --stack-name my-eks-custom-networking-vpc --query
Stacks\[].StackStatus --output text
```

Don't continue to the next step until the output of the command is CREATE_COMPLETE.

2. Define variables with the values of the private subnet IDs created by the template.

```
subnet_id_1=$(aws cloudformation describe-stack-resources --stack-name my-eks-custom-networking-vpc \
    --query "StackResources[?LogicalResourceId=='PrivateSubnet01'].PhysicalResourceId" --output text)
subnet_id_2=$(aws cloudformation describe-stack-resources --stack-name my-eks-custom-networking-vpc \
    --query "StackResources[?LogicalResourceId=='PrivateSubnet02'].PhysicalResourceId" --output text)
```

3. Define variables with the Availability Zones of the subnets retrieved in the previous step.

```
az_1=$(aws ec2 describe-subnets --subnet-ids $subnet_id_1 --query
    'Subnets[*].AvailabilityZone' --output text)
az_2=$(aws ec2 describe-subnets --subnet-ids $subnet_id_2 --query
    'Subnets[*].AvailabilityZone' --output text)
```

3. Create a cluster IAM role.

- a. Run the following command to create an IAM trust policy JSON file.

```
cat >eks-cluster-role-trust-policy.json <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "eks.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
```

- b. Create the Amazon EKS cluster IAM role. If necessary, preface eks-cluster-role-trust-policy.json with the path on your computer that you wrote the file to in the previous step. The command associates the trust policy that you created in the previous step to the role. To create an IAM role, the [IAM principal](#) that is creating the role must be assigned the iam:CreateRole action (permission).

```
aws iam create-role --role-name myCustomNetworkingAmazonEKSClusterRole --assume-role-policy-document file:///"eks-cluster-role-trust-policy.json"
```

- c. Attach the Amazon EKS managed policy named [AmazonEKSClusterPolicy](#) to the role. To attach an IAM policy to an [IAM principal](#), the principal that is attaching the policy must be assigned one of the following IAM actions (permissions): iam:AttachUserPolicy or iam:AttachRolePolicy.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/
AmazonEKSClusterPolicy --role-name myCustomNetworkingAmazonEKSClusterRole
```

4. Create an Amazon EKS cluster and configure your device to communicate with it.

- a. Create a cluster.

```
aws eks create-cluster --name my-custom-networking-cluster \
```

```
--role-arn arn:aws:iam::$account_id:role/myCustomNetworkingAmazonEKSClusterRole
\ --resources-vpc-config subnetIds=$subnet_id_1,"$subnet_id_2
```

Note

You might receive an error that one of the Availability Zones in your request doesn't have sufficient capacity to create an Amazon EKS cluster. If this happens, the error output contains the Availability Zones that can support a new cluster. Retry creating your cluster with at least two subnets that are located in the supported Availability Zones for your account. For more information, see [Insufficient capacity \(p. 562\)](#).

- b. The cluster takes several minutes to create. To check on the cluster's deployment status, run the following command.

```
aws eks describe-cluster --name my-custom-networking-cluster --query cluster.status
```

Don't continue to the next step until the output of the command is "ACTIVE".

- c. Configure kubectl to communicate with your cluster.

```
aws eks update-kubeconfig --name my-custom-networking-cluster
```

Step 2: Configure your VPC

This tutorial requires the VPC created in [the section called "Step 1: Create a test VPC and cluster" \(p. 307\)](#). For a production cluster, adjust the steps accordingly for your VPC by replacing all of the *example values* with your own.

1. Confirm that your currently-installed Amazon VPC CNI plugin for Kubernetes is the latest version. To determine the latest version for the Amazon EKS add-on type and update your version to it, see [the section called "Updating an add-on" \(p. 400\)](#). To determine the latest version for the self-managed add-on type and update your version to it, see [the section called "Amazon VPC CNI plugin for Kubernetes" \(p. 266\)](#).
2. Retrieve the ID of your cluster VPC and store it in a variable for use in later steps. For a production cluster, replace *my-custom-networking-cluster* with the name of your cluster.

```
vpc_id=$(aws eks describe-cluster --name my-custom-networking-cluster --query "cluster.resourcesVpcConfig.vpcId" --output text)
```

3. Associate an additional Classless Inter-Domain Routing (CIDR) block with your cluster's VPC. The CIDR block can't overlap with any existing associated CIDR blocks.
 1. View the current CIDR blocks associated to your VPC.

```
aws ec2 describe-vpcs --vpc-ids $vpc_id \
--query 'Vpcs[*].CidrBlockAssociationSet[*].{CidrBlock: CidrBlock, State: CidrBlockState.State}' --out table
```

An example output is as follows.

```
-----|-----|-----|
|     DescribeVpcs      | |
+-----+-----+-----+
|   CIDRBlock    |   State   | |
+-----+-----+-----+
| 192.168.0.0/24 | associated |
```

- +-----+-----+
- Associate an additional CIDR block to your VPC. For more information, see [Associate additional IPv4 CIDR blocks with your VPC](#) in the Amazon VPC User Guide.

```
aws ec2 associate-vpc-cidr-block --vpc-id $vpc_id --cidr-block 192.168.1.0/24
```

- Confirm that the new block is associated.

```
aws ec2 describe-vpcs --vpc-ids $vpc_id --query 'Vpcs[*].CidrBlockAssociationSet[*].{CIDRBlock: CidrBlock, State: CidrBlockState.State}' --out table
```

An example output is as follows.

```
+-----+
|      DescribeVpcs      |
+-----+-----+
|  CIDRBlock   |  State   |
+-----+-----+
| 192.168.0.0/24 |  associated  |
| 192.168.1.0/24 |  associated  |
+-----+-----+
```

Don't proceed to the next step until your new CIDR block's State is associated.

- Create as many subnets as you want to use in each Availability Zone that your existing subnets are in. Specify a CIDR block that's within the CIDR block that you associated with your VPC in a previous step.
- Create new subnets. The subnets must be created in a different VPC CIDR block than your existing subnets are in, but in the same Availability Zones as your existing subnets. In this example, one subnet is created in the new CIDR block in each Availability Zone that the current private subnets exist in. The IDs of the subnets created are stored in variables for use in later steps. The Name values match the values assigned to the subnets created using the Amazon EKS VPC template in a previous step. Names aren't required. You can use different names.

```
new_subnet_id_1=$(aws ec2 create-subnet --vpc-id $vpc_id --availability-zone $az_1 --
cidr-block 192.168.1.0/27 \
--tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=my-eks-custom-
networking-vpc-PrivateSubnet01},{Key=kubernetes.io/role/internal-elb,Value=1}]' \
--query Subnet.SubnetId --output text)
new_subnet_id_2=$(aws ec2 create-subnet --vpc-id $vpc_id --availability-zone $az_2 --
cidr-block 192.168.1.32/27 \
--tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=my-eks-custom-
networking-vpc-PrivateSubnet02},{Key=kubernetes.io/role/internal-elb,Value=1}]' \
--query Subnet.SubnetId --output text)
```

Important

By default, your new subnets are implicitly associated with your VPC's [main route table](#). This route table allows communication between all the resources that are deployed in the VPC. However, it doesn't allow communication with resources that have IP addresses that are outside the CIDR blocks that are associated with your VPC. You can associate your own route table to your subnets to change this behavior. For more information, see [Subnet route tables](#) in the Amazon VPC User Guide.

- View the current subnets in your VPC.

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=$vpc_id" \
```

```
--query 'Subnets[*].{SubnetId: SubnetId,AvailabilityZone: AvailabilityZone,CidrBlock: CidrBlock}' \
--output table
```

An example output is as follows.

DescribeSubnets		
AvailabilityZone	CidrBlock	SubnetId
us-west-2d	192.168.0.0/27	subnet-example1
us-west-2a	192.168.0.32/27	subnet-example2
us-west-2a	192.168.0.64/27	subnet-example3
us-west-2d	192.168.0.96/27	subnet-example4
us-west-2a	192.168.1.0/27	subnet-example5
us-west-2d	192.168.1.32/27	subnet-example6

You can see the subnets in the 192.168.1.0 CIDR block that you created are in the same Availability Zones as the subnets in the 192.168.0.0 CIDR block.

Step 3: Configure Kubernetes resources

To configure Kubernetes resources

- Set the AWS_VPC_K8S_CNI_CUSTOM_NETWORK_CFG environment variable to true in the aws-node DaemonSet.

```
kubectl set env daemonset aws-node -n kube-system
AWS_VPC_K8S_CNI_CUSTOM_NETWORK_CFG=true
```

- Retrieve the ID of your [cluster security group \(p. 263\)](#) and store it in a variable for use in the next step. Amazon EKS automatically creates this security group when you create your cluster.

```
cluster_security_group_id=$(aws eks describe-cluster --name $cluster_name --query
cluster.resourcesVpcConfig.clusterSecurityGroupId --output text)
```

- Create an ENIConfig custom resource for each subnet that you want to deploy Pods in.
 - Create a unique file for each network interface configuration.

The following commands create separate ENIConfig files for the two subnets that were created in a previous step. The value for name must be unique. The name is the same as the Availability Zone that the subnet is in. The cluster security group is assigned to the ENIConfig.

```
cat >$az_1.yaml <<EOF
apiVersion: crd.k8s.amazonaws.com/v1alpha1
kind: ENIConfig
metadata:
  name: $az_1
spec:
  securityGroups:
    - $cluster_security_group_id
  subnet: $new_subnet_id_1
EOF
```

```
cat >$az_2.yaml <<EOF
apiVersion: crd.k8s.amazonaws.com/v1alpha1
kind: ENIConfig
metadata:
  name: $az_2
spec:
  securityGroups:
    - $cluster_security_group_id
  subnet: $new_subnet_id_2
EOF
```

For a production cluster, you can make the following changes to the previous commands:

- Replace `$cluster_security_group_id` with the ID of an existing [security group](#) that you want to use for each ENIConfig.
- We recommend naming your ENIConfigs the same as the Availability Zone that you'll use the ENIConfig for, whenever possible. You might need to use different names for your ENIConfigs than the names of the Availability Zones for a variety of reasons. For example, if you have more than two subnets in the same Availability Zone and want to use them both with custom networking, then you need multiple ENIConfigs for the same Availability Zone. Since each ENIConfig requires a unique name, you can't name more than one of your ENIConfigs using the Availability Zone name.

If your ENIConfig names aren't all the same as Availability Zone names, then replace `$az_1` and `$az_2` with your own names in the previous commands and [annotate your nodes with the ENIConfig \(p. 315\)](#) later in this tutorial.

Note

If you don't specify a valid security group for use with a production cluster and you're using:

- version 1.8.0 or later of the Amazon VPC CNI plugin for Kubernetes, then the security groups associated with the node's primary elastic network interface are used.
- a version of the Amazon VPC CNI plugin for Kubernetes that's earlier than 1.8.0, then the default security group for the VPC is assigned to secondary network interfaces.

Important

- `AWS_VPC_K8S_CNI_EXTERNALSNAT=false` is a default setting in the configuration for the Amazon VPC CNI plugin for Kubernetes. If you're using the default setting, then traffic that is destined for IP addresses that aren't within one of the CIDR blocks associated with your VPC use the security groups and subnets of your node's primary network interface. The subnets and security groups defined in your ENIConfigs that are used to create secondary network interfaces aren't used for this traffic. For more information about this setting, see [SNAT for Pods \(p. 289\)](#).
- If you also use security groups for Pods, the security group that's specified in a `SecurityGroupPolicy` is used instead of the security group that's specified in the ENIConfigs. For more information, see [Tutorial: Security groups for Pods \(p. 324\)](#).

- b. Apply each custom resource file that you created to your cluster with the following commands.

```
kubectl apply -f $az_1.yaml
kubectl apply -f $az_2.yaml
```

4. Confirm that your ENIConfigs were created.

```
kubectl get ENIConfigs
```

An example output is as follows.

NAME	AGE
us-west-2a	117s
us-west-2d	105s

5. If you're enabling custom networking on a production cluster and named your ENIConfigs something other than the Availability Zone that you're using them for, then skip to the [next step \(p. 313\)](#) to deploy Amazon EC2 nodes.

Enable Kubernetes to automatically apply the ENIConfig for an Availability Zone to any new Amazon EC2 nodes created in your cluster.

1. For the test cluster in this tutorial, skip to the [next step \(p. 313\)](#).

For a production cluster, check to see if an annotation with the key `k8s.amazonaws.com/eniConfig` for the [ENI_CONFIG_ANNOTATION_DEF](#) environment variable exists in the container spec for the `aws-node` DaemonSet.

```
kubectl describe daemonset aws-node -n kube-system | grep ENI_CONFIG_ANNOTATION_DEF
```

If output is returned, the annotation exists. If no output is returned, then the variable is not set. For a production cluster, you can use either this setting or the setting in the following step. If you use this setting, it overrides the setting in the following step. In this tutorial, the setting in the next step is used.

2. Update your `aws-node` DaemonSet to automatically apply the ENIConfig for an Availability Zone to any new Amazon EC2 nodes created in your cluster.

```
kubectl set env daemonset aws-node -n kube-system  
ENI_CONFIG_LABEL_DEF=topology.kubernetes.io/zone
```

Step 4: Deploy Amazon EC2 nodes

To deploy Amazon EC2 nodes

1. Create a node IAM role.
 - a. Run the following command to create an IAM trust policy JSON file.

```
cat >node-role-trust-relationship.json <<EOF  
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "ec2.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

EOF

- b. Run the following command to set a variable for your role name. You can replace `myCustomNetworkingAmazonEKSNodeRole` with any name you choose.

```
export node_role_name=myCustomNetworkingAmazonEKSNodeRole
```

- c. Create the IAM role and store its returned Amazon Resource Name (ARN) in a variable for use in a later step.

```
node_role_arn=$(aws iam create-role --role-name $node_role_name --assume-role-policy-document file://"node-role-trust-relationship.json" \
--query Role.Arn --output text)
```

- d. Attach three required IAM managed policies to the IAM role.

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy \
--role-name $node_role_name
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly \
--role-name $node_role_name
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy \
--role-name $node_role_name
```

Important

For simplicity in this tutorial, the [AmazonEKS_CNI_Policy](#) policy is attached to the node IAM role. In a production cluster however, we recommend attaching the policy to a separate IAM role that is used only with the Amazon VPC CNI plugin for Kubernetes.

For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).

2. Create one of the following types of node groups. To determine the instance type that you want to deploy, see [Choosing an Amazon EC2 instance type \(p. 152\)](#). For this tutorial, complete the **Managed, Without a launch template or with a launch template without an AMI ID specified** option. If you're going to use the node group for production workloads, then we recommend that you familiarize yourself with all of the [managed \(p. 85\)](#) and [self-managed \(p. 108\)](#) node group options before deploying the node group.

- **Managed** – Deploy your node group using one of the following options:

- **Without a launch template or with a launch template without an AMI ID specified** – Run the following command. For this tutorial, use the *example values*. For a production node group, replace all *example values* with your own. The node group name can't be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters.

```
aws eks create-nodegroup --cluster-name $cluster_name --nodegroup-name my-nodegroup \
\
--subnets $subnet_id_1 $subnet_id_2 --instance-types t3.medium --node-role \
$node_role_arn
```

- **With a launch template with a specified AMI ID**

1. Determine the Amazon EKS recommended number of maximum Pods for your nodes. Follow the instructions in [Amazon EKS recommended maximum Pods for each Amazon EC2 instance type \(p. 154\)](#), adding `--cni-custom-networking-enabled` to step 3 in that topic. Note the output for use in the next step.

2. In your launch template, specify an Amazon EKS optimized AMI ID, or a custom AMI built off the Amazon EKS optimized AMI, then [deploy the node group using a launch template \(p. 98\)](#) and provide the following user data in the launch template. This user data passes arguments into the bootstrap.sh file. For more information about the bootstrap file, see [bootstrap.sh](#) on GitHub. You can replace **20** with either the value from the previous step (recommended) or your own value.

```
/etc/eks/bootstrap.sh my-cluster --use-max-pods false --kubelet-extra-args '--max-pods=20'
```

If you've created a custom AMI that is not built off the Amazon EKS optimized AMI, then you need to custom create the configuration yourself.

- **Self-managed**

1. Determine the Amazon EKS recommended number of maximum Pods for your nodes. Follow the instructions in [Amazon EKS recommended maximum Pods for each Amazon EC2 instance type \(p. 154\)](#), adding **--cni-custom-networking-enabled** to step 3 in that topic. Note the output for use in the next step.
2. Deploy the node group using the instructions in [Launching self-managed Amazon Linux nodes \(p. 108\)](#). Specify the following text for the **BootstrapArguments** parameter. You can replace **20** with either the value from the previous step (recommended) or your own value.

```
--use-max-pods false --kubelet-extra-args '--max-pods=20'
```

Note

If you want nodes in a production cluster to support a significantly higher number of Pods, run the script in [Amazon EKS recommended maximum Pods for each Amazon EC2 instance type \(p. 154\)](#) again. Also, add the **--cni-prefix-delegation-enabled** option to the command. For example, **110** is returned for an m5.large instance type. For instructions on how to enable this capability, see [Increase the amount of available IP addresses for your Amazon EC2 nodes \(p. 318\)](#). You can use this capability with custom networking.

Node group creation takes several minutes. You can check the status of the creation of a managed node group with the following command.

```
aws eks describe-nodegroup --cluster-name $cluster_name --nodegroup-name my-nodegroup --query nodegroup.status --output text
```

Don't continue to the next step until the output returned is ACTIVE.

3. For the tutorial, you can skip this step.

For a production cluster, if you didn't name your ENICConfigs the same as the Availability Zone that you're using them for, then you must annotate your nodes with the ENICConfig name that should be used with the node. This step isn't necessary if you only have one subnet in each Availability Zone and you named your ENICConfigs with the same names as your Availability Zones. This is because the Amazon VPC CNI plugin for Kubernetes automatically associates the correct ENICConfig with the node for you when you enabled it to do so in a [previous step \(p. 313\)](#).

- a. Get the list of nodes in your cluster.

```
kubectl get nodes
```

An example output is as follows.

NAME	STATUS	ROLES	AGE	VERSION
ip-192-168-0-126.us-west-2.compute.internal eks-810597c	Ready	<none>	8m49s	v1.22.9-
ip-192-168-0-92.us-west-2.compute.internal eks-810597c	Ready	<none>	8m34s	v1.22.9-

- b. Determine which Availability Zone each node is in. Run the following command for each node that was returned in the previous step.

```
aws ec2 describe-instances --filters Name=network-interface.private-dns-name,Values=ip-192-168-0-126.us-west-2.compute.internal \
--query 'Reservations[].[Instances].[{AvailabilityZone: Placement.AvailabilityZone, SubnetId: SubnetId}]'
```

An example output is as follows.

```
[  
  {  
    "AvailabilityZone": "us-west-2d",  
    "SubnetId": "subnet-Example5"  
  }  
]
```

- c. Annotate each node with the ENIConfig that you created for the subnet ID and Availability Zone. You can only annotate a node with one ENIConfig, though multiple nodes can be annotated with the same ENIConfig. Replace the *example values* with your own.

```
kubectl annotate node ip-192-168-0-126.us-west-2.compute.internal k8s.amazonaws.com/eniConfig=EniConfigName1  
kubectl annotate node ip-192-168-0-92.us-west-2.compute.internal k8s.amazonaws.com/eniConfig=EniConfigName2
```

4. If you had nodes in a production cluster with running Pods before you switched to using the custom networking feature, complete the following tasks:
- Make sure that you have available nodes that are using the custom networking feature.
 - Cordon and drain the nodes to gracefully shut down the Pods. For more information, see [Safely Drain a Node](#) in the Kubernetes documentation.
 - Terminate the nodes. If the nodes are in an existing managed node group, you can delete the node group. Copy the command that follows to your device. Make the following modifications to the command as needed and then run the modified command:
 - Replace *my-cluster* with the name for your cluster.
 - Replace *my-nodegroup* with the name for your node group.

```
aws eks delete-nodegroup --cluster-name my-cluster --nodegroup-name my-nodegroup
```

Only new nodes that are registered with the k8s.amazonaws.com/eniConfig label use the custom networking feature.

5. Confirm that Pods are assigned an IP address from a CIDR block that's associated to one of the subnets that you created in a previous step.

```
kubectl get pods -A -o wide
```

An example output is as follows.

NAMESPACE NODE	NAME	READY	STATUS	RESTARTS	AGE	IP READINESS GATES
kube-system	aws-node- <i>2rkn4</i>	1/1	Running	0	7m19s	<none>
	192.168.0.92	ip-192-168-0-92.us-west-2.compute.internal				<none>
kube-system	aws-node- <i>k96wp</i>	1/1	Running	0	7m15s	<none>
	192.168.0.126	ip-192-168-0-126.us-west-2.compute.internal				<none>
kube-system	coredns- <i>657694c6f4-smcg</i>	1/1	Running	0	56m	<none>
	192.168.1.23	ip-192-168-0-92.us-west-2.compute.internal				<none>
kube-system	coredns- <i>657694c6f4-stwv9</i>	1/1	Running	0	56m	<none>
	192.168.1.28	ip-192-168-0-92.us-west-2.compute.internal				<none>
kube-system	kube-proxy- <i>jgshq</i>	1/1	Running	0	7m19s	<none>
	192.168.0.92	ip-192-168-0-92.us-west-2.compute.internal				<none>
kube-system	kube-proxy- <i>wx9vk</i>	1/1	Running	0	7m15s	<none>
	192.168.0.126	ip-192-168-0-126.us-west-2.compute.internal				<none>

You can see that the coredns Pods are assigned IP addresses from the 192.168.1.0 CIDR block that you added to your VPC. Without custom networking, they would have been assigned addresses from the 192.168.0.0 CIDR block, because it was the only CIDR block originally associated with the VPC.

If a Pod's spec contains hostNetwork=true, it's assigned the primary IP address of the node. It isn't assigned an address from the subnets that you added. By default, this value is set to false. This value is set to true for the kube-proxy and Amazon VPC CNI plugin for Kubernetes (aws-node) Pods that run on your cluster. This is why the kube-proxy and the plugin's aws-node Pods aren't assigned 192.168.1.x addresses in the previous output. For more information about a Pod's hostNetwork setting, see [PodSpec v1 core](#) in the Kubernetes API reference.

Step 5: Delete tutorial resources

After you complete the tutorial, we recommend that you delete the resources that you created. You can then adjust the steps to enable custom networking for a production cluster.

To delete the tutorial resources

1. If the node group that you created was just for testing, then delete it.

```
aws eks delete-nodegroup --cluster-name $cluster_name --nodegroup-name my-nodegroup
```

Even after the AWS CLI output says that the cluster is deleted, the delete process might not actually be complete. The delete process takes a few minutes. Confirm that it's complete by running the following command.

```
aws eks describe-nodegroup --cluster-name $cluster_name --nodegroup-name my-nodegroup --query nodegroup.status --output text
```

Don't continue until the returned output is similar to the following output.

```
An error occurred (ResourceNotFoundException) when calling the DescribeNodegroup operation: No node group found for name: my-nodegroup.
```

2. If the node group that you created was just for testing, then delete the node IAM role.

- a. Detach the policies from the role.

```
aws iam detach-role-policy --role-name myCustomNetworkingAmazonEKSNodeRole --  
policy-arn arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy  
aws iam detach-role-policy --role-name myCustomNetworkingAmazonEKSNodeRole --  
policy-arn arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly  
aws iam detach-role-policy --role-name myCustomNetworkingAmazonEKSNodeRole --  
policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
```

- b. Delete the role.

```
aws iam delete-role --role-name myCustomNetworkingAmazonEKSNodeRole
```

3. Delete the cluster.

```
aws eks delete-cluster --name $cluster_name
```

Confirm the cluster is deleted with the following command.

```
aws eks describe-cluster --name $cluster_name --query cluster.status --output text
```

When output similar to the following is returned, the cluster is successfully deleted.

```
An error occurred (ResourceNotFoundException) when calling the DescribeCluster  
operation: No cluster found for name: my-cluster.
```

4. Delete the cluster IAM role.

- a. Detach the policies from the role.

```
aws iam detach-role-policy --role-name myCustomNetworkingAmazonEKSClusterRole --  
policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy
```

- b. Delete the role.

```
aws iam delete-role --role-name myCustomNetworkingAmazonEKSClusterRole
```

5. Delete the subnets that you created in a previous step.

```
aws ec2 delete-subnet --subnet-id $new_subnet_id_1  
aws ec2 delete-subnet --subnet-id $new_subnet_id_2
```

6. Delete the VPC that you created.

```
aws cloudformation delete-stack --stack-name my-eks-custom-networking-vpc
```

Increase the amount of available IP addresses for your Amazon EC2 nodes

Each Amazon EC2 instance supports a maximum number of elastic network interfaces and a maximum number of IP addresses that can be assigned to each network interface. Each node requires one IP address for each network interface. All other available IP addresses can be assigned to Pods. Each Pod requires its own IP address. As a result, you might have nodes that have available compute and memory resources, but can't accommodate additional Pods because the node has run out of IP addresses to assign to Pods.

In this topic, you learn how to significantly increase the number of IP addresses that nodes can assign to Pods by assigning IP prefixes, rather than assigning individual secondary IP addresses to your nodes.

Each prefix includes several IP addresses. If you don't configure your cluster for IP prefix assignment, your cluster must make more Amazon EC2 application programming interface (API) calls to configure network interfaces and IP addresses necessary for Pod connectivity. As clusters grow to larger sizes, the frequency of these API calls can lead to longer Pod and instance launch times. This results in scaling delays to meet the demand of large and spiky workloads, and adds cost and management overhead because you need to provision additional clusters and VPCs to meet scaling requirements. For more information, see [Kubernetes Scalability thresholds](#) on GitHub.

Considerations

- Each Amazon EC2 instance type supports a maximum number of Pods. If your managed node group consists of multiple instance types, the smallest number of maximum Pods for an instance in the cluster is applied to all nodes in the cluster.
- By default, the maximum number of Pods that you can run on a node is 110, but you can change that number. If you change the number and have an existing managed node group, the next AMI or launch template update of your node group results in new nodes coming up with the changed value.
- When transitioning from assigning IP addresses to assigning IP prefixes, we recommend that you create new node groups to increase the number of available IP addresses, rather than doing a rolling replacement of existing nodes. Running Pods on a node that has both IP addresses and prefixes assigned can lead to inconsistency in the advertised IP address capacity, impacting the future workloads on the node. For the recommended way of performing the transition, see [Replace all nodes during migration from Secondary IP mode to Prefix Delegation mode or vice versa](#) in the Amazon EKS best practices guide.
- For clusters with Linux nodes only.
 - Once you configure the add-on to assign prefixes to network interfaces, you can't downgrade your Amazon VPC CNI plugin for Kubernetes add-on to a version lower than 1.9.0 (or 1.10.1) without removing all nodes in all node groups in your cluster.
 - If you're also using security groups for Pods, with `POD_SECURITY_GROUP_ENFORCING_MODE=standard` and `AWS_VPC_K8S_CNI_EXTERNALSNAT=false`, when your Pods communicate with endpoints outside of your VPC, the node's security groups are used, rather than any security groups you've assigned to your Pods.

If you're also using [security groups for Pods \(p. 324\)](#), with `POD_SECURITY_GROUP_ENFORCING_MODE=strict`, when your Pods communicate with endpoints outside of your VPC, the Pod's security groups are used.

Prerequisites

- An existing cluster. To deploy one, see [Creating an Amazon EKS cluster \(p. 25\)](#).
- The subnets that your Amazon EKS nodes are in must have sufficient contiguous /28 (for IPv4 clusters) or /80 (for IPv6 clusters) Classless Inter-Domain Routing (CIDR) blocks. You can only have Linux nodes in an IPv6 cluster. Using IP prefixes can fail if IP addresses are scattered throughout the subnet CIDR. We recommend that following:
 - Using a subnet CIDR reservation so that even if any IP addresses within the reserved range are still in use, upon their release, the IP addresses aren't reassigned. This ensures that prefixes are available for allocation without segmentation.
 - Use new subnets that are specifically used for running the workloads that IP prefixes are assigned to. Both Windows and Linux workloads can run in the same subnet when assigning IP prefixes.
- To assign IP prefixes to your nodes, your nodes must be AWS Nitro-based. Instances that aren't Nitro-based continue to allocate individual secondary IP addresses, but have a significantly lower number of IP addresses to assign to Pods than Nitro-based instances do.

- **For clusters with Linux nodes only** – If your cluster is configured for the IPv4 family, you must have version 1.9.0 or later of the Amazon VPC CNI plugin for Kubernetes add-on installed. You can check your current version with the following command.

```
kubectl describe daemonset aws-node --namespace kube-system | grep Image | cut -d "/" -f 2
```

If your cluster is configured for the IPv6 family, you must have version 1.10.1 of the add-on installed. If your plugin version is earlier than the required versions, you must update it. For more information, see the updating sections of [Working with the Amazon VPC CNI plugin for Kubernetes Amazon EKS add-on \(p. 266\)](#).

- **For clusters with Windows nodes only**

- Your cluster and its platform version must be at, or later than the versions in the following table. To upgrade your cluster version, see [the section called “Updating Kubernetes version” \(p. 34\)](#). If your cluster isn't at the minimum platform version, then you can't assign IP prefixes to your nodes until Amazon EKS has updated your platform version.

Kubernetes version	Platform version
1.27	eks.3
1.26	eks.4
1.25	eks.5

You can check your current Kubernetes and platform version by replacing *my-cluster* in the following command with the name of your cluster and then running the modified command:
aws eks describe-cluster --name *my-cluster* --query 'cluster.{“Kubernetes Version”: version, “Platform Version”: platformVersion}’.

- Windows support enabled for your cluster. For more information, see [the section called “Enabling Windows support” \(p. 49\)](#).

To increase the amount of available IP addresses for your Amazon EC2 nodes

1. Configure your cluster to assign IP address prefixes to nodes. Complete the procedure on the tab that matches your node's operating system.

Linux

1. Enable the parameter to assign prefixes to network interfaces for the Amazon VPC CNI DaemonSet. When you deploy a 1.21 or later cluster, version 1.10.1 or later of the Amazon VPC CNI plugin for Kubernetes add-on is deployed with it. If you created the cluster with the IPv6 family, this setting was set to true by default. If you created the cluster with the IPv4 family, this setting was set to false by default.

```
kubectl set env daemonset aws-node -n kube-system ENABLE_PREFIX_DELEGATION=true
```

Important

Even if your subnet has available IP addresses, if the subnet does not have any contiguous /28 blocks available, you will see the following error in the Amazon VPC CNI plugin for Kubernetes logs.

`InsufficientCidrBlocks`: The specified subnet does not have enough free cidr blocks to satisfy the request

This can happen due to fragmentation of existing secondary IP addresses spread out across a subnet. To resolve this error, either create a new subnet and launch Pods there, or use an Amazon EC2 subnet CIDR reservation to reserve space within a subnet for use with prefix assignment. For more information, see [Subnet CIDR reservations](#) in the Amazon VPC User Guide.

2. If you plan to deploy a managed node group without a launch template, or with a launch template that you haven't specified an AMI ID in, and you're using a version of the Amazon VPC CNI plugin for Kubernetes at or later than the versions listed in the prerequisites, then skip to the next step. Managed node groups automatically calculates the maximum number of Pods for you.

If you're deploying a self-managed node group or a managed node group with a launch template that you have specified an AMI ID in, then you must determine the Amazon EKS recommend number of maximum Pods for your nodes. Follow the instructions in [Amazon EKS recommended maximum Pods for each Amazon EC2 instance type \(p. 154\)](#), adding `--cni-prefix-delegation-enabled` to step 3. Note the output for use in a later step.

Important

Managed node groups enforces a maximum number on the value of maxPods. For instances with less than 30 vCPUs the maximum number is 110 and for all other instances the maximum number is 250. This maximum number is applied whether prefix delegation is enabled or not.

3. If you're using a 1.21 or later cluster configured for IPv6, skip to the next step.

Specify the parameters in one of the following options. To determine which option is right for you and what value to provide for it, see [WARM_PREFIX_TARGET](#), [WARM_IP_TARGET](#), and [MINIMUM_IP_TARGET](#) on GitHub.

You can replace the *example values* with a value greater than zero.

- `WARM_PREFIX_TARGET`

```
kubectl set env ds aws-node -n kube-system WARM_PREFIX_TARGET=1
```

- `WARM_IP_TARGET` or `MINIMUM_IP_TARGET` – If either value is set, it overrides any value set for `WARM_PREFIX_TARGET`.

```
kubectl set env ds aws-node -n kube-system WARM_IP_TARGET=5
```

```
kubectl set env ds aws-node -n kube-system MINIMUM_IP_TARGET=2
```

4. Create one of the following types of node groups with at least one Amazon EC2 Nitro Amazon Linux 2 instance type. For a list of Nitro instance types, see [Instances built on the Nitro System](#) in the Amazon EC2 User Guide for Linux Instances. This capability is not supported on Windows. For the options that include `110`, replace it with either the value from step 3 (recommended), or your own value.
 - **Self-managed** – Deploy the node group using the instructions in [Launching self-managed Amazon Linux nodes \(p. 108\)](#). Specify the following text for the `BootstrapArguments` parameter.

```
--use-max-pods false --kubelet-extra-args '--max-pods=110'
```

If you're using eksctl to create the node group, you can use the following command.

```
eksctl create nodegroup --cluster my-cluster --managed=false --max-pods-per-node 110
```

- **Managed** – Deploy your node group using one of the following options:
 - **Without a launch template or with a launch template without an AMI ID specified** – Complete the procedure in [Creating a managed node group \(p. 85\)](#). Managed node groups automatically calculates the Amazon EKS recommended max-pods value for you.
 - **With a launch template with a specified AMI ID** – In your launch template, specify an Amazon EKS optimized AMI ID, or a custom AMI built off the Amazon EKS optimized AMI, then [deploy the node group using a launch template \(p. 98\)](#) and provide the following user data in the launch template. This user data passes arguments into the bootstrap.sh file. For more information about the bootstrap file, see [bootstrap.sh](#) on GitHub.

```
/etc/eks/bootstrap.sh my-cluster \  
  --use-max-pods false \  
  --kubelet-extra-args '--max-pods=110'
```

If you're using eksctl to create the node group, you can use the following command.

```
eksctl create nodegroup --cluster my-cluster --max-pods-per-node 110
```

If you've created a custom AMI that is not built off the Amazon EKS optimized AMI, then you need to custom create the configuration yourself.

Note

If you also want to assign IP addresses to Pods from a different subnet than the instance's, then you need to enable the capability in this step. For more information, see [Custom networking for pods \(p. 306\)](#).

Windows

1. Enable assignment of IP prefixes.
 - a. Open the amazon-vpc-cni ConfigMap for editing.

```
kubectl edit configmap -n kube-system amazon-vpc-cni -o yaml
```

- b. Add the following line to the data section.

```
enable-windows-prefix-delegation: "true"
```

- c. Save the file and close the editor.
- d. Confirm that the line was added to the ConfigMap.

```
kubectl get configmap -n kube-system amazon-vpc-cni -o "jsonpath={.data.enable-windows-prefix-delegation}"
```

If the returned output isn't true, then there might have been an error. Try completing the step again.

Important

Even if your subnet has available IP addresses, if the subnet does not have any contiguous /28 blocks available, you will see the following error in the node events.

```
"failed to allocate a private IP/Prefix address:  
InsufficientCidrBlocks: The specified subnet does not have enough free  
cidr blocks to satisfy the request"
```

This can happen due to fragmentation of existing secondary IP addresses spread out across a subnet. To resolve this error, either create a new subnet and launch Pods there, or use an Amazon EC2 subnet CIDR reservation to reserve space within a subnet for use with prefix assignment. For more information, see [Subnet CIDR reservations](#) in the Amazon VPC User Guide.

2. (Optional) Specify additional configuration for controlling the pre-scaling and dynamic scaling behavior for your cluster. For more information, see [Configuration options with Prefix Delegation mode on Windows](#) on GitHub.

- a. Open the `amazon-vpc-cni` ConfigMap for editing.

```
kubectl edit configmap -n kube-system amazon-vpc-cni -o yaml
```

- b. Replace the *example values* with a value greater than zero and add the entries that you require to the data section of the ConfigMap. If you set a value for either `warm-ip-target` or `minimum-ip-target`, the value overrides any value set for `warm-prefix-target`.

```
warm-prefix-target: "1"  
warm-ip-target: "5"  
minimum-ip-target: "2"
```

- c. Save the file and close the editor.

3. Create Windows node groups with at least one Amazon EC2 Nitro instance type. For a list of Nitro instance types, see [Instances built on the Nitro System](#) in the Amazon Amazon EC2 User Guide for Windows Instances. By default, the maximum number of Pods that you can deploy to a node is 110. If you want to increase or decrease that number, specify the following in the user data for the bootstrap configuration. Replace `max-pods-quantity` with your max pods value.

```
-KubeletExtraArgs '--max-pods=max-pods-quantity'
```

If you're deploying managed node groups, this configuration needs to be added in the launch template. For more information, see [the section called "Customizing managed nodes with launch templates" \(p. 98\)](#). For more information about the configuration parameters for Windows bootstrap script, see [the section called "Bootstrap script configuration parameters" \(p. 186\)](#).

2. Once your nodes are deployed, view the nodes in your cluster.

```
kubectl get nodes
```

An example output is as follows.

NAME	STATUS	ROLES	AGE	VERSION
ip-192-168-22-103.region-code.compute.internal <i>eks-6b746</i>	Ready	<none>	19m	v1.XX.X-

ip-192-168-97-94.region-code.compute.internal	Ready	<none>	19m	v1.XX.X-
<i>eks-6b7464</i>				

3. Describe one of the nodes to determine the value of max-pods for the node and the number of available IP addresses. Replace **192.168.30.193** with the IPv4 address in the name of one of your nodes returned in the previous output.

```
kubectl describe node ip-192-168-30-193.region-code.compute.internal | grep 'pods\\|PrivateIPv4Address'
```

An example output is as follows.

pods:	110
vpc.amazonaws.com/PrivateIPv4Address:	144

In the previous output, 110 is the maximum number of Pods that Kubernetes will deploy to the node, even though 144 IP addresses are available.

Tutorial: Security groups for Pods

Security groups for Pods integrate Amazon EC2 security groups with Kubernetes Pods. You can use Amazon EC2 security groups to define rules that allow inbound and outbound network traffic to and from Pods that you deploy to nodes running on many Amazon EC2 instance types and Fargate. For a detailed explanation of this capability, see the [Introducing security groups for Pods](#) blog post.

Considerations

Before deploying security groups for Pods, consider the following limits and conditions:

- Security groups for Pods can't be used with Windows nodes.
- Security groups for Pods can't be used with clusters configured for the IPv6 family that contain Amazon EC2 nodes. You can however, use security groups for Pods with clusters configured for the IPv6 family that contain only Fargate nodes. For more information, see [Tutorial: Assigning IPv6 addresses to Pods and services \(p. 278\)](#).
- Security groups for Pods are supported by most [Nitro-based](#) Amazon EC2 instance families, though not by all generations of a family. For example, the m5, c5, r5, p3, m6g, c6g, and r6g instance family and generations are supported. No instance types in the t family are supported. For a complete list of supported instance types, see the [limits.go](#) file on Github. Your nodes must be one of the listed instance types that have `IsTrunkingCompatible: true` in that file.
- If you're also using Pod security policies to restrict access to Pod mutation, then the `eks:vpc-resource-controller` Kubernetes user must be specified in the Kubernetes ClusterRoleBinding for the role that your psp is assigned to. If you're using the [default Amazon EKS psp, role, and ClusterRoleBinding \(p. 522\)](#), this is the `eks:podsecuritypolicy:authenticated` ClusterRoleBinding. For example, you add the user to the `subjects:` section, as shown in the following example:

```
[...]
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: system:authenticated
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: eks:vpc-resource-controller
- kind: ServiceAccount
  name: eks-vpc-resource-controller
```

- If you're using [custom networking \(p. 306\)](#) and security groups for Pods together, the security group specified by security groups for Pods is used instead of the security group specified in the ENIconfig.
- If you're using version 1.10.2 or earlier of the Amazon VPC CNI plugin and you include the terminationGracePeriodSeconds setting in your Pod spec, the value for the setting can't be zero.
- If you're using version 1.10 or earlier of the Amazon VPC CNI plugin, or version 1.11 with POD_SECURITY_GROUP_ENFORCING_MODE=strict, which is the default setting, then Kubernetes services of type NodePort and LoadBalancer using instance targets with an externalTrafficPolicy set to Local aren't supported with Pods that you assign security groups to. For more information about using a load balancer with instance targets, see [Network load balancing on Amazon EKS \(p. 369\)](#). If you're using version 1.11 or later of the plugin with POD_SECURITY_GROUP_ENFORCING_MODE=standard, then instance targets with an externalTrafficPolicy set to Local are supported.
- If you're using version 1.10 or earlier of the Amazon VPC CNI plugin or version 1.11 with POD_SECURITY_GROUP_ENFORCING_MODE=strict, which is the default setting, source NAT is disabled for outbound traffic from Pods with assigned security groups so that outbound security group rules are applied. To access the internet, Pods with assigned security groups must be launched on nodes that are deployed in a private subnet configured with a NAT gateway or instance. Pods with assigned security groups deployed to public subnets are not able to access the internet.

If you're using version 1.11 or later of the plugin with POD_SECURITY_GROUP_ENFORCING_MODE=standard, then Pod traffic destined for outside of the VPC is translated to the IP address of the instance's primary network interface. For this traffic, the rules in the security groups for the primary network interface are used, rather than the rules in the Pod's security groups.

- To use Calico network policy with Pods that have associated security groups, you must use version 1.11.0 or later of the Amazon VPC CNI plugin and set POD_SECURITY_GROUP_ENFORCING_MODE=standard. Otherwise, traffic flow to and from Pods with associated security groups are not subjected to [Calico network policy \(p. 350\)](#) enforcement and are limited to Amazon EC2 security group enforcement only. To update your Amazon VPC CNI version, see [Working with the Amazon VPC CNI plugin for Kubernetes Amazon EKS add-on \(p. 266\)](#).
- Pods running on Amazon EC2 nodes that use security groups in clusters that use [Nodelocal DNSCache](#) are only supported with version 1.11.0 or later of the Amazon VPC CNI plugin and with POD_SECURITY_GROUP_ENFORCING_MODE=standard. To update your Amazon VPC CNI plugin version, see [Working with the Amazon VPC CNI plugin for Kubernetes Amazon EKS add-on \(p. 266\)](#).
- Security groups for Pods might lead to higher Pod startup latency for Pods with high churn. This is due to rate limiting in the resource controller.

Configure the Amazon VPC CNI plugin for Kubernetes for security groups for Pods

To deploy security groups for Pods

If you're using security groups for Fargate Pods only, and don't have any Amazon EC2 nodes in your cluster, skip to [Deploy an example application \(p. 327\)](#).

1. Check your current Amazon VPC CNI plugin for Kubernetes version with the following command:

```
kubectl describe daemonset aws-node --namespace kube-system | grep amazon-k8s-cni: |  
cut -d : -f 3
```

An example output is as follows.

```
v1.7.6
```

If your Amazon VPC CNI plugin for Kubernetes version is earlier than 1.7.7, then update the plugin to version 1.7.7 or later. For more information, see [the section called “Amazon VPC CNI plugin for Kubernetes” \(p. 266\)](#).

2. Add the [AmazonEKSVPCCResourceController](#) managed IAM policy to the [cluster role \(p. 500\)](#) that is associated with your Amazon EKS cluster. The policy allows the role to manage network interfaces, their private IP addresses, and their attachment and detachment to and from network instances.
 - a. Retrieve the name of your cluster IAM role and store it in a variable. Replace *my-cluster* with the name of your cluster.

```
cluster_role=$(aws eks describe-cluster --name my-cluster --query cluster.roleArn  
--output text | cut -d / -f 2)
```

- b. Attach the policy to the role.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/  
AmazonEKSVPCCResourceController --role-name $cluster_role
```

3. Enable the Amazon VPC CNI add-on to manage network interfaces for Pods by setting the `ENABLE_POD_ENI` variable to `true` in the `aws-node` DaemonSet. Once this setting is set to `true`, for each node in the cluster the add-on adds a label with the value `vpc.amazonaws.com/has-trunk-attached=true`. The VPC resource controller creates and attaches one special network interface called a *trunk network interface* with the description `aws-k8s-trunk-eni`.

```
kubectl set env daemonset aws-node -n kube-system ENABLE_POD_ENI=true
```

Note

The trunk network interface is included in the maximum number of network interfaces supported by the instance type. For a list of the maximum number of network interfaces supported by each instance type, see [IP addresses per network interface per instance type](#) in the *Amazon EC2 User Guide for Linux Instances*. If your node already has the maximum number of standard network interfaces attached to it then the VPC resource controller will reserve a space. You will have to scale down your running Pods enough for the controller to detach and delete a standard network interface, create the trunk network interface, and attach it to the instance.

You can see which of your nodes have `aws-k8s-trunk-eni` set to `true` with the following command. If `No resources found` is returned, then wait several seconds and try again. The previous step requires restarting the Amazon VPC CNI plugin for Kubernetes Pods, which takes several seconds.

```
kubectl get nodes -o wide -l vpc.amazonaws.com/has-trunk-attached=true
```

Once the trunk network interface is created, Pods are assigned secondary IP addresses from the trunk or standard network interfaces. The trunk interface is automatically deleted if the node is deleted.

When you deploy a security group for a Pod in a later step, the VPC resource controller creates a special network interface called a *branch network interface* with a description of `aws-k8s-branch-eni` and associates the security groups to it. Branch network interfaces are created in addition to the standard and trunk network interfaces attached to the node. If you are using liveness or readiness probes, then you also need to disable TCP early demux, so that the kubelet can connect to Pods on branch network interfaces using TCP. To disable TCP early demux, run the following command:

```
kubectl patch daemonset aws-node -n kube-system \
-p '{"spec": {"template": {"spec": {"initContainers": [{"env": [{"name": "DISABLE_TCP_EARLY_DEMUX", "value": "true"}], "name": "aws-vpc-cni-init"}]}}}}'
```

Note

If you're using 1.11.0 or later of the Amazon VPC CNI plugin for Kubernetes add-on and set `POD_SECURITY_GROUP_ENFORCING_MODE=standard`, as described in the next step, then you don't need to run the previous command.

4. If your cluster uses NodeLocal DNSCache, or you want to use Calico network policy with your Pods that have their own security groups, or you have Kubernetes services of type NodePort and LoadBalancer using instance targets with an `externalTrafficPolicy` set to Local for Pods that you want to assign security groups to, then you must be using version 1.11.0 or later of the Amazon VPC CNI plugin for Kubernetes add-on, and you must enable the following setting:

```
kubectl set env daemonset aws-node -n kube-system
POD_SECURITY_GROUP_ENFORCING_MODE=standard
```

Important

- Pod security group rules aren't applied to traffic between Pods or between Pods and services, such as `kubelet` or `nodeLocalDNS`, that are on the same node. Pods using different security groups on the same node can't communicate because they are configured in different subnets, and routing is disabled between these subnets.
- Outbound traffic from Pods to addresses outside of the VPC is network address translated to the IP address of the instance's primary network interface (unless you've also set `AWS_VPC_K8S_CNI_EXTERNALSNAT=true`). For this traffic, the rules in the security groups for the primary network interface are used, rather than the rules in the Pod's security groups.
- For this setting to apply to existing Pods, you must restart the Pods or the nodes that the Pods are running on.

Deploy an example application

To use security groups for Pods, you must have an existing security group and [Deploy an Amazon EKS SecurityGroupPolicy \(p. 327\)](#) to your cluster, as described in the following procedure. The following steps show you how to use the security group policy for a Pod. Unless otherwise noted, complete all steps from the same terminal because variables are used in the following steps that don't persist across terminals.

To deploy an example Pod with a security group

1. Create a Kubernetes namespace to deploy resources to. You can replace `my-namespace` with the name of a namespace that you want to use.

```
kubectl create namespace my-namespace
```

2. Deploy an Amazon EKS SecurityGroupPolicy to your cluster.
 - a. Copy the following contents to your device. You can replace `podSelector` with `serviceAccountSelector` if you'd rather select Pods based on service account labels. You must specify one selector or the other. An empty podSelector (example: `podSelector: []`) selects all Pods in the namespace. You can change `my-role` to the name of your role. An empty serviceAccountSelector selects all service accounts in the namespace. You can replace `my-`

security-group-policy with a name for your SecurityGroupPolicy and *my-namespace* with the namespace that you want to create the SecurityGroupPolicy in.

You must replace *my_pod_security_group_id* with the ID of an existing security group. If you don't have an existing security group, then you must create one. For more information, see [Amazon EC2 security groups for Linux instances](#) in the [Amazon EC2 User Guide for Linux Instances](#). You can specify 1-5 security group IDs. If you specify more than one ID, then the combination of all the rules in all the security groups are effective for the selected Pods.

```
cat >my-security-group-policy.yaml <<EOF
apiVersion: vpcresources.k8s.aws/v1beta1
kind: SecurityGroupPolicy
metadata:
  name: my-security-group-policy
  namespace: my-namespace
spec:
  podSelector:
    matchLabels:
      role: my-role
  securityGroups:
    groupIds:
      - my_pod_security_group_id
EOF
```

Important

The security group or groups that you specify for your Pods must meet the following criteria:

- They must exist. If they don't exist, then, when you deploy a Pod that matches the selector, your Pod remains stuck in the creation process. If you describe the Pod, you'll see an error message similar to the following one: An `error occurred (InvalidSecurityGroupID.NotFound) when calling the CreateNetworkInterface operation: The securityGroup ID 'sg-05b1d815d1EXAMPLE' does not exist.`
- They must allow inbound communication from the security group applied to your nodes (for kubelet) over any ports that you've configured probes for.
- They must allow outbound communication over TCP and UDP ports 53 to a security group assigned to the Pods (or nodes that the Pods run on) running CoreDNS. The security group for your CoreDNS Pods must allow inbound TCP and UDP port 53 traffic from the security group that you specify.
- They must have necessary inbound and outbound rules to communicate with other Pods that they need to communicate with.
- They must have rules that allow the Pods to communicate with the Kubernetes control plane if you're using the security group with Fargate. The easiest way to do this is to specify the cluster security group as one of the security groups.

Security group policies only apply to newly scheduled Pods. They do not affect running Pods.

- b. Deploy the policy.

```
kubectl apply -f my-security-group-policy.yaml
```

3. Deploy a sample application with a label that matches the *my-role* value for *podSelector* that you specified in a previous step.

- a. Copy the following contents to your device. Replace the *example values* with your own and then run the modified command. If you replace *my-role*, make sure that it's the same as the value you specified for the selector in a previous step.

```
cat >sample-application.yaml <<EOF
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-deployment
  namespace: my-namespace
  labels:
    app: my-app
spec:
  replicas: 4
  selector:
    matchLabels:
      app: my-app
  template:
    metadata:
      labels:
        app: my-app
        role: my-role
    spec:
      terminationGracePeriodSeconds: 120
      containers:
        - name: nginx
          image: public.ecr.aws/nginx/nginx:1.23
          ports:
            - containerPort: 80
---
apiVersion: v1
kind: Service
metadata:
  name: my-app
  namespace: my-namespace
  labels:
    app: my-app
spec:
  selector:
    app: my-app
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
EOF
```

- b. Deploy the application with the following command. When you deploy the application, the Amazon VPC CNI plugin for Kubernetes matches the `role` label and the security groups that you specified in the previous step are applied to the Pod.

```
kubectl apply -f sample-application.yaml
```

4. View the Pods deployed with the sample application. For the remainder of this topic, this terminal is referred to as TerminalA.

```
kubectl get pods -n my-namespace -o wide
```

An example output is as follows.

NAME NODE	READY	STATUS	RESTARTS	AGE	IP NOMINATED NODE	READINESS	GATES
--------------	-------	--------	----------	-----	----------------------	-----------	-------

my-deployment-5df6f7687b-4fbjm	1/1	Running	0	7m51s	192.168.53.48
ip-192-168-33-28.region-code.compute.internal	<none>			<none>	
my-deployment-5df6f7687b-j9fl4	1/1	Running	0	7m51s	192.168.70.145
ip-192-168-92-33.region-code.compute.internal	<none>			<none>	
my-deployment-5df6f7687b-rjxcz	1/1	Running	0	7m51s	192.168.73.207
ip-192-168-92-33.region-code.compute.internal	<none>			<none>	
my-deployment-5df6f7687b-zmb42	1/1	Running	0	7m51s	192.168.63.27
ip-192-168-33-28.region-code.compute.internal	<none>			<none>	

Note

- If any Pods are stuck in the Waiting state, then run `kubectl describe pod my-deployment-xxxxxxxxxx-xxxx -n my-namespace`. If you see Insufficient permissions: Unable to create Elastic Network Interface., confirm that you added the IAM policy to the IAM cluster role in a previous step.
- If any Pods are stuck in the Pending state, confirm that your node instance type is listed in [limits.go](#) and that the product of the maximum number of branch network interfaces supported by the instance type multiplied times the number of nodes in your node group hasn't already been met. For example, an m5.large instance supports nine branch network interfaces. If your node group has five nodes, then a maximum of 45 branch network interfaces can be created for the node group. The 46th Pod that you attempt to deploy will sit in Pending state until another Pod that has associated security groups is deleted.

If you run `kubectl describe pod my-deployment-xxxxxxxxxx-xxxx -n my-namespace` and see a message similar to the following message, then it can be safely ignored. This message might appear when the Amazon VPC CNI plugin for Kubernetes tries to set up host networking and fails while the network interface is being created. The plugin logs this event until the network interface is created.

```
Failed to create Pod sandbox: rpc error: code = Unknown desc = failed to set up sandbox container "e24268322e55c8185721f52df6493684f6c2c3bf4fd59c9c121fd4cdc894579f" network for Pod "my-deployment-5df6f7687b-4fbjm": networkPlugin cni failed to set up Pod "my-deployment-5df6f7687b-4fbjm-c89wx_my-namespace" network: add cmd: failed to assign an IP address to container
```

You can't exceed the maximum number of Pods that can be run on the instance type. For a list of the maximum number of Pods that you can run on each instance type, see [eni-max-pods.txt](#) on GitHub. When you delete a Pod that has associated security groups, or delete the node that the Pod is running on, the VPC resource controller deletes the branch network interface. If you delete a cluster with Pods using Pods for security groups, then the controller doesn't delete the branch network interfaces, so you'll need to delete them yourself. For information about how to delete network interfaces, see [Delete a network interface](#) in the Amazon EC2 User Guide for Linux Instances.

- In a separate terminal, shell into one of the Pods. For the remainder of this topic, this terminal is referred to as TerminalB. Replace **5df6f7687b-4fbjm** with the ID of one of the Pods returned in your output from the previous step.

```
kubectl exec -it -n my-namespace my-deployment-5df6f7687b-4fbjm -- /bin/bash
```

- From the shell in TerminalB, confirm that the sample application works.

```
curl my-app
```

An example output is as follows.

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
[...]
```

You received the output because all Pods running the application are associated with the security group that you created. That group contains a rule that allows all traffic between all Pods that the security group is associated to. DNS traffic is allowed outbound from that security group to the cluster security group, which is associated with your nodes. The nodes are running the CoreDNS Pods, which your Pods did a name lookup to.

7. From TerminalA, remove the security group rules that allow DNS communication to the cluster security group from your security group. If you didn't add the DNS rules to the cluster security group in a previous step, then replace `$my_cluster_security_group_id` with the ID of the security group that you created the rules in.

```
aws ec2 revoke-security-group-ingress --group-id $my_cluster_security_group_id --
security-group-rule-ids $my_tcp_rule_id
aws ec2 revoke-security-group-ingress --group-id $my_cluster_security_group_id --
security-group-rule-ids $my_udp_rule_id
```

8. From TerminalB, attempt to access the application again.

```
curl my-app
```

An example output is as follows.

```
curl: (6) Could not resolve host: my-app
```

The attempt fails because the Pod is no longer able to access the CoreDNS Pods, which have the cluster security group associated to them. The cluster security group no longer has the security group rules that allow DNS communication from the security group associated to your Pod.

If you attempt to access the application using the IP addresses returned for one of the Pods in a previous step, you still receive a response because all ports are allowed between Pods that have the security group associated to them and a name lookup isn't required.

9. Once you've finished experimenting, you can remove the sample security group policy, application, and security group that you created. Run the following commands from TerminalA.

```
kubectl delete namespace my-namespace
aws ec2 revoke-security-group-ingress --group-id $my_pod_security_group_id --security-
group-rule-ids $my_inbound_self_rule_id
wait
sleep 45s
aws ec2 delete-security-group --group-id $my_pod_security_group_id
```

Multiple network interfaces for Pods

Multus CNI is a container network interface (CNI) plugin for Amazon EKS that enables attaching multiple network interfaces to a Pod. For more information, see the [Multus-CNI](#) documentation on GitHub.

In Amazon EKS, each Pod has one network interface assigned by the Amazon VPC CNI plugin. With Multus, you can create a multi-homed Pod that has multiple interfaces. This is accomplished by Multus

acting as a "meta-plugin"; a CNI plugin that can call multiple other CNI plugins. AWS support for Multus comes configured with the Amazon VPC CNI plugin as the default delegate plugin.

Considerations

- Amazon EKS won't be building and publishing single root I/O virtualization (SR-IOV) and Data Plane Development Kit (DPDK) CNI plugins. However, you can achieve packet acceleration by connecting directly to Amazon EC2 Elastic Network Adapters (ENA) through Multus managed host-device and `ipvlan` plugins.
- Amazon EKS is supporting Multus, which provides a generic process that enables simple chaining of additional CNI plugins. Multus and the process of chaining is supported, but AWS won't provide support for all compatible CNI plugins that can be chained, or issues that may arise in those CNI plugins that are unrelated to the chaining configuration.
- Amazon EKS is providing support and life cycle management for the Multus plugin, but isn't responsible for any IP address or additional management associated with the additional network interfaces. The IP address and management of the default network interface utilizing the Amazon VPC CNI plugin remains unchanged.
- Only the Amazon VPC CNI plugin is officially supported as the default delegate plugin. You need to modify the published Multus installation manifest to reconfigure the default delegate plugin to an alternate CNI if you choose not to use the Amazon VPC CNI plugin for primary networking.
- Multus is only supported when using the Amazon VPC CNI as the primary CNI. We do not support the Amazon VPC CNI when used for higher order interfaces, secondary or otherwise.
- To prevent the Amazon VPC CNI plugin from trying to manage additional network interfaces assigned to Pods, add the following tag to the network interface:

key: node.k8s.amazonaws.com/no_manage

value: true

- Multus is compatible with network policies, but the policy has to be enriched to include ports and IP addresses that may be part of additional network interfaces attached to Pods.

For an implementation walk through, see the [Multus Setup Guide](#) on GitHub.

Alternate compatible CNI plugins

The [Amazon VPC CNI plugin for Kubernetes](#) is the only CNI plugin supported by Amazon EKS. Amazon EKS runs upstream Kubernetes, so you can install alternate compatible CNI plugins to Amazon EC2 nodes in your cluster. If you have Fargate nodes in your cluster, the Amazon VPC CNI plugin for Kubernetes is already on your Fargate nodes. It's the only CNI plugin you can use with Fargate nodes. An attempt to install an alternate CNI plugin on Fargate nodes fails.

If you plan to use an alternate CNI plugin on Amazon EC2 nodes, we recommend that you obtain commercial support for the plugin or have the in-house expertise to troubleshoot and contribute fixes to the CNI plugin project.

Amazon EKS maintains relationships with a network of partners that offer support for alternate compatible CNI plugins. For details about the versions, qualifications, and testing performed, see the following partner documentation.

Partner	Product	Documentation
Tigera	Calico	Installation instructions
Isovalent	Cilium	Installation instructions

Partner	Product	Documentation
Juniper	Cloud-Native Contrail Networking (CN2)	Installation instructions
Weaveworks	Weave Net	Installation instructions
VMware	Antrea	Installation instructions

Amazon EKS aims to give you a wide selection of options to cover all use cases. If you develop a commercially supported Kubernetes CNI plugin not listed here, contact our partner team at aws-container-partners@amazon.com for more information.

Installing the AWS Load Balancer Controller add-on

Important

In versions 2.5 and newer, the AWS Load Balancer Controller becomes the default controller for Kubernetes *service* resources with the type: `LoadBalancer` and makes an AWS Network Load Balancer (NLB) for each service. It does this by making a mutating webhook for services, which sets the `spec.loadBalancerClass` field to `service.k8s.aws/nlb` for new services of type: `LoadBalancer`. You can turn off this feature and revert to using the [legacy Cloud Provider](#) as the default controller, by setting the helm chart value `enableServiceMutatorWebhook` to `false`. The cluster won't provision new Classic Load Balancers for your services unless you turn off this feature. Existing Classic Load Balancers will continue to work.

The AWS Load Balancer Controller manages AWS Elastic Load Balancers for a Kubernetes cluster. The controller provisions the following resources:

Kubernetes Ingress

The AWS Load Balancer Controller creates an AWS Application Load Balancer (ALB) when you create a Kubernetes Ingress.

Kubernetes service of the `LoadBalancer` type

The AWS Load Balancer Controller creates an AWS Network Load Balancer (NLB) when you create a Kubernetes service of type `LoadBalancer`. In the past, the Kubernetes network load balancer was used for *instance* targets, but the AWS Load balancer Controller was used for *IP* targets. With the AWS Load Balancer Controller version 2.3.0 or later, you can create NLBs using either target type. For more information about NLB target types, see [Target type](#) in the User Guide for Network Load Balancers.

The AWS Load Balancer Controller was formerly named the *AWS ALB Ingress Controller*. It's an [open-source project](#) managed on GitHub.

This topic describes how to install the controller using default options. You can view the full [documentation](#) for the controller on GitHub. Before deploying the controller, we recommend that you review the prerequisites and considerations in [Application load balancing on Amazon EKS \(p. 375\)](#) and [Network load balancing on Amazon EKS \(p. 369\)](#). Those topics also include steps on how to deploy a sample application that require the AWS Load Balancer Controller to provision AWS Application Load Balancers and Network Load Balancers.

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Getting started with Amazon EKS \(p. 6\)](#).

- An existing AWS Identity and Access Management (IAM) OpenID Connect (OIDC) provider for your cluster. To determine whether you already have one, or to create one, see [Creating an IAM OIDC provider for your cluster \(p. 465\)](#).
- Make sure that your Amazon VPC CNI plugin for Kubernetes, kube-proxy, and CoreDNS add-ons are at the minimum versions listed in [Service account tokens \(p. 463\)](#).
- Familiarity with AWS Elastic Load Balancing. For more information, see the [Elastic Load Balancing User Guide](#).
- Familiarity with Kubernetes [service](#) and [ingress](#) resources.

To deploy the AWS Load Balancer Controller to an Amazon EKS cluster

In the following steps, replace the *example values* with your own values.

1. Create an IAM policy.

- a. Download an IAM policy for the AWS Load Balancer Controller that allows it to make calls to AWS APIs on your behalf.
 - AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions

```
$ curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.5.4/docs/install/iam_policy_us-gov.json
```

- All other AWS Regions

```
$ curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.5.4/docs/install/iam_policy.json
```

- b. Create an IAM policy using the policy downloaded in the previous step. If you downloaded `iam_policy_us-gov.json`, change `iam_policy.json` to `iam_policy_us-gov.json` before running the command.

```
$ aws iam create-policy \
--policy-name AWSLoadBalancerControllerIAMPolicy \
--policy-document file://iam_policy.json
```

Note

If you view the policy in the AWS Management Console, the console shows warnings for the **ELB** service, but not for the **ELB v2** service. This happens because some of the actions in the policy exist for **ELB v2**, but not for **ELB**. You can ignore the warnings for **ELB**.

2. Create an IAM role. Create a Kubernetes service account named `aws-load-balancer-controller` in the `kube-system` namespace for the AWS Load Balancer Controller and annotate the Kubernetes service account with the name of the IAM role.

You can use `eksctl` or the AWS CLI and `kubectl` to create the IAM role and Kubernetes service account.

`eksctl`

Replace `my-cluster` with the name of your cluster, `111122223333` with your account ID, and then run the command. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

```
$ eksctl create iamserviceaccount \
--cluster=my-cluster \
```

```
--namespace=kube-system \
--name=aws-load-balancer-controller \
--role-name AmazonEKSLoadBalancerControllerRole \
--attach-policy-arn=arn:aws:iam::111122223333:policy/AWSLoadBalancerControllerIAMPolicy \
--approve
```

AWS CLI and kubectl

Using the AWS CLI and kubectl

- Retrieve your cluster's OIDC provider ID and store it in a variable.

```
oidc_id=$(aws eks describe-cluster --name my-cluster --query "cluster.identity.oidc.issuer" --output text | cut -d '/' -f 5)
```

- Determine whether an IAM OIDC provider with your cluster's ID is already in your account.

```
aws iam list-open-id-connect-providers | grep $oidc_id | cut -d "/" -f4
```

If output is returned, then you already have an IAM OIDC provider for your cluster. If no output is returned, then you must create an IAM OIDC provider for your cluster. For more information, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#).

- Copy the following contents to your device. Replace **111122223333** with your account ID. Replace **region-code** with the AWS Region that your cluster is in. Replace **EXAMPLED539D4633E53DE1B71EXAMPLE** with the output returned in the previous step. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`. After replacing the text, run the modified command to create the `load-balancer-role-trust-policy.json` file.

```
cat >load-balancer-role-trust-policy.json <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::111122223333:oidc-provider/
oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringEquals": {
                    "oidc.eks.region-code.amazonaws.com/
id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com",
                    "oidc.eks.region-code.amazonaws.com/
id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:kube-system:aws-
load-balancer-controller"
                }
            }
        }
    ]
}
EOF
```

- Create the IAM role.

```
aws iam create-role \
--role-name AmazonEKSLoadBalancerControllerRole \
```

```
--assume-role-policy-document file://"load-balancer-role-trust-policy.json"
```

- e. Attach the required Amazon EKS managed IAM policy to the IAM role. Replace **111122223333** with your account ID.

```
aws iam attach-role-policy \
--policy-arn
arn:aws:iam::111122223333:policy/AWSLoadBalancerControllerIAMPolicy \
--role-name AmazonEKSLoadBalancerControllerRole
```

- f. Copy the following contents to your device. Replace **111122223333** with your account ID. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace arn:aws: with arn:aws-us-gov:. After replacing the text, run the modified command to create the aws-load-balancer-controller-service-account.yaml file.

```
cat >aws-load-balancer-controller-service-account.yaml <<EOF
apiVersion: v1
kind: ServiceAccount
metadata:
  labels:
    app.kubernetes.io/component: controller
    app.kubernetes.io/name: aws-load-balancer-controller
  name: aws-load-balancer-controller
  namespace: kube-system
  annotations:
    eks.amazonaws.com/role-arn:
      arn:aws:iam::111122223333:role/AmazonEKSLoadBalancerControllerRole
EOF
```

- g. Create the Kubernetes service account on your cluster. The Kubernetes service account named aws-load-balancer-controller is annotated with the IAM role that you created named **AmazonEKSLoadBalancerControllerRole**.

```
$ kubectl apply -f aws-load-balancer-controller-service-account.yaml
```

3. (Optional) Configure the AWS Security Token Service endpoint type used by your Kubernetes service account. For more information, see [Configuring the AWS Security Token Service endpoint for a service account \(p. 474\)](#).
4. If you don't currently have the AWS ALB Ingress Controller for Kubernetes installed, or don't currently have the 0.1.x version of the AWS Load Balancer Controller installed with Helm, then skip to the next step.

Uninstall the AWS ALB Ingress Controller or 0.1.x version of the AWS Load Balancer Controller (only if installed with Helm). Complete the procedure using the tool that you originally installed it with. The AWS Load Balancer Controller replaces the functionality of the AWS ALB Ingress Controller for Kubernetes.

Helm

- a. If you installed the incubator/aws-alb-ingress-controller Helm chart, uninstall it.

```
$ helm delete aws-alb-ingress-controller -n kube-system
```

- b. If you have version 0.1.x of the eks-charts/aws-load-balancer-controller chart installed, uninstall it. The upgrade from 0.1.x to version 1.0.0 doesn't work due to incompatibility with the webhook API version.

```
$ helm delete aws-load-balancer-controller -n kube-system
```

Kubernetes manifest

- a. Check to see if the controller is currently installed.

```
$ kubectl get deployment -n kube-system alb-ingress-controller
```

This is the output if the controller isn't installed. Skip to the [install controller \(p. 338\)](#) step.

Error from server (NotFound): deployments.apps "alb-ingress-controller" not found

This is the output if the controller is installed.

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
alb-ingress-controller	1/1	1	1	122d

- b. Enter the following commands to remove the controller.

```
$ kubectl delete -f https://raw.githubusercontent.com/kubernetes-sigs/aws-alb-ingress-controller/v1.1.8/docs/examples/alb-ingress-controller.yaml  
kubectl delete -f https://raw.githubusercontent.com/kubernetes-sigs/aws-alb-ingress-controller/v1.1.8/docs/examples/rbac-role.yaml
```

- c. Add the following IAM policy to the IAM role created in a [previous step \(p. 334\)](#). The policy allows the AWS Load Balancer Controller access to the resources that were created by the ALB Ingress Controller for Kubernetes.

1. Download the IAM policy. You can also [view the policy](#).

```
$ curl -o https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.5.4/docs/install/iam_policy_v1_to_v2_additional.json
```

2. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`

```
$ sed -i.bak -e 's|arn:aws:|arn:aws-us-gov:|'  
iam_policy_v1_to_v2_additional.json
```

3. Create the IAM policy and note the ARN that is returned.

```
$ aws iam create-policy \  
--policy-name AWSLoadBalancerControllerAdditionalIAMPolicy \  
--policy-document file://iam_policy_v1_to_v2_additional.json
```

4. Attach the IAM policy to the IAM role that you created in a [previous step \(p. 334\)](#). Replace `your-role-name` with the name of the role. If you created the role using `eksctl`, then to find the role name that was created, open the [AWS CloudFormation console](#) and select the `eksctl-my-cluster-addon-iamserviceaccount-kube-system-aws-load-balancer-controller` stack. Select the **Resources** tab. The role name is in the **Physical ID** column. If you used the AWS Management Console to create the role, then the role name is whatever you named it, such as `AmazonEKSLoadBalancerControllerRole`. If your cluster is in the AWS GovCloud (US-East) or AWS GovCloud (US-West) AWS Regions, then replace `arn:aws:` with `arn:aws-us-gov:`.

```
$ aws iam attach-role-policy \  
--role-name your-role-name \  
--policy-arn arn:aws:iam::aws:policy/AWSLoadBalancerControllerAdditionalIAMPolicy
```

```
--policy-arn
arn:aws:iam::111122223333:policy/AWSLoadBalancerControllerAdditionalIAMPolicy
```

5. Install the AWS Load Balancer Controller using [Helm V3 \(p. 450\)](#) or later or by applying a Kubernetes manifest. If you want to deploy the controller on Fargate, use the Helm procedure. The Helm procedure doesn't depend on cert-manager because it generates a self-signed certificate.

Helm

- a. Add the eks-charts repository.

```
$ helm repo add eks https://aws.github.io/eks-charts
```

- b. Update your local repo to make sure that you have the most recent charts.

```
$ helm repo update eks
```

- c. If your nodes don't have access to the Amazon ECR Public image repository, then you need to pull the following container image and push it to a repository that your nodes have access to. For more information on how to pull, tag, and push an image to your own repository, see [Copy a container image from one repository to another repository \(p. 381\)](#).

```
public.ecr.aws/eks/aws-load-balancer-controller:v2.5.4
```

- d. Install the AWS Load Balancer Controller. If you're deploying the controller to Amazon EC2 nodes that have [restricted access to the Amazon EC2 instance metadata service \(IMDS\)](#), or if you're deploying to Fargate, then add the following flags to the helm command that follows:

- **--set region=region-code**
- **--set vpcId=vpc-xxxxxxxx**

Replace **my-cluster** with the name of your cluster. In the following command, aws-load-balancer-controller is the Kubernetes service account that you created in a previous step.

```
$ helm install aws-load-balancer-controller eks/aws-load-balancer-controller \
-n kube-system \
--set clusterName=my-cluster \
--set serviceAccount.create=false \
--set serviceAccount.name=aws-load-balancer-controller
```

Important

The deployed chart doesn't receive security updates automatically. You need to manually upgrade to a newer chart when it becomes available. When upgrading, change **install** to **upgrade** in the previous command, but run the following command to install the TargetGroupBinding custom resource definitions before running the previous command.

```
$ kubectl apply -k "github.com/awslabs/eks-charts/stable/aws-load-balancer-
controller/crds?ref=master"
```

Kubernetes manifest

- a. Install cert-manager using one of the following methods to inject certificate configuration into the webhooks. For more information, see [Getting Started](#) on the *cert-manager Documentation*.

- If your nodes have access to the quay.io container registry, install cert-manager to inject certificate configuration into the webhooks.

```
$ kubectl apply \
--validate=false \
-f https://github.com/jetstack/cert-manager/releases/download/v1.12.3/cert-
manager.yaml
```

- If your nodes don't have access to the quay.io container registry, then complete the following tasks:

- i. Download the manifest.

```
curl -Lo cert-manager.yaml https://github.com/jetstack/cert-manager/releases/
download/v1.12.3/cert-manager.yaml
```

- ii. Pull the following images and push them to a repository that your nodes have access to. For more information on how to pull, tag, and push the images to your own repository, see [Copy a container image from one repository to another repository \(p. 381\)](#).

```
quay.io/jetstack/cert-manager-cainjector:v1.12.3
quay.io/jetstack/cert-manager-controller:v1.12.3
quay.io/jetstack/cert-manager-webhook:v1.12.3
```

- iii. Replace quay.io in the manifest for the three images with your own registry name.

The following command assumes that your private repository's name is the same as the source repository. Replace *111122223333.dkr.ecr.region-code.amazonaws.com* with your private registry.

```
$ sed -i.bak -e 's|quay.io|111122223333.dkr.ecr.region-
code.amazonaws.com|' ./cert-manager.yaml
```

- iv. Apply the manifest.

```
$ kubectl apply \
--validate=false \
-f ./cert-manager.yaml
```

- b. Install the controller.

- i. Download the controller specification. For more information about the controller, see the [documentation](#) on GitHub.

```
curl -Lo v2_5_4_full.yaml https://github.com/kubernetes-sigs/aws-load-balancer-
controller/releases/download/v2.5.4/v2_5_4_full.yaml
```

- ii. Make the following edits to the file.

- If you downloaded the v2_5_4_full.yaml file, run the following command to remove the ServiceAccount section in the manifest. If you don't remove this section, the required annotation that you made to the service account in a previous step is overwritten. Removing this section also preserves the service account that you created in a previous step if you delete the controller.

```
$ sed -i.bak -e '596,604d' ./v2_5_4_full.yaml
```

If you downloaded a different file version, then open the file in an editor and remove the following lines.

```
apiVersion: v1
kind: ServiceAccount
metadata:
  labels:
    app.kubernetes.io/component: controller
    app.kubernetes.io/name: aws-load-balancer-controller
  name: aws-load-balancer-controller
  namespace: kube-system
---
```

- Replace `your-cluster-name` in the Deployment spec section of the file with the name of your cluster by replacing `my-cluster` with the name of your cluster.

```
$ sed -i.bak -e 's|your-cluster-name|my-cluster|' ./v2_5_4_full.yaml
```

- If your nodes don't have access to the Amazon EKS Amazon ECR image repositories, then you need to pull the following image and push it to a repository that your nodes have access to. For more information on how to pull, tag, and push an image to your own repository, see [Copy a container image from one repository to another repository \(p. 381\)](#).

```
public.ecr.aws/eks/aws-load-balancer-controller:v2.5.4
```

Add your registry's name to the manifest. The following command assumes that your private repository's name is the same as the source repository and adds your private registry's name to the file. Replace `11122223333.dkr.ecr.region-code.amazonaws.com` with your registry. This line assumes that you named your private repository the same as the source repository. If not, change the `eks/aws-load-balancer-controller` text after your private registry name to your repository name.

```
$ sed -i.bak -e 's|public.ecr.aws/eks/aws-load-balancer-controller|11122223333.dkr.ecr.region-code.amazonaws.com/eks/aws-load-balancer-controller|' ./v2_5_4_full.yaml
```

- If you're deploying the controller to Amazon EC2 nodes that have [restricted access to the Amazon EC2 instance metadata service \(IMDS\)](#), or if you're deploying to Fargate, then add the **following parameters** under `- args:`

```
[...]
spec:
  containers:
    - args:
        - --cluster-name=your-cluster-name
        - --ingress-class=alb
        - --aws-vpc-id=vpc-xxxxxxxx
        - --aws-region=region-code
[...]
```

- Apply the file.

```
$ kubectl apply -f v2_5_4_full.yaml
```

- Download the `IngressClass` and `IngressClassParams` manifest to your cluster.

```
$ curl -Lo v2_5_4_ingclass.yaml https://github.com/kubernetes-sigs/aws-load-balancer-controller/releases/download/v2.5.4/v2_5_4_ingclass.yaml
```

- v. Apply the manifest to your cluster.

```
$ kubectl apply -f v2_5_4_ingclass.yaml
```

6. Verify that the controller is installed.

```
$ kubectl get deployment -n kube-system aws-load-balancer-controller
```

An example output is as follows.

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
aws-load-balancer-controller	2/2	2	2	84s

You receive the previous output if you deployed using Helm. If you deployed using the Kubernetes manifest, you only have one replica.

7. Before using the controller to provision AWS resources, your cluster must meet specific requirements. For more information, see [Application load balancing on Amazon EKS \(p. 375\)](#) and [Network load balancing on Amazon EKS \(p. 369\)](#).

Working with the CoreDNS Amazon EKS add-on

CoreDNS is a flexible, extensible DNS server that can serve as the Kubernetes cluster DNS. When you launch an Amazon EKS cluster with at least one node, two replicas of the CoreDNS image are deployed by default, regardless of the number of nodes deployed in your cluster. The CoreDNS Pods provide name resolution for all Pods in the cluster. The CoreDNS Pods can be deployed to Fargate nodes if your cluster includes an [AWS Fargate profile \(p. 136\)](#) with a namespace that matches the namespace for the CoreDNS deployment. For more information about CoreDNS, see [Using CoreDNS for Service Discovery](#) in the Kubernetes documentation.

The following table lists the latest version of the Amazon EKS add-on type for each Kubernetes version.

Kubernetes version	1.28	1.27	1.26	1.25	1.24	1.23
	v1.10.1-eksbuild.4eksbuild.4	v1.10.1-eksbuild.4eksbuild.4	v1.9.3-eksbuild.7eksbuild.7	v1.9.3-eksbuild.7eksbuild.7	v1.9.3-eksbuild.7eksbuild.7	v1.8.7-eksbuild.7eksbuild.7

Important

- If you're self-managing this add-on, the versions in the table might not be the same as the available self-managed versions. For more information about updating the self-managed type of this add-on, see [the section called "Updating the self-managed add-on" \(p. 345\)](#).
- To improve the stability and availability of the CoreDNS Deployment, versions v1.9.3-eksbuild.5 and later and v1.10.1-eksbuild.2 are deployed with a PodDisruptionBudget. If you've deployed an existing PodDisruptionBudget, your upgrade to these versions might fail. If the upgrade fails, completing one of the following tasks should resolve the issue:
 - When doing the upgrade of the Amazon EKS add-on, choose to override the existing settings as your conflict resolution option. If you've made other custom settings to the

Deployment, make sure to back up your settings before upgrading so that you can reapply your other custom settings after the upgrade.

- Remove your existing PodDisruptionBudget and try the upgrade again.
- In EKS add-on versions v1.9.3-eksbuild.6 and later and v1.10.1-eksbuild.6 and later, the CoreDNS Deployment sets the readinessProbe to use the /ready endpoint. This endpoint is enabled in the Corefile configuration file for CoreDNS.

If you use a custom Corefile, you must add the ready plugin to the config, so that the /ready endpoint is active in CoreDNS for the probe to use.

- In EKS add-on versions v1.9.3-eksbuild.7 and later and v1.10.1-eksbuild.4 and later, you can change the PodDisruptionBudget. You can edit the add-on and change these settings in the **Optional configuration settings** using the fields in the following example. This example shows the default PodDisruptionBudget.

```
{  
  "podDisruptionBudget": {  
    "enabled": true,  
    "maxUnavailable": 1  
  }  
}
```

You can set maxUnavailable or minAvailable, but you can't set both in a single PodDisruptionBudget. For more information about PodDisruptionBudgets, see [Specifying a PodDisruptionBudget](#) in the *Kubernetes documentation*.

Note that if you set enabled to false, the PodDisruptionBudget isn't removed. After you set this field to false, you must delete the PodDisruptionBudget object. Similarly, if you edit the add-on to use an older version of the add-on (downgrade the add-on) after upgrading to a version with a PodDisruptionBudget, the PodDisruptionBudget isn't removed. To delete the PodDisruptionBudget, you can run the following command:

```
kubectl delete poddisruptionbudget coredns -n kube-system
```

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Getting started with Amazon EKS \(p. 6\)](#).

Creating the Amazon EKS add-on

Create the Amazon EKS type of the add-on.

1. See which version of the add-on is installed on your cluster.

```
kubectl describe deployment coredns --namespace kube-system | grep coredns: | cut -d : -f 3
```

An example output is as follows.

```
v1.9.3-eksbuild.7
```

2. See which type of the add-on is installed on your cluster. Depending on the tool that you created your cluster with, you might not currently have the Amazon EKS add-on type installed on your cluster. Replace *my-cluster* with the name of your cluster.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns --query
addon.addonVersion --output text
```

If a version number is returned, you have the Amazon EKS type of the add-on installed on your cluster and don't need to complete the remaining steps in this procedure. If an error is returned, you don't have the Amazon EKS type of the add-on installed on your cluster. Complete the remaining steps of this procedure to install it.

3. Save the configuration of your currently installed add-on.

```
kubectl get deployment coredns -n kube-system -o yaml > aws-k8s-coredns-old.yaml
```

4. Create the add-on using the AWS CLI. If you want to use the AWS Management Console or eksctl to create the add-on, see [the section called "Creating an add-on" \(p. 393\)](#) and specify coredns for the add-on name. Copy the command that follows to your device. Make the following modifications to the command, as needed, and then run the modified command.
 - Replace *my-cluster* with the name of your cluster.
 - Replace *v1.10.1-eksbuild.4* with the latest version listed in the [latest version table \(p. 341\)](#) for your cluster version.

```
aws eks create-addon --cluster-name my-cluster --addon-name coredns --addon-
version v1.10.1-eksbuild.4
```

If you've applied custom settings to your current add-on that conflict with the default settings of the Amazon EKS add-on, creation might fail. If creation fails, you receive an error that can help you resolve the issue. Alternatively, you can add **--resolve-conflicts OVERWRITE** to the previous command. This allows the add-on to overwrite any existing custom settings. Once you've created the add-on, you can update it with your custom settings.

5. Confirm that the latest version of the add-on for your cluster's Kubernetes version was added to your cluster. Replace *my-cluster* with the name of your cluster.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns --query
addon.addonVersion --output text
```

It might take several seconds for add-on creation to complete.

An example output is as follows.

```
v1.10.1-eksbuild.4
```

6. If you made custom settings to your original add-on, before you created the Amazon EKS add-on, use the configuration that you saved in a previous step to [update \(p. 343\)](#) the Amazon EKS add-on with your custom settings.

Updating the Amazon EKS add-on

Update the Amazon EKS type of the add-on. If you haven't added the Amazon EKS type of the add-on to your cluster, either [add it \(p. 342\)](#) or see [the section called "Updating the self-managed add-on" \(p. 345\)](#), instead of completing this procedure.

1. See which version of the add-on is installed on your cluster. Replace *my-cluster* with your cluster name.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns --query "addon.addonVersion" --output text
```

An example output is as follows.

```
v1.9.3-eksbuild.7
```

If the version returned is the same as the version for your cluster's Kubernetes version in the [latest version table \(p. 341\)](#), then you already have the latest version installed on your cluster and don't need to complete the rest of this procedure. If you receive an error, instead of a version number in your output, then you don't have the Amazon EKS type of the add-on installed on your cluster. You need to [create the add-on \(p. 342\)](#) before you can update it with this procedure.

2. Save the configuration of your currently installed add-on.

```
kubectl get deployment coredns -n kube-system -o yaml > aws-k8s-coredns-old.yaml
```

3. Update your add-on using the AWS CLI. If you want to use the AWS Management Console or eksctl to update the add-on, see [the section called "Updating an add-on" \(p. 400\)](#). Copy the command that follows to your device. Make the following modifications to the command, as needed, and then run the modified command.
 - Replace *my-cluster* with the name of your cluster.
 - Replace *v1.10.1-eksbuild.4* with the latest version listed in the [latest version table \(p. 341\)](#) for your cluster version.
 - The **--resolve-conflicts** *PRESERVE* option preserves existing configuration values for the add-on. If you've set custom values for add-on settings, and you don't use this option, Amazon EKS overwrites your values with its default values. If you use this option, then we recommend testing any field and value changes on a non-production cluster before updating the add-on on your production cluster. If you change this value to OVERWRITE, all settings are changed to Amazon EKS default values. If you've set custom values for any settings, they might be overwritten with Amazon EKS default values. If you change this value to none, Amazon EKS doesn't change the value of any settings, but the update might fail. If the update fails, you receive an error message to help you resolve the conflict.
 - If you're not updating a configuration setting, remove **--configuration-values** '*{"replicaCount":3}*' from the command. If you're updating a configuration setting, replace '*replicaCount*:3' with the setting that you want to set. In this example, the number of replicas of CoreDNS is set to 3. The value that you specify must be valid for the configuration schema. If you don't know the configuration schema, run **aws eks describe-addon-configuration --addon-name coredns --addon-version v1.10.1-eksbuild.4**, replacing *v1.10.1-eksbuild.4* with the version number of the add-on that you want to see the configuration for. The schema is returned in the output. If you have any existing custom configuration, want to remove it all, and set the values for all settings back to Amazon EKS defaults, remove '*replicaCount*:3' from the command, so that you have empty *{}*. For more information about CoreDNS settings, see [Customizing DNS Service](#) in the Kubernetes documentation.

```
aws eks update-addon --cluster-name my-cluster --addon-name coredns --addon-version v1.10.1-eksbuild.4 \
--resolve-conflicts PRESERVE --configuration-values '{"replicaCount":3}'
```

It might take several seconds for the update to complete.

4. Confirm that the add-on version was updated. Replace *my-cluster* with the name of your cluster.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns
```

It might take several seconds for the update to complete.

An example output is as follows.

```
{  
    "addon": {  
        "addonName": "coredns",  
        "clusterName": "my-cluster",  
        "status": "ACTIVE",  
        "addonVersion": "v1.10.1-eksbuild.4",  
        "health": {  
            "issues": []  
        },  
        "addonArn": "arn:aws:eks:region:111122223333:addon/my-cluster/coredns/  
d2c34f06-1111-2222-1eb0-24f64ce37fa4",  
        "createdAt": "2023-03-01T16:41:32.442000+00:00",  
        "modifiedAt": "2023-03-01T18:16:54.332000+00:00",  
        "tags": {},  
        "configurationValues": "{\"replicaCount\":3}"  
    }  
}
```

Updating the self-managed add-on

Important

We recommend adding the Amazon EKS type of the add-on to your cluster instead of using the self-managed type of the add-on. If you're not familiar with the difference between the types, see [the section called “Amazon EKS add-ons” \(p. 385\)](#). For more information about adding an Amazon EKS add-on to your cluster, see [the section called “Creating an add-on” \(p. 393\)](#). If you're unable to use the Amazon EKS add-on, we encourage you to submit an issue about why you can't to the [Containers roadmap GitHub repository](#).

1. Confirm that you have the self-managed type of the add-on installed on your cluster. Replace *my-cluster* with the name of your cluster.

```
aws eks describe-addon --cluster-name my-cluster --addon-name coredns --query  
addon.addonVersion --output text
```

If an error message is returned, you have the self-managed type of the add-on installed on your cluster. Complete the remaining steps in this procedure. If a version number is returned, you have the Amazon EKS type of the add-on installed on your cluster. To update the Amazon EKS type of the add-on, use the procedure in [the section called “Updating the Amazon EKS add-on” \(p. 343\)](#), rather than using this procedure. If you're not familiar with the differences between the add-on types, see [the section called “Amazon EKS add-ons” \(p. 385\)](#).

2. See which version of the container image is currently installed on your cluster.

```
kubectl describe deployment coredns -n kube-system | grep Image | cut -d ":" -f 3
```

An example output is as follows.

```
v1.8.7-eksbuild.2
```

3. If your current CoreDNS version is v1.5.0 or later, but earlier than the version listed in the [CoreDNS versions \(p. 341\)](#) table, then skip this step. If your current version is earlier than 1.5.0, then you need to modify the ConfigMap for CoreDNS to use the forward add-on, rather than the proxy add-on.

1. Open the configmap with the following command.

```
kubectl edit configmap coredns -n kube-system
```

2. Replace proxy in the following line with forward. Save the file and exit the editor.

```
proxy . /etc/resolv.conf
```

4. If you originally deployed your cluster on Kubernetes 1.17 or earlier, then you may need to remove a discontinued line from your CoreDNS manifest.

Important

You must complete this step before updating to CoreDNS version 1.7.0, but it's recommended that you complete this step even if you're updating to an earlier version.

1. Check to see if your CoreDNS manifest has the line.

```
kubectl get configmap coredns -n kube-system -o jsonpath='{$.data.Corefile}' | grep upstream
```

If no output is returned, your manifest doesn't have the line and you can skip to the next step to update CoreDNS. If output is returned, then you need to remove the line.

2. Edit the ConfigMap with the following command, removing the line in the file that has the word upstream in it. Do not change anything else in the file. Once the line is removed, save the changes.

```
kubectl edit configmap coredns -n kube-system -o yaml
```

5. Retrieve your current CoreDNS image version:

```
kubectl describe deployment coredns -n kube-system | grep Image
```

An example output is as follows.

```
602401143452.dkr.ecr.region-code.amazonaws.com/eks/coredns:v1.8.7-eksbuild.2
```

6. If you're updating to CoreDNS 1.8.3 or later, then you need to add the endpointslices permission to the system:coredns Kubernetes clusterrole.

```
kubectl edit clusterrole system:coredns -n kube-system
```

Add the following lines under the existing permissions lines in the rules section of the file.

```
[...]
- apiGroups:
  - discovery.k8s.io
  resources:
  - endpointslices
  verbs:
  - list
```

```
- watch  
[...]
```

7. Update the CoreDNS add-on by replacing `602401143452` and `region-code` with the values from the output returned in a previous step. Replace `v1.10.1-eksbuild.4` with the CoreDNS version listed in the [latest versions table \(p. 341\)](#) for your Kubernetes version.

```
kubectl set image deployment.apps/coredns -n kube-system  
coredns=602401143452.dkr.ecr.region-code.amazonaws.com/eks/coredns:v1.10.1-eksbuild.4
```

An example output is as follows.

```
deployment.apps/coredns image updated
```

8. Check the container image version again to confirm that it was updated to the version that you specified in the previous step.

```
kubectl describe deployment coredns -n kube-system | grep Image | cut -d ":" -f 3
```

An example output is as follows.

```
v1.10.1-eksbuild.4
```

Updating the Kubernetes kube-proxy self-managed add-on

Important

We recommend adding the Amazon EKS type of the add-on to your cluster instead of using the self-managed type of the add-on. If you're not familiar with the difference between the types, see [the section called "Amazon EKS add-ons" \(p. 385\)](#). For more information about adding an Amazon EKS add-on to your cluster, see [the section called "Creating an add-on" \(p. 393\)](#). If you're unable to use the Amazon EKS add-on, we encourage you to submit an issue about why you can't to the [Containers roadmap GitHub repository](#).

The kube-proxy add-on is deployed on each Amazon EC2 node in your Amazon EKS cluster. It maintains network rules on your nodes and enables network communication to your Pods. The add-on isn't deployed to Fargate nodes in your cluster. For more information, see [kube-proxy](#) in the Kubernetes documentation.

There are two types of the kube-proxy container image available for each Amazon EKS cluster version:

- **Default** – This image type is based on a Debian-based Docker image that is maintained by the Kubernetes upstream community.
- **Minimal** – This image type is based on a [minimal base image](#) maintained by Amazon EKS Distro, which contains minimal packages and doesn't have shells. For more information, see [Amazon EKS Distro](#).

Latest available self-managed kube-proxy container image version for each Amazon EKS cluster version

Image type	1.28	1.27	1.26	1.25	1.24	1.23
kube-proxy (default type)	Only minimal	Only minimal	Only minimal	Only minimal	v1.24.10-eksbuild.2	v1.23.16-eksbuild.2

Image type	1.28	1.27	1.26	1.25	1.24	1.23
	type is available	type is available	type is available	type is available		
kube-proxy (minimal type)	v1.28.2-minimal-eksbuild.2eksbuild.2	v1.27.6-minimal-eksbuild.2eksbuild.2	v1.26.9-minimal-eksbuild.2eksbuild.2	v1.25.14-minimal-eksbuild.2eksbuild.2	v1.24.17-minimal-eksbuild.2eksbuild.2	v1.23.17-minimal-eksbuild.2eksbuild.3

Important

- The default image type isn't available for Kubernetes version 1.25 and later. You must use the minimal image type.
- When you [update an Amazon EKS add-on type \(p. 400\)](#), you specify a valid Amazon EKS add-on version, which might not be a version listed in this table. This is because [Amazon EKS add-on \(p. 387\)](#) versions don't always match container image versions specified when updating the self-managed type of this add-on. When you update the self-managed type of this add-on, you specify a valid container image version listed in this table.

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Getting started with Amazon EKS \(p. 6\)](#).

Considerations

- Kube-proxy on an Amazon EKS cluster has the same [compatibility and skew policy as Kubernetes](#).
- Kube-proxy must be the same minor version as kubelet on your Amazon EC2 nodes.
- Kube-proxy can't be later than the minor version of your cluster's control plane.
- The kube-proxy version on your Amazon EC2 nodes can't be more than two minor versions earlier than your control plane. For example, if your control plane is running Kubernetes 1.28, then the kube-proxy minor version can't be earlier than 1.26.
- If you recently updated your cluster to a new Kubernetes minor version, then update your Amazon EC2 nodes to the same minor version *before* updating kube-proxy to the same minor version as your nodes.

To update the kube-proxy self-managed add-on

- Confirm that you have the self-managed type of the add-on installed on your cluster. Replace **my-cluster** with the name of your cluster.

```
aws eks describe-addon --cluster-name my-cluster --addon-name kube-proxy --query
addon.addonVersion --output text
```

If an error message is returned, you have the self-managed type of the add-on installed on your cluster. The remaining steps in this topic are for updating the self-managed type of the add-on. If a version number is returned, you have the Amazon EKS type of the add-on installed on your cluster. To update it, use the procedure in [the section called "Updating an add-on" \(p. 400\)](#), rather than using the procedure in this topic. If you're not familiar with the differences between the add-on types, see [the section called "Amazon EKS add-ons" \(p. 385\)](#).

- See which version of the container image is currently installed on your cluster.

```
kubectl describe daemonset kube-proxy -n kube-system | grep Image
```

An example output is as follows.

```
Image: 602401143452.dkr.ecr.region-code.amazonaws.com/eks/kube-proxy:v1.25.6-minimal-eksbuild.2
```

In the example output, *v1.25.6-minimal-eksbuild.2* is the version installed on the cluster.

3. Update the kube-proxy add-on by replacing *602401143452* and *region-code* with the values from your output. In the previous step Replace *v1.26.2-minimal-eksbuild.2* with the kube-proxy version listed in the [Latest available self-managed kube-proxy container image version for each Amazon EKS cluster version \(p. 347\)](#) table. You can specify a version number for the *default* or *minimal* image type.

```
kubectl set image daemonset.apps/kube-proxy -n kube-system kube-proxy=602401143452.dkr.ecr.region-code.amazonaws.com/eks/kube-proxy:v1.26.2-minimal-eksbuild.2
```

An example output is as follows.

```
daemonset.apps/kube-proxy image updated
```

4. Confirm that the new version is now installed on your cluster.

```
kubectl describe daemonset kube-proxy -n kube-system | grep Image | cut -d ":" -f 3
```

An example output is as follows.

```
v1.26.2-minimal-eksbuild.2
```

5. If you're using x86 and Arm nodes in the same cluster and your cluster was deployed before August 17, 2020. Then, edit your kube-proxy manifest to include a node selector for multiple hardware architectures with the following command. This is a one-time operation. After you've added the selector to your manifest, you don't need to add it each time you update the add-on. If your cluster was deployed on or after August 17, 2020, then kube-proxy is already multi-architecture capable.

```
kubectl edit -n kube-system daemonset/kube-proxy
```

Add the following node selector to the file in the editor and then save the file. For an example of where to include this text in the editor, see the [CNI manifest](#) file on GitHub. This enables Kubernetes to pull the correct hardware image based on the node's hardware architecture.

```
- key: "kubernetes.io/arch"
operator: In
values:
- amd64
- arm64
```

6. If your cluster was originally created with Kubernetes version 1.14 or later, then you can skip this step because kube-proxy already includes this Affinity Rule. If you originally created an Amazon EKS cluster with Kubernetes version 1.13 or earlier and intend to use Fargate nodes in your cluster, then edit your kube-proxy manifest to include a NodeAffinity rule to prevent kube-proxy Pods from scheduling on Fargate nodes. This is a one-time edit. Once you've added the Affinity Rule to your manifest, you don't need to add it each time that you update the add-on. Edit your kube-proxy DaemonSet.

```
kubectl edit -n kube-system daemonset/kube-proxy
```

Add the following Affinity Rule to the DaemonSet spec section of the file in the editor and then save the file. For an example of where to include this text in the editor, see the [CNI manifest](#) file on GitHub.

```
- key: eks.amazonaws.com/compute-type
  operator: NotIn
  values:
  - fargate
```

Installing the Calico network policy engine add-on

[Project Calico](#) is a network policy engine for Kubernetes. With Calico network policy enforcement, you can implement network segmentation and tenant isolation. This is useful in multi-tenant environments where you must isolate tenants from each other or when you want to create separate environments for development, staging, and production. Network policies are similar to AWS security groups in that you can create network ingress and egress rules. Instead of assigning instances to a security group, you assign network policies to Pods using Pod selectors and labels.

Considerations

- Calico is not supported when using Fargate with Amazon EKS.
- Calico adds rules to iptables on the node that may be higher priority than existing rules that you've already implemented outside of Calico. Consider adding existing iptables rules to your Calico policies to avoid having rules outside of Calico policy overridden by Calico.
- If you're using the Amazon VPC CNI add-on version 1.10 or earlier, [security groups for Pods \(p. 324\)](#) traffic flow to Pods on branch network interfaces is not subjected to Calico network policy enforcement and is limited to Amazon EC2 security group enforcement only. If you're using 1.11.0 or later of the Amazon VPC CNI add-on, traffic flow to Pods on branch network interfaces is subject to Calico network policy enforcement if you set `POD_SECURITY_GROUP_ENFORCING_MODE=standard` for the Amazon VPC CNI add-on.
- The IP family setting for your cluster must be IPv4. You can't use the Calico network policy engine add-on if your cluster was created to use the IPv6 family.

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Getting started with Amazon EKS \(p. 6\)](#).
- The `kubectl` command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use `kubectl` version 1.26, 1.27, or 1.28 with it. To install or upgrade `kubectl`, see [Installing or updating kubectl \(p. 6\)](#).

The following procedure shows you how to install Calico on Linux nodes in your Amazon EKS cluster. To install Calico on Windows nodes, see [Using Calico on Amazon EKS Windows Containers](#).

Install Calico on your Amazon EKS Linux nodes

Important

Amazon EKS doesn't maintain the charts used in the following procedures. The recommended way to install Calico on Amazon EKS is by using the [Calico Operator](#). Install the Calico Operator by following the guide at [Amazon Elastic Kubernetes Service | Calico Documentation](#) on the

Calico Documentation website. If you encounter issues during installation and usage of Calico, submit issues to [Calico Operator](#) and the [Calico](#) project directly. You should always contact Tigera for compatibility of any new Calico operator and Calico versions before installing them on your cluster.

Prerequisite

Helm version 3.0 or later installed on your computer. To install or upgrade Helm, see [Using Helm with Amazon EKS \(p. 450\)](#).

To install Calico using Helm

1. Install Calico version 3.25 using the Tigera instructions. For more information, see [Install Calico](#) in the Calico documentation.
2. View the resources in the `tigera-operator` namespace.

```
kubectl get all -n tigera-operator
```

An example output is as follows.

NAME	READY	STATUS	RESTARTS	AGE
pod/tigera-operator-768d489967-6cv58	1/1	Running	0	27m
deployment.apps/tigera-operator	1/1	Up-to-date	1	27m
replicaset.apps/tigera-operator-768d489967	1	Desired	1	27m

The values in the DESIRED and READY columns for the replicaset should match.

3. View the resources in the `calico-system` namespace.

```
kubectl get all -n calico-system
```

An example output is as follows.

NAME	READY	STATUS	RESTARTS	AGE	
pod/calico-kube-controllers-55c98678-gh6cc	1/1	Running	0	4m29s	
pod/calico-node-khw4w	1/1	Running	0	4m29s	
pod/calico-node-rrz8k	1/1	Running	0	4m29s	
pod/calico-typfa-696bcd55cb-49ptr	1/1	Running	0	4m29s	
pod/csi-node-driver-6v2z5	2/2	Running	0	4m29s	
pod/csi-node-driver-wrw2d	2/2	Running	0	4m29s	
NAME	TYPE	CLUSTER-IP	EXTERNAL-IP		
PORT(S)	AGE				
service/calico-kube-controllers-metrics	ClusterIP	None	<none>		
9094/TCP 4m23s					
service/calico-typfa	ClusterIP	10.100.67.39	<none>		
5473/TCP 4m30s					
NAME	DESIRED	CURRENT	READY	UP-TO-DATE	AVAILABLE
NODE SELECTOR	AGE				
daemonset.apps/calico-node	2	2	2	2	2
kubernetes.io/os=linux	4m29s				
daemonset.apps/csi-node-driver	2	2	2	2	2
kubernetes.io/os=linux	4m29s				
NAME	READY	UP-TO-DATE	AVAILABLE	AGE	

deployment.apps/calico-kube-controllers	1/1	1	1	4m29s
deployment.apps/calico-typfa	1/1	1	1	4m29s
NAME	DESIRED	CURRENT	READY	AGE
replicaset.apps/calico-kube-controllers- 55c98678	1	1	1	4m29s
replicaset.apps/calico-typfa- 696bcd55cb	1	1	1	4m29s

The values in the DESIRED and READY columns for the calico-node daemonset should match. The values in the DESIRED and READY columns for the two replicasesets should also match. The number in the DESIRED column for daemonset.apps/calico-node varies based on the number of nodes in your cluster.

4. Confirm that the logs for one of your calico-node, calico-typfa, and tigera-operator Pods don't contain ERROR. Replace the values in the following commands with the values returned in your output for the previous steps.

```
kubectl logs tigera-operator-768d489967-6cv58 -n tigera-operator | grep ERROR
kubectl logs calico-node-khw4w -c calico-node -n calico-system | grep ERROR
kubectl logs calico-typfa-696bcd55cb-49ptr -n calico-system | grep ERROR
```

If no output is returned from the previous commands, then ERROR doesn't exist in your logs and everything should be running correctly.

5. If you're using version 1.9.3 or later of the Amazon VPC CNI plugin for Kubernetes, then enable the plugin to add the Pod IP address to an annotation in the calico-kube-controllers-**55c98678-gh6cc** Pod spec. For more information about this setting, see [_ANNOATATE_POD_IP](#) on GitHub.

- a. See which version of the plugin is installed on your cluster with the following command.

```
kubectl describe daemonset aws-node -n kube-system | grep amazon-k8s-cni: | cut -d ":" -f 3
```

An example output is as follows.

```
v1.12.2-eksbuild.1
```

- b. Create a configuration file that you can apply to your cluster that grants the aws-node Kubernetes clusterrole the permission to patch Pods.

```
cat << EOF > append.yaml
- apiGroups:
  - ""
  resources:
  - pods
  verbs:
  - patch
EOF
```

- c. Apply the updated permissions to your cluster.

```
kubectl apply -f <(cat <(kubectl get clusterrole aws-node -o yaml) append.yaml)
```

- d. Set the environment variable for the plugin.

```
kubectl set env daemonset aws-node -n kube-system ANNOTATE_POD_IP=true
```

- e. Delete the calico-kube-controllers-**55c98678-gh6cc**

```
kubectl delete pod calico-kube-controllers-55c98678-gh6cc -n calico-system
```

- f. View the Pods in the calico-system namespace again to see the ID of the new calico-kube-controllers Pod that Kubernetes replaced the calico-kube-controllers-*55c98678-gh6cc* Pod that you deleted in the previous step with.

```
kubectl get pods -n calico-system
```

- g. Confirm that the `vpc.amazonaws.com/pod-ips` annotation is added to the new calico-kube-controllers Pod.
 - Replace *5cd7d477df-2xqpd* with the ID for the Pod returned in a previous step.

```
kubectl describe pod calico-kube-controllers-5cd7d477df-2xqpd -n calico-system  
| grep vpc.amazonaws.com/pod-ips
```

An example output is as follows.

```
vpc.amazonaws.com/pod-ips: 192.168.25.9
```

Stars policy demo

You can apply network policies to be used by any network policy engine. Because of this, you can follow the [Stars demo of network policy \(p. 296\)](#) with Calico.

Remove Calico

Remove Calico from your cluster using Helm.

```
helm uninstall calico
```

Note

Even after deleting the resources, there can still be `iptables` rules on the nodes that might interfere in unexpected ways with networking in your cluster. The only sure way to remove Calico is to terminate all of the nodes and recycle them. To terminate all nodes, either set the Auto Scaling Group desired count to 0, then back up to the desired number, or just terminate the nodes.

Access the Amazon Elastic Kubernetes Service using an interface endpoint (AWS PrivateLink)

You can use AWS PrivateLink to create a private connection between your VPC and Amazon Elastic Kubernetes Service. You can access Amazon EKS as if it were in your VPC, without the use of an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to access Amazon EKS.

You establish this private connection by creating an interface endpoint powered by AWS PrivateLink. We create an endpoint network interface in each subnet that you enable for the interface endpoint. These are requester-managed network interfaces that serve as the entry point for traffic destined for Amazon EKS.

For more information, see [Access AWS services through AWS PrivateLink](#) in the [AWS PrivateLink Guide](#).

Considerations for Amazon EKS

- Before you set up an interface endpoint for Amazon EKS, review [Considerations](#) in the [AWS PrivateLink Guide](#).
- Amazon EKS supports making calls to all of its API actions through the interface endpoint, but not to the Kubernetes APIs. The Kubernetes API server already supports a [private endpoint \(p. 41\)](#). The Kubernetes API server private endpoint creates a private endpoint for the Kubernetes API server that you use to communicate with your cluster (using Kubernetes management tools such as kubectl). You can enable [private access \(p. 58\)](#) to the Kubernetes API server so that all communication between your nodes and the API server stays within your VPC. AWS PrivateLink for the Amazon EKS API helps you call the Amazon EKS APIs from your VPC without exposing traffic to the public internet.
- You can't configure Amazon EKS to only be accessed through an interface endpoint.
- Standard pricing for AWS PrivateLink applies for interface endpoints for Amazon EKS. You are billed for every hour that an interface endpoint is provisioned in each Availability Zone and for data processed through the interface endpoint. For more information, see [AWS PrivateLink pricing](#).
- VPC endpoint policies are not supported for Amazon EKS. By default, full access to Amazon EKS is allowed through the interface endpoint. Alternatively, you can associate a security group with the endpoint network interfaces to control traffic to Amazon EKS through the interface endpoint.
- You can use VPC flow logs to capture information about IP traffic going to and from network interfaces, including interface endpoints. You can publish flow log data to Amazon CloudWatch or Amazon S3. For more information, see [Logging IP traffic using VPC Flow Logs](#) in the Amazon VPC User Guide.
- You can access the Amazon EKS APIs from an on-premises data center by connecting it to a VPC that has an interface endpoint. You can use AWS Direct Connect or AWS Site-to-Site VPN to connect your on-premises sites to a VPC.
- You can connect other VPCs to the VPC with an interface endpoint using an AWS Transit Gateway or VPC peering. VPC peering is a networking connection between two VPCs. You can establish a VPC peering connection between your VPCs, or with a VPC in another account. The VPCs can be in different AWS Regions. Traffic between peered VPCs stays on the AWS network. The traffic doesn't traverse the public internet. A Transit Gateway is a network transit hub that you can use to interconnect VPCs. Traffic between a VPC and a Transit Gateway remains on the AWS global private network. The traffic isn't exposed to the public internet.
- VPC interface endpoints for Amazon EKS are only accessible over IPv4. IPv6 isn't supported.
- AWS PrivateLink support isn't available in the Asia Pacific (Hyderabad), Asia Pacific (Jakarta), Asia Pacific (Melbourne), Asia Pacific (Osaka), Europe (Spain), Europe (Zurich), Israel (Tel Aviv), or Middle East (UAE) AWS Regions.

Create an interface endpoint for Amazon EKS

You can create an interface endpoint for Amazon EKS using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see [Create a VPC endpoint](#) in the [AWS PrivateLink Guide](#).

Create an interface endpoint for Amazon EKS using the following service name:

```
com.amazonaws.region.eks
```

The private DNS feature is enabled by default when creating an interface endpoint for Amazon EKS and other AWS services. However, you must ensure that the following VPC attributes are set to true: enableDnsHostnames and enableDnsSupport. For more information, see [View and update DNS](#)

[attributes for your VPC](#) in the Amazon VPC User Guide. With the private DNS feature enabled for the interface endpoint:

- You can make any API request to Amazon EKS using its default Regional DNS name. For example, `eks.region.amazonaws.com`. For a list of APIs, see [Actions](#) in the Amazon EKS API Reference.
- You don't need to make any changes to your applications that call the EKS APIs.
- Any call made to the Amazon EKS default service endpoint is automatically routed through the interface endpoint over the private AWS network.

Workloads

Your workloads are deployed in containers, which are deployed in Pods in Kubernetes. A Pod includes one or more containers. Typically, one or more Pods that provide the same service are deployed in a Kubernetes service. Once you've deployed multiple Pods that provide the same service, you can:

- [View information about the workloads \(p. 529\)](#) running on each of your clusters using the AWS Management Console.
- Vertically scale Pods up or down with the Kubernetes [Vertical Pod Autoscaler \(p. 363\)](#).
- Horizontally scale the number of Pods needed to meet demand up or down with the Kubernetes [Horizontal Pod Autoscaler \(p. 367\)](#).
- Create an external (for internet-accessible Pods) or an internal (for private Pods) [network load balancer \(p. 369\)](#) to balance network traffic across Pods. The load balancer routes traffic at Layer 4 of the OSI model.
- Create an [Application load balancing on Amazon EKS \(p. 375\)](#) to balance application traffic across Pods. The application load balancer routes traffic at Layer 7 of the OSI model.
- If you're new to Kubernetes, this topic helps you [Deploy a sample application \(p. 356\)](#).
- You can [restrict IP addresses that can be assigned to a service \(p. 379\)](#) with externalIPs.

Deploy a sample application

In this topic, you deploy a sample application to your cluster.

Prerequisites

- An existing Kubernetes cluster with at least one node. If you don't have an existing Amazon EKS cluster, you can deploy one using one of the [Getting started with Amazon EKS \(p. 6\)](#) guides. If you're deploying a Windows application, then you must have [Windows support \(p. 49\)](#) enabled for your cluster and at least one Amazon EC2 Windows node.
- Kubectl installed on your computer. For more information, see [Installing or updating kubectl \(p. 6\)](#).
- Kubectl configured to communicate with your cluster. For more information, see [Creating or updating a kubeconfig file for an Amazon EKS cluster \(p. 431\)](#).
- If you plan to deploy your sample workload to Fargate, then you must have an existing [Fargate profile \(p. 136\)](#) that includes the same namespace created in this tutorial, which is eks-sample-app, unless you change the name. If you used one of the [getting started guides \(p. 6\)](#) to create your cluster, then you'll have to create a new profile, or add the namespace to your existing profile, because the profile created in the getting started guides doesn't specify the namespace used in this tutorial. Your VPC must also have at least one private subnet.

To deploy a sample application

Though many variables are changeable in the following steps, we recommend only changing variable values where specified. Once you have a better understanding of Kubernetes Pods, deployments, and services, you can experiment with changing other values.

1. Create a namespace. A namespace allows you to group resources in Kubernetes. For more information, see [Namespaces](#) in the Kubernetes documentation. If you plan to deploy your sample application to [AWS Fargate \(p. 131\)](#), make sure that the value for namespace in your [AWS Fargate profile \(p. 136\)](#) is eks-sample-app.

```
kubectl create namespace eks-sample-app
```

2. Create a Kubernetes deployment. This sample deployment pulls a container image from a public repository and deploys three replicas (individual Pods) of it to your cluster. To learn more, see [Deployments](#) in the Kubernetes documentation. You can deploy the application to Linux or Windows nodes. If you're deploying to Fargate, then you can only deploy a Linux application.
 - a. Save the following contents to a file named `eks-sample-deployment.yaml`. The containers in the sample application don't use network storage, but you might have applications that need to. For more information, see [Storage \(p. 228\)](#).

Linux

The `amd64` or `arm64` values under the `kubernetes.io/arch` key mean that the application can be deployed to either hardware architecture (if you have both in your cluster). This is possible because this image is a multi-architecture image, but not all are. You can determine the hardware architecture that the image is supported on by viewing the [image details](#) in the repository that you're pulling it from. When deploying images that don't support a hardware architecture type, or that you don't want the image deployed to, remove that type from the manifest. For more information, see [Well-Known Labels, Annotations and Taints](#) in the Kubernetes documentation.

The `kubernetes.io/os: linux` `nodeSelector` means that if you had Linux and Windows nodes (for example) in your cluster, the image would only be deployed to Linux nodes. For more information, see [Well-Known Labels, Annotations and Taints](#) in the Kubernetes documentation.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: eks-sample-linux-deployment
  namespace: eks-sample-app
  labels:
    app: eks-sample-linux-app
spec:
  replicas: 3
  selector:
    matchLabels:
      app: eks-sample-linux-app
  template:
    metadata:
      labels:
        app: eks-sample-linux-app
    spec:
      affinity:
        nodeAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
            nodeSelectorTerms:
              - matchExpressions:
                  - key: kubernetes.io/arch
                    operator: In
                    values:
                      - amd64
                      - arm64
      containers:
        - name: nginx
          image: public.ecr.aws/nginx/nginx:1.23
          ports:
            - name: http
              containerPort: 80
          imagePullPolicy: IfNotPresent
```

```
nodeSelector:  
  kubernetes.io/os: linux
```

Windows

The `kubernetes.io/os: windows` nodeSelector means that if you had Windows and Linux nodes (for example) in your cluster, the image would only be deployed to Windows nodes. For more information, see [Well-Known Labels, Annotations and Taints](#) in the Kubernetes documentation.

```
apiVersion: apps/v1  
kind: Deployment  
metadata:  
  name: eks-sample-windows-deployment  
  namespace: eks-sample-app  
  labels:  
    app: eks-sample-windows-app  
spec:  
  replicas: 3  
  selector:  
    matchLabels:  
      app: eks-sample-windows-app  
  template:  
    metadata:  
      labels:  
        app: eks-sample-windows-app  
    spec:  
      affinity:  
        nodeAffinity:  
          requiredDuringSchedulingIgnoredDuringExecution:  
            nodeSelectorTerms:  
              - matchExpressions:  
                  - key: beta.kubernetes.io/arch  
                    operator: In  
                    values:  
                      - amd64  
      containers:  
        - name: windows-server-iis  
          image: mcr.microsoft.com/windows/servercore:ltsc2019  
          ports:  
            - name: http  
              containerPort: 80  
          imagePullPolicy: IfNotPresent  
          command:  
            - powershell.exe  
            - -command  
            - "Add-WindowsFeature Web-Server; Invoke-WebRequest -UseBasicParsing  
-Uri 'https://dotnetbinaries.blob.core.windows.net/servicemonitor/2.0.1.6/  
ServiceMonitor.exe' -OutFile 'C:\\ServiceMonitor.exe'; echo '<html><body><br>  
<br><marquee><H1>Hello EKS!!!<H1><marquee></body></html>' > C:\\inetpub\\  
\\wwwroot\\default.html; C:\\ServiceMonitor.exe 'w3svc'; "  
          nodeSelector:  
            kubernetes.io/os: windows
```

- b. Apply the deployment manifest to your cluster.

```
kubectl apply -f eks-sample-deployment.yaml
```

3. Create a service. A service allows you to access all replicas through a single IP address or name. For more information, see [Service](#) in the Kubernetes documentation. Though not implemented in the sample application, if you have applications that need to interact with other AWS services, we recommend that you create Kubernetes service accounts for your Pods, and associate them to AWS

IAM accounts. By specifying service accounts, your Pods have only the minimum permissions that you specify for them to interact with other services. For more information, see [IAM roles for service accounts \(p. 464\)](#).

- a. Save the following contents to a file named `eks-sample-service.yaml`. Kubernetes assigns the service its own IP address that is accessible only from within the cluster. To access the service from outside of your cluster, deploy the [AWS Load Balancer Controller \(p. 333\)](#) to load balance [application \(p. 375\)](#) or [network \(p. 369\)](#) traffic to the service.

Linux

```
apiVersion: v1
kind: Service
metadata:
  name: eks-sample-linux-service
  namespace: eks-sample-app
  labels:
    app: eks-sample-linux-app
spec:
  selector:
    app: eks-sample-linux-app
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
```

Windows

```
apiVersion: v1
kind: Service
metadata:
  name: eks-sample-windows-service
  namespace: eks-sample-app
  labels:
    app: eks-sample-windows-app
spec:
  selector:
    app: eks-sample-windows-app
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
```

- b. Apply the service manifest to your cluster.

```
kubectl apply -f eks-sample-service.yaml
```

4. View all resources that exist in the `eks-sample-app` namespace.

```
kubectl get all -n eks-sample-app
```

An example output is as follows.

If you deployed Windows resources, then all instances of `Linux` in the following output are `windows`. The other *example values* may be different from your output.

NAME	READY	STATUS	RESTARTS	AGE
pod/eks-sample- <code>Linux</code> -deployment- <code>65b7669776-m6qxz</code>	1/1	Running	0	27m
pod/eks-sample- <code>Linux</code> -deployment- <code>65b7669776-mmxdv</code>	1/1	Running	0	27m
pod/eks-sample- <code>Linux</code> -deployment- <code>65b7669776-qzn22</code>	1/1	Running	0	27m

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)
AGE service/eks-sample- <i>linux</i> -service	ClusterIP	<i>10.100.74.8</i>	<none>	80/TCP
NAME deployment.apps/eks-sample- <i>linux</i> -deployment	READY 3/3	UP-TO-DATE 3	AVAILABLE 3	AGE 27m
NAME AGE replicaset.apps/eks-sample- <i>linux</i> -deployment- <i>776d8f8fd8</i>	DESIRED 3	CURRENT 3	READY 3	27m

In the output, you see the service and deployment that were specified in the sample manifests deployed in previous steps. You also see three Pods. This is because 3 replicas were specified in the sample manifest. For more information about Pods, see [Pods](#) in the Kubernetes documentation. Kubernetes automatically creates the replicaset resource, even though it isn't specified in the sample manifests. For more information about ReplicaSets, see [ReplicaSet](#) in the Kubernetes documentation.

Note

Kubernetes maintains the number of replicas that are specified in the manifest. If this were a production deployment and you wanted Kubernetes to horizontally scale the number of replicas or vertically scale the compute resources for the Pods, use the [Horizontal Pod Autoscaler \(p. 367\)](#) and the [Vertical Pod Autoscaler \(p. 363\)](#) to do so.

- View the details of the deployed service. If you deployed a Windows service, replace *Linux* with **windows**.

```
kubectl -n eks-sample-app describe service eks-sample-linux-service
```

An example output is as follows.

If you deployed Windows resources, then all instances of *linux* in the following output are windows. The other *example values* may be different from your output.

Name:	eks-sample- <i>linux</i> -service
Namespace:	eks-sample-app
Labels:	app=eks-sample- <i>linux</i> -app
Annotations:	<none>
Selector:	app=eks-sample- <i>linux</i> -app
Type:	ClusterIP
IP Families:	<none>
IP:	<i>10.100.74.8</i>
IPs:	<i>10.100.74.8</i>
Port:	<unset> 80/TCP
TargetPort:	80/TCP
Endpoints:	<i>192.168.24.212:80,192.168.50.185:80,192.168.63.93:80</i>
Session Affinity:	None
Events:	<none>

In the previous output, the value for IP: is a unique IP address that can be reached from any node or Pod within the cluster, but it can't be reached from outside of the cluster. The values for Endpoints are IP addresses assigned from within your VPC to the Pods that are part of the service.

- View the details of one of the Pods listed in the output when you [viewed the namespace \(p. 359\)](#) in a previous step. If you deployed a Windows app, replace *Linux* with **windows** and replace *776d8f8fd8-78w66* with the value returned for one of your Pods.

```
kubectl -n eks-sample-app describe pod eks-sample-linux-deployment-65b7669776-m6qxz
```

Abbreviated output

If you deployed Windows resources, then all instances of `linux` in the following output are windows. The other *example values* may be different from your output.

```
Name: eks-sample-linux-deployment-65b7669776-m6qxz
Namespace: eks-sample-app
Priority: 0
Node: ip-192-168-45-132.us-west-2.compute.internal/192.168.45.132
[...]
IP: 192.168.63.93
IPs:
  IP: 192.168.63.93
Controlled By: ReplicaSet/eks-sample-linux-deployment-65b7669776
[...]
Conditions:
  Type Status
  Initialized True
  Ready True
  ContainersReady True
  PodScheduled True
[...]
Events:
  Type Reason Age From
  Message
  ---- -----
  Normal Scheduled 3m20s default-scheduler
  Successfully assigned eks-sample-app/eks-sample-linux-deployment-65b7669776-m6qxz to
  ip-192-168-45-132.us-west-2.compute.internal
[...]
```

In the previous output, the value for IP: is a unique IP that's assigned to the Pod from the CIDR block assigned to the subnet that the node is in. If you prefer to assign Pods IP addresses from different CIDR blocks, you can change the default behavior. For more information, see [Custom networking for pods \(p. 306\)](#). You can also see that the Kubernetes scheduler scheduled the Pod on the Node with the IP address `192.168.45.132`.

Tip

Rather than using the command line, you can view many details about Pods, services, deployments, and other Kubernetes resources in the AWS Management Console. For more information, see [View Kubernetes resources \(p. 529\)](#).

7. Run a shell on the Pod that you described in the previous step, replacing `65b7669776-m6qxz` with the ID of one of your Pods.

Linux

```
kubectl exec -it eks-sample-linux-deployment-65b7669776-m6qxz -n eks-sample-app
-- /bin/bash
```

Windows

```
kubectl exec -it eks-sample-windows-deployment-65b7669776-m6qxz -n eks-sample-app
-- powershell.exe
```

8. From the Pod shell, view the output from the web server that was installed with your deployment in a previous step. You only need to specify the service name. It is resolved to the service's IP address by CoreDNS, which is deployed with an Amazon EKS cluster, by default.

Linux

```
curl eks-sample-linux-service
```

An example output is as follows.

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
[...]
```

Windows

```
Invoke-WebRequest -uri eks-sample-windows-service/default.html -UseBasicParsing
```

An example output is as follows.

```
Statuscode      : 200
StatusDescription : OK
Content        : < h t m l > < b o d y > < b r / > < b r / > < m a r q u e e > <
H 1 > H e l l o
                           E K S ! ! ! < H 1 > < m a r q u e e > < / b o d y > < h t m l
>
```

9. From the Pod shell, view the DNS server for the Pod.

Linux

```
cat /etc/resolv.conf
```

An example output is as follows.

```
nameserver 10.100.0.10
search eks-sample-app.svc.cluster.local svc.cluster.local cluster.local us-
west-2.compute.internal
options ndots:5
```

In the previous output, 10.100.0.10 is automatically assigned as the nameserver for all Pods deployed to the cluster.

Windows

```
Get-NetIPConfiguration
```

Abbreviated output

```
InterfaceAlias      : vEthernet
[...]
IPv4Address        : 192.168.63.14
[...]
DNSServer          : 10.100.0.10
```

In the previous output, `10.100.0.10` is automatically assigned as the DNS server for all Pods deployed to the cluster.

10. Disconnect from the Pod by typing `exit`.
11. Once you're finished with the sample application, you can remove the sample namespace, service, and deployment with the following command.

```
kubectl delete namespace eks-sample-app
```

Vertical Pod Autoscaler

The Kubernetes [Vertical Pod Autoscaler](#) automatically adjusts the CPU and memory reservations for your Pods to help "right size" your applications. This adjustment can improve cluster resource utilization and free up CPU and memory for other Pods. This topic helps you to deploy the Vertical Pod Autoscaler to your cluster and verify that it is working.

Prerequisites

- You have an existing Amazon EKS cluster. If you don't, see [Getting started with Amazon EKS \(p. 6\)](#).
- You have the Kubernetes Metrics Server installed. For more information, see [Installing the Kubernetes Metrics Server \(p. 450\)](#).
- You are using a `kubectl` client that is [configured to communicate with your Amazon EKS cluster \(p. 19\)](#).
- OpenSSL 1.1.1 or later installed on your device.

Deploy the Vertical Pod Autoscaler

In this section, you deploy the Vertical Pod Autoscaler to your cluster.

To deploy the Vertical Pod Autoscaler

1. Open a terminal window and navigate to a directory where you would like to download the Vertical Pod Autoscaler source code.
2. Clone the [kubernetes/autoscaler](#) GitHub repository.

```
git clone https://github.com/kubernetes/autoscaler.git
```

3. Change to the `vertical-pod-autoscaler` directory.

```
cd autoscaler/vertical-pod-autoscaler/
```

4. (Optional) If you have already deployed another version of the Vertical Pod Autoscaler, remove it with the following command.

```
./hack/vpa-down.sh
```

5. If your nodes don't have internet access to the `registry.k8s.io` container registry, then you need to pull the following images and push them to your own private repository. For more information about how to pull the images and push them to your own private repository, see [Copy a container image from one repository to another repository \(p. 381\)](#).

```
registry.k8s.io/autoscaling/vpa-admission-controller:0.10.0
```

```
registry.k8s.io/autoscaling/vpa-recommender:0.10.0
registry.k8s.io/autoscaling/vpa-updater:0.10.0
```

If you're pushing the images to a private Amazon ECR repository, then replace `registry.k8s.io` in the manifests with your registry. Replace `111122223333` with your account ID. Replace `region-code` with the AWS Region that your cluster is in. The following commands assume that you named your repository the same as the repository name in the manifest. If you named your repository something different, then you'll need to change it too.

```
sed -i.bak -e 's/registry.k8s.io/111122223333.dkr.ecr.region-codeamazonaws.com/' ./deploy/admission-controller-deployment.yaml
sed -i.bak -e 's/registry.k8s.io/111122223333.dkr.ecr.region-codeamazonaws.com/' ./deploy/recommender-deployment.yaml
sed -i.bak -e 's/registry.k8s.io/111122223333.dkr.ecr.region-codeamazonaws.com/' ./deploy/updater-deployment.yaml
```

6. Deploy the Vertical Pod Autoscaler to your cluster with the following command.

```
./hack/vpa-up.sh
```

7. Verify that the Vertical Pod Autoscaler Pods have been created successfully.

```
kubectl get pods -n kube-system
```

An example output is as follows.

NAME	READY	STATUS	RESTARTS	AGE
[...]				
metrics-server-8459fc497-kfj8w	1/1	Running	0	83m
vpa-admission-controller-68c748777d-ppspd	1/1	Running	0	7s
vpa-recommender-6fc8c67d85-gljpl	1/1	Running	0	8s
vpa-updater-786b96955c-bgp9d	1/1	Running	0	8s

Test your Vertical Pod Autoscaler installation

In this section, you deploy a sample application to verify that the Vertical Pod Autoscaler is working.

To test your Vertical Pod Autoscaler installation

1. Deploy the `hamster.yaml` Vertical Pod Autoscaler example with the following command.

```
kubectl apply -f examples/hamster.yaml
```

2. Get the Pods from the `hamster` example application.

```
kubectl get pods -l app=hamster
```

An example output is as follows.

hamster-c7d89d6db-rglf5	1/1	Running	0	48s
hamster-c7d89d6db-znvz5	1/1	Running	0	48s

3. Describe one of the Pods to view its cpu and memory reservation. Replace `c7d89d6db-rglf5` with one of the IDs returned in your output from the previous step.

```
kubectl describe pod hamster-c7d89d6db-rglf5
```

An example output is as follows.

```
[...]
Containers:
  hamster:
    Container ID: docker://e76c2413fc720ac395c33b64588c82094fc8e5d590e373d5f818f3978f577e24
      Image:          registry.k8s.io/ubuntu-slim:0.1
      Image ID:       docker-pullable://registry.k8s.io/ubuntu-
slim@sha256:b6f8c3885f5880a4f1a7cf717c07242eb4858fdd5a84b5ffe35b1cf680ea17b1
      Port:           <none>
      Host Port:     <none>
      Command:       /bin/sh
      Args:
        -c
        while true; do timeout 0.5s yes >/dev/null; sleep 0.5s; done
      State:          Running
      Started:       Fri, 27 Sep 2019 10:35:16 -0700
      Ready:          True
      Restart Count:  0
      Requests:
        cpu:          100m
        memory:       50Mi
[...]
```

You can see that the original Pod reserves 100 millicpu of CPU and 50 mebibytes of memory. For this example application, 100 millicpu is less than the Pod needs to run, so it is CPU-constrained. It also reserves much less memory than it needs. The Vertical Pod Autoscaler vpa-recommender deployment analyzes the hamster Pods to see if the CPU and memory requirements are appropriate. If adjustments are needed, the vpa-updater relaunches the Pods with updated values.

4. Wait for the vpa-updater to launch a new hamster Pod. This should take a minute or two. You can monitor the Pods with the following command.

Note

If you are not sure that a new Pod has launched, compare the Pod names with your previous list. When the new Pod launches, you will see a new Pod name.

```
kubectl get --watch Pods -l app=hamster
```

5. When a new hamster Pod is started, describe it and view the updated CPU and memory reservations.

```
kubectl describe pod hamster-c7d89d6db-jxgfv
```

An example output is as follows.

```
[...]
Containers:
  hamster:
    Container ID: docker://2c3e7b6fb7ce0d8c86444334df654af6fb3fc88aad4c5d710eac3b1e7c58f7db
      Image:          registry.k8s.io/ubuntu-slim:0.1
      Image ID:       docker-pullable://registry.k8s.io/ubuntu-
slim@sha256:b6f8c3885f5880a4f1a7cf717c07242eb4858fdd5a84b5ffe35b1cf680ea17b1
      Port:           <none>
```

```

Host Port:      <none>
Command:
  /bin/sh
Args:
  -c
    while true; do timeout 0.5s yes >/dev/null; sleep 0.5s; done
State:          Running
  Started:     Fri, 27 Sep 2019 10:37:08 -0700
Ready:          True
Restart Count:  0
Requests:
  cpu:        587m
  memory:    262144k
[...]

```

In the previous output, you can see that the cpu reservation increased to 587 millicpu, which is over five times the original value. The memory increased to 262,144 Kilobytes, which is around 250 mebibytes, or five times the original value. This Pod was under-resourced, and the Vertical Pod Autoscaler corrected the estimate with a much more appropriate value.

6. Describe the hamster-vpa resource to view the new recommendation.

```
kubectl describe vpa/hamster-vpa
```

An example output is as follows.

```

Name:        hamster-vpa
Namespace:   default
Labels:      <none>
Annotations: kubectl.kubernetes.io/last-applied-configuration:
             {"apiVersion":"autoscaling.k8s.io/v1beta2","kind":"VerticalPodAutoscaler","metadata":{"annotations":{},"name":"hamster-vpa","namespace":"d...}}
API Version: autoscaling.k8s.io/v1beta2
Kind:        VerticalPodAutoscaler
Metadata:
  Creation Timestamp: 2019-09-27T18:22:51Z
  Generation:        23
  Resource Version:  14411
  Self Link:         /apis/autoscaling.k8s.io/v1beta2/namespaces/default/verticalpodautoscalers/hamster-vpa
  UID:               d0d85fb9-e153-11e9-ae53-0205785d75b0
Spec:
  Target Ref:
    API Version:  apps/v1
    Kind:         Deployment
    Name:         hamster
Status:
  Conditions:
    Last Transition Time: 2019-09-27T18:23:28Z
    Status:        True
    Type:          RecommendationProvided
  Recommendation:
    Container Recommendations:
      Container Name: hamster
      Lower Bound:
        Cpu:      550m
        Memory:  262144k
      Target:
        Cpu:      587m
        Memory:  262144k
      Uncapped Target:
        Cpu:      587m

```

```
Memory: 262144k
Upper Bound:
Cpu: 21147m
Memory: 387863636
Events: <none>
```

- When you finish experimenting with the example application, you can delete it with the following command.

```
kubectl delete -f examples/hamster.yaml
```

Horizontal Pod Autoscaler

The Kubernetes [Horizontal Pod Autoscaler](#) automatically scales the number of Pods in a deployment, replication controller, or replica set based on that resource's CPU utilization. This can help your applications scale out to meet increased demand or scale in when resources are not needed, thus freeing up your nodes for other applications. When you set a target CPU utilization percentage, the Horizontal Pod Autoscaler scales your application in or out to try to meet that target.

The Horizontal Pod Autoscaler is a standard API resource in Kubernetes that simply requires that a metrics source (such as the Kubernetes metrics server) is installed on your Amazon EKS cluster to work. You do not need to deploy or install the Horizontal Pod Autoscaler on your cluster to begin scaling your applications. For more information, see [Horizontal Pod Autoscaler](#) in the Kubernetes documentation.

Use this topic to prepare the Horizontal Pod Autoscaler for your Amazon EKS cluster and to verify that it is working with a sample application.

Note

This topic is based on the [Horizontal Pod autoscaler walkthrough](#) in the Kubernetes documentation.

Prerequisites

- You have an existing Amazon EKS cluster. If you don't, see [Getting started with Amazon EKS \(p. 6\)](#).
- You have the Kubernetes Metrics Server installed. For more information, see [Installing the Kubernetes Metrics Server \(p. 450\)](#).
- You are using a `kubectl` client that is [configured to communicate with your Amazon EKS cluster \(p. 19\)](#).

Run a Horizontal Pod Autoscaler test application

In this section, you deploy a sample application to verify that the Horizontal Pod Autoscaler is working.

Note

This example is based on the [Horizontal Pod autoscaler walkthrough](#) in the Kubernetes documentation.

To test your Horizontal Pod Autoscaler installation

- Deploy a simple Apache web server application with the following command.

```
kubectl apply -f https://k8s.io/examples/application/php-apache.yaml
```

This Apache web server Pod is given a 500 millicpu CPU limit and it is serving on port 80.

2. Create a Horizontal Pod Autoscaler resource for the php-apache deployment.

```
kubectl autoscale deployment php-apache --cpu-percent=50 --min=1 --max=10
```

This command creates an autoscaler that targets 50 percent CPU utilization for the deployment, with a minimum of one Pod and a maximum of ten Pods. When the average CPU load is lower than 50 percent, the autoscaler tries to reduce the number of Pods in the deployment, to a minimum of one. When the load is greater than 50 percent, the autoscaler tries to increase the number of Pods in the deployment, up to a maximum of ten. For more information, see [How does a HorizontalPodAutoscaler work?](#) in the Kubernetes documentation.

3. Describe the autoscaler with the following command to view its details.

```
kubectl get hpa
```

An example output is as follows.

NAME	REFERENCE	TARGETS	MINPODS	MAXPODS	REPLICAS	AGE
php-apache	Deployment/php-apache	0%/50%	1	10	1	51s

As you can see, the current CPU load is 0%, because there's no load on the server yet. The Pod count is already at its lowest boundary (one), so it cannot scale in.

4. Create a load for the web server by running a container.

```
kubectl run -i \
    --tty load-generator \
    --rm --image=busybox \
    --restart=Never \
    -- /bin/sh -c "while sleep 0.01; do wget -q -O- http://php-apache; done"
```

5. To watch the deployment scale out, periodically run the following command in a separate terminal from the terminal that you ran the previous step in.

```
kubectl get hpa php-apache
```

An example output is as follows.

NAME	REFERENCE	TARGETS	MINPODS	MAXPODS	REPLICAS	AGE
php-apache	Deployment/php-apache	250%/50%	1	10	5	4m44s

It may take over a minute for the replica count to increase. As long as actual CPU percentage is higher than the target percentage, then the replica count increases, up to 10. In this case, it's 250%, so the number of REPLICAS continues to increase.

Note

It may take a few minutes before you see the replica count reach its maximum. If only 6 replicas, for example, are necessary for the CPU load to remain at or under 50%, then the load won't scale beyond 6 replicas.

6. Stop the load. In the terminal window you're generating the load in, stop the load by holding down the `Ctrl+C` keys. You can watch the replicas scale back to 1 by running the following command again in the terminal that you're watching the scaling in.

```
kubectl get hpa
```

An example output is as follows.

NAME	REFERENCE	TARGETS	MINPODS	MAXPODS	REPLICAS	AGE
php-apache	Deployment/php-apache	0%/50%	1	10	1	25m

Note

The default timeframe for scaling back down is five minutes, so it will take some time before you see the replica count reach 1 again, even when the current CPU percentage is 0 percent. The timeframe is modifiable. For more information, see [Horizontal Pod Autoscaler](#) in the Kubernetes documentation.

- When you are done experimenting with your sample application, delete the php-apache resources.

```
kubectl delete deployment.apps/php-apache service/php-apache
horizontalpodautoscaler.autoscaling/php-apache
```

Network load balancing on Amazon EKS

Network traffic is load balanced at L4 of the OSI model. To load balance application traffic at L7, you deploy a Kubernetes ingress, which provisions an AWS Application Load Balancer. For more information, see [Application load balancing on Amazon EKS \(p. 375\)](#). To learn more about the differences between the two types of load balancing, see [Elastic Load Balancing features](#) on the AWS website.

When you create a Kubernetes Service of type LoadBalancer, the AWS cloud provider load balancer controller creates AWS [Classic Load Balancers](#) by default, but can also create AWS [Network Load Balancers](#). This controller is only receiving critical bug fixes in the future. For more information about using the AWS cloud provider load balancer, see [AWS cloud provider load balancer controller](#) in the Kubernetes documentation. Its use is not covered in this topic.

We recommend that you use version 2.5.4 or later of the [AWS Load Balancer Controller \(p. 333\)](#) instead of the AWS cloud provider load balancer controller. The AWS Load Balancer Controller creates AWS Network Load Balancers, but doesn't create AWS Classic Load Balancers. The remainder of this topic is about using the AWS Load Balancer Controller.

An AWS Network Load Balancer can load balance network traffic to Pods deployed to Amazon EC2 IP and instance [targets](#) or to AWS Fargate IP targets. For more information, see [AWS Load Balancer Controller](#) on GitHub.

Prerequisites

Before you can load balance network traffic using the AWS Load Balancer Controller, you must meet the following requirements.

- Have an existing cluster. If you don't have an existing cluster, see [Getting started with Amazon EKS \(p. 6\)](#). If you need to update the version of an existing cluster, see [Updating an Amazon EKS cluster Kubernetes version \(p. 34\)](#).
- Have the AWS Load Balancer Controller deployed on your cluster. For more information, see [Installing the AWS Load Balancer Controller add-on \(p. 333\)](#). We recommend version 2.5.4 or later.
- At least one subnet. If multiple tagged subnets are found in an Availability Zone, the controller chooses the first subnet whose subnet ID comes first lexicographically. The subnet must have at least eight available IP addresses.
- If you're using the AWS Load Balancer Controller version 2.1.1 or earlier, subnets must be tagged as follows. If using version 2.1.2 or later, this tag is optional. You might want to tag a subnet if you have multiple clusters running in the same VPC, or multiple AWS services sharing subnets in a VPC, and want more control over where load balancers are provisioned for each cluster. If you explicitly specify subnet IDs as an annotation on a service object, then Kubernetes and the AWS Load Balancer

Controller use those subnets directly to create the load balancer. Subnet tagging isn't required if you choose to use this method for provisioning load balancers and you can skip the following private and public subnet tagging requirements. Replace *my-cluster* with your cluster name.

- **Key** – kubernetes.io/cluster/*my-cluster*
- **Value** – shared or owned
- Your public and private subnets must meet the following requirements, unless you explicitly specify subnet IDs as an annotation on a service or ingress object. If you provision load balancers by explicitly specifying subnet IDs as an annotation on a service or ingress object, then Kubernetes and the AWS Load Balancer Controller use those subnets directly to create the load balancer and the following tags aren't required.
 - **Private subnets** – Must be tagged in the following format. This is so that Kubernetes and the AWS Load Balancer Controller know that the subnets can be used for internal load balancers. If you use eksctl or an Amazon EKS AWS CloudFormation template to create your VPC after March 26, 2020, then the subnets are tagged appropriately when they're created. For more information about the Amazon EKS AWS CloudFormation VPC templates, see [Creating a VPC for your Amazon EKS cluster \(p. 259\)](#).
 - **Key** – kubernetes.io/role/internal-elb
 - **Value** – 1
 - **Public subnets** – Must be tagged in the following format. This is so that Kubernetes knows to use only those subnets for external load balancers instead of choosing a public subnet in each Availability Zone (based on the lexicographical order of the subnet IDs). If you use eksctl or an Amazon EKS AWS CloudFormation template to create your VPC after March 26, 2020, then the subnets are tagged appropriately when they're created. For more information about the Amazon EKS AWS CloudFormation VPC templates, see [Creating a VPC for your Amazon EKS cluster \(p. 259\)](#).
 - **Key** – kubernetes.io/role/elb
 - **Value** – 1

If the subnet role tags aren't explicitly added, the Kubernetes service controller examines the route table of your cluster VPC subnets to determine if the subnet is private or public. We recommend that you don't rely on this behavior, and instead explicitly add the private or public role tags. The AWS Load Balancer Controller doesn't examine route tables, and requires the private and public tags to be present for successful auto discovery.

Considerations

- The configuration of your load balancer is controlled by annotations that are added to the manifest for your service. Service annotations are different when using the AWS Load Balancer Controller than they are when using the AWS cloud provider load balancer controller. Make sure to review the [annotations](#) for the AWS Load Balancer Controller before deploying services.
- When using the [Amazon VPC CNI plugin for Kubernetes \(p. 266\)](#), the AWS Load Balancer Controller can load balance to Amazon EC2 IP or instance targets and Fargate IP targets. When using [Alternate compatible CNI plugins \(p. 332\)](#), the controller can only load balance to instance targets. For more information about Network Load Balancer target types, see [Target type](#) in the User Guide for Network Load Balancers
- If you want to add tags to the load balancer when or after it's created, add the following annotation in your service specification. For more information, see [AWS Resource Tags](#) in the AWS Load Balancer Controller documentation.

```
service.beta.kubernetes.io/aws-load-balancer-additional-resource-tags
```

- You can assign [Elastic IP addresses](#) to the Network Load Balancer by adding the following annotation. Replace the *example values* with the Allocation IDs of your Elastic IP addresses. The number of Allocation IDs must match the number of subnets that are used for the load balancer. For more information, see the [AWS Load Balancer Controller](#) documentation.

```
service.beta.kubernetes.io/aws-load-balancer-eip-allocations:  
eipalloc-xxxxxxxxxxxxxxxxxx,eipalloc-yyyyyyyyyyyyyyyyy
```

- Amazon EKS adds one inbound rule to the node's security group for client traffic and one rule for each load balancer subnet in the VPC for health checks for each Network Load Balancer that you create. Deployment of a service of type LoadBalancer can fail if Amazon EKS attempts to create rules that exceed the quota for the maximum number of rules allowed for a security group. For more information, see [Security groups](#) in Amazon VPC quotas in the Amazon VPC User Guide. Consider the following options to minimize the chances of exceeding the maximum number of rules for a security group:
 - Request an increase in your rules per security group quota. For more information, see [Requesting a quota increase](#) in the Service Quotas User Guide.
 - Use IP targets, rather than instance targets. With IP targets, you can share rules for the same target ports. You can manually specify load balancer subnets with an annotation. For more information, see [Annotations](#) on GitHub.
 - Use an ingress, instead of a service of type LoadBalancer, to send traffic to your service. The AWS Application Load Balancer requires fewer rules than Network Load Balancers. You can share an ALB across multiple ingresses. For more information, see [Application load balancing on Amazon EKS \(p. 375\)](#). You can't share a Network Load Balancer across multiple services.
 - Deploy your clusters to multiple accounts.
- If your Pods run on Windows in an Amazon EKS cluster, a single service with a load balancer can support up to 1024 back-end Pods. Each Pod has its own unique IP address.
- We recommend only creating new Network Load Balancers with the AWS Load Balancer Controller. Attempting to replace existing Network Load Balancers created with the AWS cloud provider load balancer controller can result in multiple Network Load Balancers that might cause application downtime.

Create a network load balancer

You can create a network load balancer with IP or instance targets.

IP targets

You can use IP targets with Pods deployed to Amazon EC2 nodes or Fargate. Your Kubernetes service must be created as type LoadBalancer. For more information, see [Type LoadBalancer](#) in the Kubernetes documentation.

To create a load balancer that uses IP targets, add the following annotations to a service manifest and deploy your service. The external value for aws-load-balancer-type is what causes the AWS Load Balancer Controller, rather than the AWS cloud provider load balancer controller, to create the Network Load Balancer. You can view a [sample service manifest \(p. 374\)](#) with the annotations.

```
service.beta.kubernetes.io/aws-load-balancer-type: "external"  
service.beta.kubernetes.io/aws-load-balancer-nlb-target-type: "ip"
```

Note

If you're load balancing to IPv6 Pods, add the following annotation. You can only load balance over IPv6 to IP targets, not instance targets. Without this annotation, load balancing is over IPv4.

```
service.beta.kubernetes.io/aws-load-balancer-ip-address-type: dualstack
```

Network Load Balancers are created with the `internal aws-load-balancer-scheme`, by default. You can launch Network Load Balancers in any subnet in your cluster's VPC, including subnets that weren't specified when you created your cluster.

Kubernetes examines the route table for your subnets to identify whether they are public or private. Public subnets have a route directly to the internet using an internet gateway, but private subnets do not.

If you want to create a Network Load Balancer in a public subnet to load balance to Amazon EC2 nodes (Fargate can only be private), specify `internet-facing` with the following annotation:

```
service.beta.kubernetes.io/aws-load-balancer-scheme: "internet-facing"
```

Note

The `service.beta.kubernetes.io/aws-load-balancer-type: "nlb-ip"` annotation is still supported for backwards compatibility. However, we recommend using the previous annotations for new load balancers instead of `service.beta.kubernetes.io/aws-load-balancer-type: "nlb-ip"`.

Important

Do not edit the annotations after creating your service. If you need to modify it, delete the service object and create it again with the desired value for this annotation.

Instance targets

The AWS cloud provider load balancer controller creates Network Load Balancers with instance targets only. Version 2.2.0 and later of the AWS Load Balancer Controller also creates Network Load Balancers with instance targets. We recommend using it, rather than the AWS cloud provider load balancer controller, to create new Network Load Balancers. You can use Network Load Balancer instance targets with Pods deployed to Amazon EC2 nodes, but not to Fargate. To load balance network traffic across Pods deployed to Fargate, you must use IP targets.

To deploy a Network Load Balancer to a private subnet, your service specification must have the following annotations. You can view a [sample service manifest \(p. 374\)](#) with the annotations. The external value for `aws-load-balancer-type` is what causes the AWS Load Balancer Controller, rather than the AWS cloud provider load balancer controller, to create the Network Load Balancer.

```
service.beta.kubernetes.io/aws-load-balancer-type: "external"
service.beta.kubernetes.io/aws-load-balancer-nlb-target-type: "instance"
```

Network Load Balancers are created with the `internal aws-load-balancer-scheme`, by default. For internal Network Load Balancers, your Amazon EKS cluster must be configured to use at least one private subnet in your VPC. Kubernetes examines the route table for your subnets to identify whether they are public or private. Public subnets have a route directly to the internet using an internet gateway, but private subnets do not.

If you want to create an Network Load Balancer in a public subnet to load balance to Amazon EC2 nodes, specify `internet-facing` with the following annotation:

```
service.beta.kubernetes.io/aws-load-balancer-scheme: "internet-facing"
```

Important

Do not edit the annotations after creating your service. If you need to modify it, delete the service object and create it again with the desired value for this annotation.

(Optional) Deploy a sample application

Prerequisites

- At least one public or private subnet in your cluster VPC.
- Have the AWS Load Balancer Controller deployed on your cluster. For more information, see [Installing the AWS Load Balancer Controller add-on \(p. 333\)](#). We recommend version 2.5.4 or later.

To deploy a sample application

1. If you're deploying to Fargate, make sure you have an available private subnet in your VPC and create a Fargate profile. If you're not deploying to Fargate, skip this step. You can create the profile by running the following command or in the [AWS Management Console \(p. 138\)](#) using the same values for name and namespace that are in the command. Replace the *example values* with your own.

```
eksctl create fargateprofile \
  --cluster my-cluster \
  --region region-code \
  --name nlb-sample-app \
  --namespace nlb-sample-app
```

2. Deploy a sample application.
 - a. Create a namespace for the application.

```
kubectl create namespace nlb-sample-app
```

- b. Save the following contents to a file named *sample-deployment.yaml* file on your computer.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nlb-sample-app
  namespace: nlb-sample-app
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
        - name: nginx
          image: public.ecr.aws/nginx/nginx:1.23
          ports:
            - name: tcp
              containerPort: 80
```

- c. Apply the manifest to the cluster.

```
kubectl apply -f sample-deployment.yaml
```

3. Create a service with an internet-facing Network Load Balancer that load balances to IP targets.

- a. Save the following contents to a file named `sample-service.yaml` on your computer. If you're deploying to Fargate nodes, remove the `service.beta.kubernetes.io/aws-load-balancer-scheme: internet-facing` line.

```
apiVersion: v1
kind: Service
metadata:
  name: nlb-sample-service
  namespace: nlb-sample-app
  annotations:
    service.beta.kubernetes.io/aws-load-balancer-type: external
    service.beta.kubernetes.io/aws-load-balancer-nlb-target-type: ip
    service.beta.kubernetes.io/aws-load-balancer-scheme: internet-facing
spec:
  ports:
    - port: 80
      targetPort: 80
      protocol: TCP
    type: LoadBalancer
  selector:
    app: nginx
```

- b. Apply the manifest to the cluster.

```
kubectl apply -f sample-service.yaml
```

4. Verify that the service was deployed.

```
kubectl get svc nlb-sample-service -n nlb-sample-app
```

An example output is as follows.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
<code>sample-service</code>	LoadBalancer	<code>10.100.240.137</code>	<code>k8s-nlbsmpl-nlbsmpl-xxxxxxxxxx-xxxxxxxxxxxxxx.elb.region-code.amazonaws.com</code>		
		<code>80:32400/TCP</code>		16h	

Note

The values for `10.100.240.137` and `xxxxxxxxxx-xxxxxxxxxxxxxx` will be different than the example output (they will be unique to your load balancer) and `us-west-2` may be different for you, depending on which AWS Region that your cluster is in.

5. Open the [Amazon EC2 AWS Management Console](#). Select **Target Groups** (under **Load Balancing**) in the left navigation pane. In the **Name** column, select the target group's name where the value in the **Load balancer** column matches a portion of the name in the **EXTERNAL-IP** column of the output in the previous step. For example, you'd select the target group named `k8s-default-samplese-xxxxxxxxxx` if your output were the same as the previous output. The **Target type** is IP because that was specified in the sample service manifest.
6. Select the **Target group** and then select the **Targets** tab. Under **Registered targets**, you should see three IP addresses of the three replicas deployed in a previous step. Wait until the status of all targets is **healthy** before continuing. It might take several minutes before all targets are healthy. The targets might be in an unhealthy state before changing to a healthy state.
7. Send traffic to the service replacing `xxxxxxxxxx-xxxxxxxxxxxxxx` and `us-west-2` with the values returned in the output for a [previous step \(p. 374\)](#) for EXTERNAL-IP. If you deployed to a private subnet, then you'll need to view the page from a device within your VPC, such as a bastion host. For more information, see [Linux Bastion Hosts on AWS](#).

```
curl k8s-default-sample-e-xxxxxxxxxx-xxxxxxxxxxxxxx.elb.region-code.amazonaws.com
```

An example output is as follows.

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
[...]
```

- When you're finished with the sample deployment, service, and namespace, remove them.

```
kubectl delete namespace nlb-sample-app
```

Application load balancing on Amazon EKS

When you create a Kubernetes ingress, an AWS Application Load Balancer (ALB) is provisioned that load balances application traffic. To learn more, see [What is an Application Load Balancer?](#) in the [Application Load Balancers User Guide](#) and [Ingress](#) in the Kubernetes documentation. ALBs can be used with Pods that are deployed to nodes or to AWS Fargate. You can deploy an ALB to public or private subnets.

Application traffic is balanced at L7 of the OSI model. To load balance network traffic at L4, you deploy a Kubernetes service of the LoadBalancer type. This type provisions an AWS Network Load Balancer. For more information, see [Network load balancing on Amazon EKS \(p. 369\)](#). To learn more about the differences between the two types of load balancing, see [Elastic Load Balancing features](#) on the AWS website.

Prerequisites

Before you can load balance application traffic to an application, you must meet the following requirements.

- Have an existing cluster. If you don't have an existing cluster, see [Getting started with Amazon EKS \(p. 6\)](#). If you need to update the version of an existing cluster, see [Updating an Amazon EKS cluster Kubernetes version \(p. 34\)](#).
- Have the AWS Load Balancer Controller deployed on your cluster. For more information, see [Installing the AWS Load Balancer Controller add-on \(p. 333\)](#). We recommend version 2.5.4 or later.
- At least two subnets in different Availability Zones. The AWS Load Balancer Controller chooses one subnet from each Availability Zone. When multiple tagged subnets are found in an Availability Zone, the controller chooses the subnet whose subnet ID comes first lexicographically. Each subnet must have at least eight available IP addresses.

If you're using multiple security groups attached to worker node, exactly one security group must be tagged as follows. Replace **my-cluster** with your cluster name.

- Key** – kubernetes.io/cluster/**my-cluster**
- Value** – shared or owned
- If you're using the AWS Load Balancer Controller version 2.1.1 or earlier, subnets must be tagged in the format that follows. If you're using version 2.1.2 or later, tagging is optional. However, we recommend that you tag a subnet if any of the following is the case. You have multiple clusters that are running in the same VPC, or have multiple AWS services that share subnets in a VPC. Or, you want more control over where load balancers are provisioned for each cluster. Replace **my-cluster** with your cluster name.

- **Key** – `kubernetes.io/cluster/my-cluster`
- **Value** – shared or owned
- Your public and private subnets must meet the following requirements. This is unless you explicitly specify subnet IDs as an annotation on a service or ingress object. Assume that you provision load balancers by explicitly specifying subnet IDs as an annotation on a service or ingress object. In this situation, Kubernetes and the AWS load balancer controller use those subnets directly to create the load balancer and the following tags aren't required.
 - **Private subnets** – Must be tagged in the following format. This is so that Kubernetes and the AWS load balancer controller know that the subnets can be used for internal load balancers. If you use `eksctl` or an Amazon EKS AWS CloudFormation template to create your VPC after March 26, 2020, the subnets are tagged appropriately when created. For more information about the Amazon EKS AWS CloudFormation VPC templates, see [Creating a VPC for your Amazon EKS cluster \(p. 259\)](#).
 - **Key** – `kubernetes.io/role/internal-elb`
 - **Value** – 1
 - **Public subnets** – Must be tagged in the following format. This is so that Kubernetes knows to use only the subnets that were specified for external load balancers. This way, Kubernetes doesn't choose a public subnet in each Availability Zone (lexicographically based on their subnet ID). If you use `eksctl` or an Amazon EKS AWS CloudFormation template to create your VPC after March 26, 2020, the subnets are tagged appropriately when created. For more information about the Amazon EKS AWS CloudFormation VPC templates, see [Creating a VPC for your Amazon EKS cluster \(p. 259\)](#).
 - **Key** – `kubernetes.io/role/elb`
 - **Value** – 1

If the subnet role tags aren't explicitly added, the Kubernetes service controller examines the route table of your cluster VPC subnets. This is to determine if the subnet is private or public. We recommend that you don't rely on this behavior. Rather, explicitly add the private or public role tags. The AWS Load Balancer Controller doesn't examine route tables. It also requires the private and public tags to be present for successful auto discovery.

Considerations

- The [AWS Load Balancer Controller](#) creates ALBs and the necessary supporting AWS resources whenever a Kubernetes ingress resource is created on the cluster with the `kubernetes.io/ingress.class: alb` annotation. The ingress resource configures the ALB to route HTTP or HTTPS traffic to different Pods within the cluster. To ensure that your ingress objects use the AWS Load Balancer Controller, add the following annotation to your Kubernetes ingress specification. For more information, see [Ingress specification](#) on GitHub.

```
annotations:  
  kubernetes.io/ingress.class: alb
```

Note

If you're load balancing to IPv6 Pods, add the following annotation to your ingress spec. You can only load balance over IPv6 to IP targets, not instance targets. Without this annotation, load balancing is over IPv4.

```
alb.ingress.kubernetes.io/ip-address-type: dualstack
```

- The AWS Load Balancer Controller supports the following traffic modes:
 - **Instance** – Registers nodes within your cluster as targets for the ALB. Traffic reaching the ALB is routed to NodePort for your service and then proxied to your Pods. This is the default traffic mode. You can also explicitly specify it with the `alb.ingress.kubernetes.io/target-type: instance` annotation.

Note

Your Kubernetes service must specify the NodePort or "LoadBalancer" type to use this traffic mode.

- **IP** – Registers Pods as targets for the ALB. Traffic reaching the ALB is directly routed to Pods for your service. You must specify the `alb.ingress.kubernetes.io/target-type: ip` annotation to use this traffic mode. The IP target type is required when target Pods are running on Fargate.
- To tag ALBs created by the controller, add the following annotation to the controller: `alb.ingress.kubernetes.io/tags`. For a list of all available annotations supported by the AWS Load Balancer Controller, see [Ingress annotations](#) on GitHub.
- Upgrading or downgrading the ALB controller version can introduce breaking changes for features that rely on it. For more information about the breaking changes that are introduced in each release, see the [ALB controller release notes](#) on GitHub.

To share an application load balancer across multiple service resources using IngressGroups

To join an ingress to a group, add the following annotation to a Kubernetes ingress resource specification.

```
alb.ingress.kubernetes.io/group.name: my-group
```

The group name must:

- Be 63 or fewer characters in length.
- Consist of lower case letters, numbers, -, and .
- Start and end with a letter or number.

The controller automatically merges ingress rules for all ingresses in the same ingress group. It supports them with a single ALB. Most annotations that are defined on an ingress only apply to the paths defined by that ingress. By default, ingress resources don't belong to any ingress group.

Warning

Potential security risk: Specify an ingress group for an ingress only when all the Kubernetes users that have RBAC permission to create or modify ingress resources are within the same trust boundary. If you add the annotation with a group name, other Kubernetes users might create or modify their ingresses to belong to the same ingress group. Doing so can cause undesirable behavior, such as overwriting existing rules with higher priority rules.

You can add an order number of your ingress resource.

```
alb.ingress.kubernetes.io/group.order: '10'
```

The number can be 1-1000. The lowest number for all ingresses in the same ingress group is evaluated first. All ingresses without this annotation are evaluated with a value of zero. Duplicate rules with a higher number can overwrite rules with a lower number. By default, the rule order between ingresses within the same ingress group is determined lexicographically based namespace and name.

Important

Ensure that each ingress in the same ingress group has a unique priority number. You can't have duplicate order numbers across ingresses.

(Optional) Deploy a sample application

Prerequisites

- At least one public or private subnet in your cluster VPC.

- Have the AWS Load Balancer Controller deployed on your cluster. For more information, see [Installing the AWS Load Balancer Controller add-on \(p. 333\)](#). We recommend version 2.5.4 or later.

To deploy a sample application

You can run the sample application on a cluster that has Amazon EC2 nodes, Fargate Pods, or both.

1. If you're not deploying to Fargate, skip this step. If you're deploying to Fargate, create a Fargate profile. You can create the profile by running the following command or in the [AWS Management Console \(p. 138\)](#) using the same values for name and namespace that are in the command. Replace the *example values* with your own.

```
eksctl create fargateprofile \
    --cluster my-cluster \
    --region region-code \
    --name alb-sample-app \
    --namespace game-2048
```

2. Deploy the game [2048](#) as a sample application to verify that the AWS Load Balancer Controller creates an AWS ALB as a result of the ingress object. Complete the steps for the type of subnet you're deploying to.
 - a. If you're deploying to Pods in a cluster that you created with the IPv6 family, skip to the next step.

- **Public**

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.5.4/docs/examples/2048/2048_full.yaml
```

- **Private**

1. Download the manifest.

```
curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.5.4/docs/examples/2048/2048_full.yaml
```

2. Edit the file and find the line that says `alb.ingress.kubernetes.io/scheme: internet-facing`.
3. Change *internet-facing* to **internal** and save the file.
4. Apply the manifest to your cluster.

```
kubectl apply -f 2048_full.yaml
```

- b. If you're deploying to Pods in a cluster that you created with the [IPv6 family \(p. 278\)](#), complete the following steps.

1. Download the manifest.

```
curl -O https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.5.4/docs/examples/2048/2048_full.yaml
```

2. Open the file in an editor and add the following line to the annotations in the ingress spec.

```
alb.ingress.kubernetes.io/ip-address-type: dualstack
```

3. If you're load balancing to internal Pods, rather than internet facing Pods, change the line that says `alb.ingress.kubernetes.io/scheme`: `internet-facing` to `alb.ingress.kubernetes.io/scheme: internal`
4. Save the file.
5. Apply the manifest to your cluster.

```
kubectl apply -f 2048_full.yaml
```

3. After a few minutes, verify that the ingress resource was created with the following command.

```
kubectl get ingress/ingress-2048 -n game-2048
```

An example output is as follows.

NAME	CLASS	HOSTS	ADDRESS	PORTS	AGE
ingress-2048	<none>	*	k8s-game2048-ingress2-xxxxxxxxxx-yyyyyyyyyyyy.region-code.elb.amazonaws.com	80	2m32s

Note

If you created the load balancer in a private subnet, the value under ADDRESS in the previous output is prefaced with `internal-`.

If your ingress wasn't successfully created after several minutes, run the following command to view the AWS Load Balancer Controller logs. These logs might contain error messages that you can use to diagnose issues with your deployment.

```
kubectl logs -f -n kube-system -l app.kubernetes.io/instance=aws-load-balancer-controller
```

4. If you deployed to a public subnet, open a browser and navigate to the ADDRESS URL from the previous command output to see the sample application. If you don't see anything, refresh your browser and try again. If you deployed to a private subnet, then you'll need to view the page from a device within your VPC, such as a bastion host. For more information, see [Linux Bastion Hosts on AWS](#).
5. When you finish experimenting with your sample application, delete it by running one of the the following commands.
 - If you applied the manifest, rather than applying a copy that you downloaded, use the following command.

```
kubectl delete -f https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.5.4/docs/examples/2048/2048_full.yaml
```

- If you downloaded and edited the manifest, use the following command.

```
kubectl delete -f 2048_full.yaml
```

Restricting external IP addresses that can be assigned to services

Kubernetes services can be reached from inside of a cluster through:

- A cluster IP address that is assigned automatically by Kubernetes
- Any IP address that you specify for the `externalIPs` property in a service spec. External IP addresses are not managed by Kubernetes and are the responsibility of the cluster administrator. External IP addresses specified with `externalIPs` are different than the external IP address assigned to a service of type `LoadBalancer` by a cloud provider.

To learn more about Kubernetes services, see [Service](#) in the Kubernetes documentation. You can restrict the IP addresses that can be specified for `externalIPs` in a service spec.

To restrict the IP addresses that can be specified for `externalIPs` in a service spec

1. Deploy `cert-manager` to manage webhook certificates. For more information, see the [cert-manager](#) documentation.

```
kubectl apply -f https://github.com/jetstack/cert-manager/releases/download/v1.5.4/cert-manager.yaml
```

2. Verify that the `cert-manager` Pods are running.

```
kubectl get pods -n cert-manager
```

An example output is as follows.

NAME	READY	STATUS	RESTARTS	AGE
cert-manager-58c8844bb8-nlx7q	1/1	Running	0	15s
cert-manager-cainjector-745768f6ff-696h5	1/1	Running	0	15s
cert-manager-webhook-67cc76975b-4v4nk	1/1	Running	0	14s

3. Review your existing services to ensure that none of them have external IP addresses assigned to them that aren't contained within the CIDR block you want to limit addresses to.

```
kubectl get services -A
```

An example output is as follows.

NAMESPACE	CLUSTER-IP	EXTERNAL-IP	NAME	PORT(S)	AGE	TYPE
cert-manager	10.100.102.137	<none>	cert-manager	9402/TCP	20m	ClusterIP
cert-manager	10.100.6.136	<none>	cert-manager-webhook	443/TCP	20m	ClusterIP
default	10.100.0.1	<none>	kubernetes	443/TCP	2d1h	ClusterIP
externalip-validation-system	10.100.234.179	<none>	externalip-validation-webhook-service	443/TCP	16s	ClusterIP
kube-system	10.100.0.10	<none>	kube-dns	53/UDP, 53/TCP	2d1h	ClusterIP
my-namespace	10.100.128.10	192.168.1.1	my-service	80/TCP	149m	ClusterIP

If any of the values are IP addresses that are not within the block you want to restrict access to, you'll need to change the addresses to be within the block, and redeploy the services. For example, the `my-service` service in the previous output has an external IP address assigned to it that isn't within the CIDR block example in step 5.

4. Download the external IP webhook manifest. You can also view the [source code for the webhook](#) on GitHub.

```
curl -0 https://s3.us-west-2.amazonaws.com/amazon-eks/docs/externalip-webhook.yaml
```

5.

Specify CIDR blocks. Open the downloaded file in your editor and remove the # at the start of the following lines.

```
#args:  
#- --allowed-external-ip-cidrs=10.0.0.0/8
```

Replace 10.0.0.0/8 with your own CIDR block. You can specify as many blocks as you like. If specifying multiple blocks, add a comma between blocks.

6.

If your cluster is not in the us-west-2 AWS Region, then replace us-west-2, 602401143452, and amazonaws.com in the file with the following commands. Before running the commands, replace *region-code* and *111122223333* with the value for your AWS Region from the list in [Amazon container image registries \(p. 383\)](#).

```
sed -i.bak -e 's|602401143452|111122223333|' externalip-webhook.yaml  
sed -i.bak -e 's|us-west-2|region-code|' externalip-webhook.yaml  
sed -i.bak -e 's|amazonaws.com||' externalip-webhook.yaml
```

7. Apply the manifest to your cluster.

```
kubectl apply -f externalip-webhook.yaml
```

An attempt to deploy a service to your cluster with an IP address specified for externalIPs that is not contained in the blocks that you specified in the [Specify CIDR blocks \(p. 381\)](#) step will fail.

Copy a container image from one repository to another repository

This topic describes how to pull a container image from a repository that your nodes don't have access to and push the image to a repository that your nodes have access to. You can push the image to Amazon ECR or an alternative repository that your nodes have access to.

Prerequisites

- The Docker engine installed and configured on your computer. For instructions, see [Install Docker Engine](#) in the Docker documentation.
- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with aws --version | cut -d / -f2 | cut -d ' ' -f1. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.
- An interface VPC endpoint for Amazon ECR if you want your nodes to pull container images from or push container images to a private Amazon ECR repository over Amazon's network. For more information, see [Create the VPC endpoints for Amazon ECR](#) in the Amazon Elastic Container Registry User Guide.

Complete the following steps to pull a container image from a repository and push it to your own repository. In the following examples that are provided in this topic, the image for the [Amazon VPC CNI plugin for Kubernetes metrics helper](#) is pulled. When you follow these steps, make sure to replace the *example values* with your own values.

To copy a container image from one repository to another repository

1. If you don't already have an Amazon ECR repository or another repository, then create one that your nodes have access to. The following command creates an Amazon ECR private repository. An Amazon ECR private repository name must start with a letter. It can only contain lowercase letters, numbers, hyphens (-), underscores (_), and forward slashes (/). For more information, see [Creating a private repository](#) in the Amazon Elastic Container Registry User Guide.

You can replace *cni-metrics-helper* with whatever you choose. As a best practice, create a separate repository for each image. We recommend this because image tags must be unique within a repository. Replace *region-code* with an [AWS Region supported by Amazon ECR](#).

```
aws ecr create-repository --region region-code --repository-name cni-metrics-helper
```

2. Determine the registry, repository, and tag (optional) of the image that your nodes need to pull. This information is in the `registry/repository[:tag]` format.

Many of the Amazon EKS topics about installing images require that you apply a manifest file or install the image using a Helm chart. However, before you apply a manifest file or install a Helm chart, first view the contents of the manifest or chart's `values.yaml` file. That way, you can determine the registry, repository, and tag to pull.

For example, you can find the following line in the [manifest file](#) for the [Amazon VPC CNI plugin for Kubernetes metrics helper](#). The registry is `602401143452.dkr.ecr.us-west-2.amazonaws.com`, which is an Amazon ECR private registry. The repository is `cni-metrics-helper`.

```
image: "602401143452.dkr.ecr.us-west-2.amazonaws.com/cni-metrics-helper:v1.12.6"
```

You may see the following variations for an image location:

- Only `repository-name:tag`. In this case, `docker.io` is usually the registry, but not specified since Kubernetes prepends it to a repository name by default if no registry is specified.
- `repository-name/repository-namespace/repository:tag`. A repository namespace is optional, but is sometimes specified by the repository owner for categorizing images. For example, all [Amazon EC2 images in the Amazon ECR Public Gallery](#) use the `aws-ec2` namespace.

Before installing an image with Helm, view the Helm `values.yaml` file to determine the image location. For example, the `values.yaml` file for the [Amazon VPC CNI plugin for Kubernetes metrics helper](#) includes the following lines.

```
image:  
  region: us-west-2  
  tag: v1.12.6  
  account: "602401143452"  
  domain: "amazonaws.com"
```

3. Pull the container image specified in the manifest file.

- a. If you're pulling from a public registry, such as the [Amazon ECR Public Gallery](#), you can skip to the next sub-step, because authentication isn't required. In this example, you authenticate to an Amazon ECR private registry that contains the repository for the CNI metrics helper

image. Amazon EKS maintains the image in each registry listed in [Amazon container image registries \(p. 383\)](#). You can authenticate to any of the registries by replacing **602401143452** and **region-code** with the information for a different registry. A separate registry exists for each [AWS Region that Amazon EKS is supported in](#).

```
aws ecr get-login-password --region region-code | docker login --username AWS --password-stdin 602401143452.dkr.ecr.region-code.amazonaws.com
```

- b. Pull the image. In this example, you pull from the registry that you authenticated to in the previous sub-step. Replace **602401143452** and **region-code** with the information that you provided in the previous sub-step.

```
docker pull 602401143452.dkr.ecr.region-code.amazonaws.com/cni-metrics-helper:v1.12.6
```

4. Tag the image that you pulled with your registry, repository, and tag. The following example assumes that you pulled the image from the manifest file and are going to push it to the Amazon ECR private repository that you created in the first step. Replace **111122223333** with your account ID. Replace **region-code** with the AWS Region that you created your Amazon ECR private repository in.

```
docker tag cni-metrics-helper:v1.12.6 111122223333.dkr.ecr.region-code.amazonaws.com/cni-metrics-helper:v1.12.6
```

5. Authenticate to your registry. In this example, you authenticate to the Amazon ECR private registry that you created in the first step. For more information, see [Registry authentication](#) in the Amazon Elastic Container Registry User Guide.

```
aws ecr get-login-password --region region-code | docker login --username AWS --password-stdin 111122223333.dkr.ecr.region-code.amazonaws.com
```

6. Push the image to your repository. In this example, you push the image to the Amazon ECR private repository that you created in the first step. For more information, see [Pushing a Docker image](#) in the Amazon Elastic Container Registry User Guide.

```
docker push 111122223333.dkr.ecr.region-code.amazonaws.com/cni-metrics-helper:v1.12.6
```

7. Update the manifest file that you used to determine the image in a previous step with the `registry/repository:tag` for the image that you pushed. If you're installing with a Helm chart, there's often an option to specify the `registry/repository:tag`. When installing the chart, specify the `registry/repository:tag` for the image that you pushed to your repository.

Amazon container image registries

When you deploy [AWS Amazon EKS add-ons \(p. 386\)](#) to your cluster, your nodes pull the required container images from the registry specified in the installation mechanism for the add-on, such as an installation manifest or a Helm values.yaml file. The images are pulled from an Amazon EKS Amazon ECR private repository. Amazon EKS replicates the images to a repository in each Amazon EKS supported AWS Region. Your nodes can pull the container image over the internet from any of the following registries. Alternatively, your nodes can pull the image over Amazon's network if you created an [interface VPC endpoint for Amazon ECR \(AWS PrivateLink\)](#) in your VPC. The registries require authentication with an AWS IAM account. Your nodes authenticate using the [Amazon EKS node IAM role \(p. 501\)](#), which has the permissions in the [AmazonEC2ContainerRegistryReadOnly](#) managed IAM policy associated to it.

AWS Region	Registry
af-south-1	877085696533.dkr.ecr.af-south-1.amazonaws.com
ap-east-1	800184023465.dkr.ecr.ap-east-1.amazonaws.com
ap-northeast-1	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
ap-northeast-2	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
ap-northeast-3	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
ap-south-1	602401143452.dkr.ecr.ap-south-1.amazonaws.com
ap-south-2	900889452093.dkr.ecr.ap-south-2.amazonaws.com
ap-southeast-1	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com
ap-southeast-2	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
ap-southeast-3	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
ap-southeast-4	491585149902.dkr.ecr.ap-southeast-4.amazonaws.com
ca-central-1	602401143452.dkr.ecr.ca-central-1.amazonaws.com
cn-north-1	918309763551.dkr.ecr.cn-north-1.amazonaws.com.cn
cn-northwest-1	961992271922.dkr.ecr.cn-northwest-1.amazonaws.com.cn
eu-central-1	602401143452.dkr.ecr.eu-central-1.amazonaws.com
eu-central-2	900612956339.dkr.ecr.eu-central-2.amazonaws.com
eu-north-1	602401143452.dkr.ecr.eu-north-1.amazonaws.com
eu-south-1	590381155156.dkr.ecr.eu-south-1.amazonaws.com
eu-south-2	455263428931.dkr.ecr.eu-south-2.amazonaws.com
eu-west-1	602401143452.dkr.ecr.eu-west-1.amazonaws.com
eu-west-2	602401143452.dkr.ecr.eu-west-2.amazonaws.com

AWS Region	Registry
eu-west-3	602401143452.dkr.ecr.eu-west-3.amazonaws.com
il-central-1	066635153087.dkr.ecr.il-central-1.amazonaws.com
me-south-1	558608220178.dkr.ecr.me-south-1.amazonaws.com
me-central-1	759879836304.dkr.ecr.me-central-1.amazonaws.com
sa-east-1	602401143452.dkr.ecr.sa-east-1.amazonaws.com
us-east-1	602401143452.dkr.ecr.us-east-1.amazonaws.com
us-east-2	602401143452.dkr.ecr.us-east-2.amazonaws.com
us-gov-east-1	151742754352.dkr.ecr.us-gov-east-1.amazonaws.com
us-gov-west-1	013241004608.dkr.ecr.us-gov-west-1.amazonaws.com
us-west-1	602401143452.dkr.ecr.us-west-1.amazonaws.com
us-west-2	602401143452.dkr.ecr.us-west-2.amazonaws.com

Amazon EKS add-ons

An add-on is software that provides supporting operational capabilities to Kubernetes applications, but is not specific to the application. This includes software like observability agents or Kubernetes drivers that allow the cluster to interact with underlying AWS resources for networking, compute, and storage. Add-on software is typically built and maintained by the Kubernetes community, cloud providers like AWS, or third-party vendors. Amazon EKS automatically installs self-managed add-ons such as the Amazon VPC CNI plugin for Kubernetes, kube-proxy, and CoreDNS for every cluster. You can change the default configuration of the add-ons and update them when desired.

Amazon EKS add-ons provide installation and management of a curated set of add-ons for Amazon EKS clusters. All Amazon EKS add-ons include the latest security patches, bug fixes, and are validated by AWS to work with Amazon EKS. Amazon EKS add-ons allow you to consistently ensure that your Amazon EKS clusters are secure and stable and reduce the amount of work that you need to do in order to install, configure, and update add-ons. If a self-managed add-on, such as kube-proxy is already running on your cluster and is available as an Amazon EKS add-on, then you can install the kube-proxy Amazon EKS add-on to start benefiting from the capabilities of Amazon EKS add-ons.

You can update specific Amazon EKS managed configuration fields for Amazon EKS add-ons through the Amazon EKS API. You can also modify configuration fields not managed by Amazon EKS directly within the Kubernetes cluster once the add-on starts. This includes defining specific configuration fields for an add-on where applicable. These changes are not overridden by Amazon EKS once they are made. This is made possible using the Kubernetes server-side apply feature. For more information, see [Kubernetes field management \(p. 406\)](#).

You can use Amazon EKS add-ons with any Amazon EKS [node type \(p. 77\)](#).

Considerations

- To configure add-ons for the cluster your [IAM principal](#) must have IAM permissions to work with add-ons. For more information, see the actions with Addon in their name in [Actions defined by Amazon Elastic Kubernetes Service](#).
- Amazon EKS add-ons run on the nodes that you provision or configure for your cluster. Node types include Amazon EC2 instances and Fargate.
- You can modify fields that aren't managed by Amazon EKS to customize the installation of an Amazon EKS add-on. For more information, see [Kubernetes field management \(p. 406\)](#).
- If you create a cluster with the AWS Management Console, the Amazon EKS kube-proxy, Amazon VPC CNI plugin for Kubernetes, and CoreDNS Amazon EKS add-ons are automatically added to your cluster. If you use eksctl to create your cluster with a config file, eksctl can also create the cluster with Amazon EKS add-ons. If you create your cluster using eksctl without a config file or with any other tool, the self-managed kube-proxy, Amazon VPC CNI plugin for Kubernetes, and CoreDNS add-ons are installed, rather than the Amazon EKS add-ons. You can either manage them yourself or add the Amazon EKS add-ons manually after cluster creation.
- The `eks:addon-cluster-admin` ClusterRoleBinding binds the `cluster-admin` ClusterRole to the `eks:addon-manager` Kubernetes identity. The role has the necessary permissions for the `eks:addon-manager` identity to create Kubernetes namespaces and install add-ons into namespaces. If the `eks:addon-cluster-admin` ClusterRoleBinding is removed, the Amazon EKS cluster will continue to function, however Amazon EKS is no longer able to manage any add-ons.

You can add, update, or delete Amazon EKS add-ons using the Amazon EKS API, AWS Management Console, AWS CLI, and eksctl. For more information, see [the section called "Managing add-ons" \(p. 393\)](#). You can also create Amazon EKS add-ons using [AWS CloudFormation](#).

Available Amazon EKS add-ons from Amazon EKS

The following Amazon EKS add-ons are available to create on your cluster. You can always view the most current list of available add-ons using eksctl, the AWS Management Console, or the AWS CLI. To see all available add-ons or to install an add-on, see [the section called "Creating an add-on" \(p. 393\)](#). If an add-on requires IAM permissions, then you must have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one, or to create one, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#). You can [update \(p. 400\)](#) or [delete \(p. 404\)](#) an add-on once you've installed it.

Choose an add-on to learn more about it and its installation requirements.

Amazon VPC CNI plugin for Kubernetes

- **Name** – vpc-cni
- **Description** – A [Kubernetes container network interface \(CNI\) plugin](#) that provides native VPC networking for your cluster. The self-managed or managed type of this add-on is installed on each Amazon EC2 node, by default.
- **Required IAM permissions** – This add-on utilizes the [the section called "IAM roles for service accounts" \(p. 464\)](#) capability of Amazon EKS. If your cluster uses the IPv4 family, the permissions in the [AmazonEKS_CNI_Policy](#) are required. If your cluster uses the IPv6 family, you must [create an IAM policy](#) with the permissions in [IPv6 mode](#). You can create an IAM role, attach one of the policies to it, and annotate the Kubernetes service account used by the add-on with the following command.

Replace `my-cluster` with the name of your cluster and `AmazonEKSVPCCNIRole` with the name for your role. If your cluster uses the IPv6 family, then replace `AmazonEKS_CNT_Policy` with the name of the policy that you created. This command requires that you have [eksctl \(p. 13\)](#), installed on your device. If you need to use a different tool to create the role, attach the policy to it,

and annotate the Kubernetes service account, see [the section called "Configuring role and service account" \(p. 466\)](#).

```
eksctl create iamserviceaccount --name aws-node --namespace kube-system --cluster my-cluster --role-name AmazonEKSVPCCNIRole \
--role-only --attach-policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy --approve
```

- **Additional information** – To learn more about the add-on's configurable settings, see [aws-vpc-cni-k8s](#) on GitHub. To learn more about the plugin, see [Proposal: CNI plugin for Kubernetes networking over AWS VPC](#). For more information about creating the add-on, see [the section called "Creating the Amazon EKS add-on" \(p. 267\)](#).
- **Update information** – You can only update one minor version at a time. For example, if your current version is `1.26.x-eksbuild.y` and you want to update to `1.28.x-eksbuild.y`, then you must update your current version to `1.27.x-eksbuild.y` and then update it again to `1.28.x-eksbuild.y`. For more information about updating the add-on, see [the section called "Updating the Amazon EKS add-on" \(p. 269\)](#).

CoreDNS

- **Name** – coredns
- **Description** – A flexible, extensible DNS server that can serve as the Kubernetes cluster DNS. The self-managed or managed type of this add-on was installed, by default, when you created your cluster. When you launch an Amazon EKS cluster with at least one node, two replicas of the CoreDNS image are deployed by default, regardless of the number of nodes deployed in your cluster. The CoreDNS Pods provide name resolution for all Pods in the cluster. You can deploy the CoreDNS Pods to Fargate nodes if your cluster includes an [AWS Fargate profile \(p. 136\)](#) with a namespace that matches the namespace for the CoreDNS deployment.
- **Required IAM permissions** – This add-on doesn't require any permissions.
- **Additional information** – To learn more about CoreDNS, see [Using CoreDNS for Service Discovery](#) and [Customizing DNS Service](#) in the Kubernetes documentation.

Kube-proxy

- **Name** – kube-proxy
- **Description** – Maintains network rules on each Amazon EC2 node. It enables network communication to your Pods. The self-managed or managed type of this add-on is installed on each Amazon EC2 node in your cluster, by default.
- **Required IAM permissions** – This add-on doesn't require any permissions.
- **Additional information** – To learn more about kube-proxy, see [kube-proxy](#) in the Kubernetes documentation.
- **Update information** – Before updating your current version, consider the following requirements:
 - Kube-proxy on an Amazon EKS cluster has the same [compatibility and skew policy as Kubernetes](#).
 - Kube-proxy must be the same minor version as kubelet on your Amazon EC2 nodes.
 - Kube-proxy can't be later than the minor version of your cluster's control plane.
 - The kube-proxy version on your Amazon EC2 nodes can't be more than two minor versions earlier than your control plane. For example, if your control plane is running Kubernetes 1.28, then the kube-proxy minor version can't be earlier than 1.26.
 - If you recently updated your cluster to a new Kubernetes minor version, then update your Amazon EC2 nodes to the same minor version *before* updating kube-proxy to the same minor version as your nodes.

Amazon EBS CSI driver

- **Name** – aws-ebs-csi-driver
- **Description** – A Kubernetes Container Storage Interface (CSI) plugin that provides Amazon EBS storage for your cluster.
- **Required IAM permissions** – This add-on utilizes the [the section called “IAM roles for service accounts” \(p. 464\)](#) capability of Amazon EKS. The permissions in the [AmazonEBSCSIDriverPolicy](#) AWS managed policy are required. You can create an IAM role and attach the managed policy to it with the following command. Replace *my-cluster* with the name of your cluster and *AmazonEKS_EBS_CSI_DriverRole* with the name for your role. This command requires that you have [eksctl \(p. 13\)](#) installed on your device. If you need to use a different tool or you need to use a custom [KMS key](#) for encryption, see [Creating the Amazon EBS CSI driver IAM role \(p. 228\)](#).

```
eksctl create iamserviceaccount \
--name ebs-csi-controller-sa \
--namespace kube-system \
--cluster my-cluster \
--role-name AmazonEKS_EBS_CSI_DriverRole \
--role-only \
--attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy \
--approve
```

- **Additional information** – To learn more about the add-on, see [Amazon EBS CSI driver \(p. 228\)](#).

Amazon EFS CSI driver

Important

The Amazon EFS driver is only available as a self-managed installation in AWS GovCloud (US-East) and AWS GovCloud (US-West). For instructions on how to add it as a self-managed installation, see [Installation](#) on GitHub.

- **Name** – aws-efs-csi-driver
- **Description** – A Kubernetes Container Storage Interface (CSI) plugin that provides Amazon EFS storage for your cluster.
- **Required IAM permissions** – This add-on utilizes the [the section called “IAM roles for service accounts” \(p. 464\)](#) capability of Amazon EKS. The permissions in the [AmazonEFSCSIDriverPolicy](#) AWS managed policy are required. You can create an IAM role and attach the managed policy to it with the following commands. Replace *my-cluster* with the name of your cluster and *AmazonEKS_EFS_CSI_DriverRole* with the name for your role. These commands require that you have [eksctl \(p. 13\)](#) installed on your device. If you need to use a different tool, see [Creating an IAM role \(p. 245\)](#).

```
export cluster_name=my-cluster
export role_name=AmazonEKS_EFS_CSI_DriverRole
eksctl create iamserviceaccount \
--name efs-csi-controller-sa \
--namespace kube-system \
--cluster $cluster_name \
--role-name $role_name \
--role-only \
--attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy \
--approve
eksctl create iamserviceaccount \
--name efs-csi-node-sa \
--namespace kube-system \
--cluster $cluster_name \
--role-name $role_name \
--role-only \
```

```
--attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy \
--approve
$TRUST_POLICY=$(aws iam get-role --role-name $role_name --query
'Role.AssumeRolePolicyDocument' | \
sed -e 's/efs-csi-controller-sa/efs-csi-*/' -e 's/StringEquals/StringLike/')
aws iam update-assume-role-policy --role-name $role_name --policy-document
"$TRUST_POLICY"
```

- **Additional information** – To learn more about the add-on, see [Amazon EFS CSI driver \(p. 244\)](#).

ADOT

- **Name** – adot
- **Description** – The [AWS Distro for OpenTelemetry](#) (ADOT) is a secure, production-ready, AWS supported distribution of the OpenTelemetry project.
- **Required IAM permissions** – This add-on utilizes the [the section called "IAM roles for service accounts" \(p. 464\)](#) capability of Amazon EKS. The permissions in the [AmazonPrometheusRemoteWriteAccess](#), [AWSXrayWriteOnlyAccess](#), and [CloudWatchAgentServerPolicy](#) AWS managed policies are required. You can create an IAM role, attach the managed policies to it, and annotate the Kubernetes service account used by the add-on with the following command. Replace `my-cluster` with the name of your cluster and [AmazonEKS_ADOT_Collector_Role](#) with the name for your role. This command requires that you have [eksctl \(p. 13\)](#) installed on your device. If you need to use a different tool to create the role, attach the policy to it, and annotate the Kubernetes service account, see [the section called "Configuring role and service account" \(p. 466\)](#).

```
eksctl create iamserviceaccount \
--name adot-collector \
--namespace default \
--cluster my-cluster \
--role-name AmazonEKS_ADOT_Collector_Role \
--attach-policy-arn arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess \
--attach-policy-arn arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess \
--attach-policy-arn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy \
--approve
```

- **Additional information** – For more information, see [Getting Started with AWS Distro for OpenTelemetry using EKS Add-Ons](#) in the AWS Distro for OpenTelemetry documentation.
 - ADOT requires that `cert-manager` is deployed on the cluster as a pre-requisite, otherwise this add-on will not work if deployed directly using the [Amazon EKSTerraform](#) 'cluster_addons' property.

Amazon GuardDuty agent

- **Name** – aws-guardduty-agent
- **Description** – Amazon GuardDuty is a security monitoring service that analyzes and processes [foundational data sources](#) including AWS CloudTrail management events and Amazon VPC flow logs. Amazon GuardDuty also processes [features](#), such as Kubernetes audit logs and runtime monitoring.
- **Required IAM permissions** – This add-on doesn't require any permissions.
- **Additional information** – For more information, see [Amazon EKS Protection in Amazon GuardDuty](#).
 - To detect potential security threats in your Amazon EKS clusters, enable Amazon GuardDuty runtime monitoring and deploy the GuardDuty security agent to your Amazon EKS clusters.

Additional Amazon EKS add-ons from independent software vendors

In addition to the previous list of Amazon EKS add-ons, you can also add a wide selection of operational software Amazon EKS add-ons from independent software vendors. Choose an add-on to learn more about it and its installation requirements.

Dynatrace

- **Publisher** – Dynatrace
- **Name** – dynatrace_dynatrace-operator
- **Namespace** – dynatrace
- **Service account name** – A service account isn't used with this add-on.
- **AWS managed IAM policy** – A managed policy isn't used with this add-on.
- **Custom IAM permissions** – Custom permissions aren't used with this add-on.
- **Setup and usage instructions** – See [Kubernetes monitoring](#) in the dynatrace documentation.

Kpow

- **Publisher** – Factorhouse
- **Name** – factorhouse_kpow
- **Namespace** – factorhouse
- **Service account name** – kpow
- **AWS managed IAM policy** – [AWSLicenseManagerConsumptionPolicy](#)
- **Command to create required IAM role** – The following command requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one, or to create one, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#). Replace *my-cluster* with the name of your cluster and *my-kpow-role* with the name for your role. This command requires that you have [eksctl \(p. 13\)](#) installed on your device. If you need to use a different tool to create the role and annotate the Kubernetes service account, see [the section called "Configuring role and service account" \(p. 466\)](#).

```
eksctl create iamserviceaccount --name kpow --namespace factorhouse --cluster my-cluster
  --role-name my-kpow-role \
    --role-only --attach-policy-arn arn:aws:iam::aws:policy/service-role/
AWSLicenseManagerConsumptionPolicy --approve
```

- **Custom IAM permissions** – Custom permissions aren't used with this add-on.
- **Setup and usage instructions** – See [AWS Marketplace LM](#) in the Kpow documentation.

Kubecost

- **Publisher** – Kubecost
- **Name** – kubecost_kubecost
- **Namespace** – kubecost
- **Service account name** – A service account isn't used with this add-on.
- **AWS managed IAM policy** – A managed policy isn't used with this add-on.
- **Custom IAM permissions** – Custom permissions aren't used with this add-on.
- **Setup and usage instructions** – See [Amazon EKS integration](#) in the Kubecost documentation.

- If your cluster is version 1.23 or later, you must have the [the section called “Amazon EBS CSI driver” \(p. 228\)](#) installed on your cluster. otherwise you will receive an error.

Teleport

- **Publisher** – Teleport
- **Name** – teleport_teleport
- **Namespace** – teleport
- **Service account name** – A service account isn't used with this add-on.
- **AWS managed IAM policy** – A managed policy isn't used with this add-on.
- **Custom IAM permissions** – Custom permissions aren't used with this add-on.
- **Setup and usage instructions** – See [How Teleport Works](#) in the Teleport documentation.

Tetrate

- **Publisher** – Tetrate Io
- **Name** – tetrate-io_istio-distro
- **Namespace** – istio-system
- **Service account name** – A service account isn't used with this add-on.
- **AWS managed IAM policy** – A managed policy isn't used with this add-on.
- **Custom IAM permissions** – Custom permissions aren't used with this add-on.
- **Setup and usage instructions** – See the [Tetrate Istio Distro](#) web site.

Upbound Universal Crossplane

- **Publisher** – Upbound
- **Name** – upbound_universal-crossplane
- **Namespace** – upbound-system
- **Service account name** – A service account isn't used with this add-on.
- **AWS managed IAM policy** – A managed policy isn't used with this add-on.
- **Custom IAM permissions** – Custom permissions aren't used with this add-on.
- **Setup and usage instructions** – See [Upbound Universal Crossplane \(UXP\)](#) in the Upbound documentation.

Datree

- **Publisher** – Datree
- **Name** – datree_engine-pro
- **Namespace** – datree
- **Service account name** – datree-webhook-server-awsmp
- **AWS managed IAM policy** – [AWSLicenseManagerConsumptionPolicy](#)
- **Command to create required IAM role** – The following command requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one, or to create one, see [the section called “Creating an IAM OIDC provider” \(p. 465\)](#). Replace *my-cluster* with the name of your cluster and *my-datree-role* with the name for your role. This command requires that you have [eksctl \(p. 13\)](#) installed on your device. If you need to use a different tool to create the role and annotate the Kubernetes service account, see [the section called “Configuring role and service account” \(p. 466\)](#).

```
eksctl create iamserviceaccount --name datree-webhook-server-awsmp --namespace datree --cluster my-cluster --role-name my-datree-role \  
    --role-only --attach-policy-arn arn:aws:iam::aws:policy/service-role/  
AWSLicenseManagerConsumptionPolicy --approve
```

- **Custom IAM permissions** – Custom permissions aren't used with this add-on.
- **Setup and usage instructions** – See [Amazon EKS-intergration](#) in the Datree documentation.

Kasten

- **Publisher** – Kasten by Veeam
- **Name** – kasten_k10
- **Namespace** – kasten-io
- **Service account name** – k10-k10
- **AWS managed IAM policy** – [AWSLicenseManagerConsumptionPolicy](#)
- **Command to create required IAM role** – The following command requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one, or to create one, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#). Replace **my-cluster** with the name of your cluster and **my-kasten-role** with the name for your role. This command requires that you have [eksctl \(p. 13\)](#) installed on your device. If you need to use a different tool to create the role and annotate the Kubernetes service account, see [the section called "Configuring role and service account" \(p. 466\)](#).

```
eksctl create iamserviceaccount --name k10-k10 --namespace kasten-io --cluster my-cluster \  
    --role-name my-kasten-role \  
        --role-only --attach-policy-arn arn:aws:iam::aws:policy/service-role/  
AWSLicenseManagerConsumptionPolicy --approve
```

- **Custom IAM permissions** – Custom permissions aren't used with this add-on.
- **Setup and usage instructions** – See [Installing K10 on AWS using Amazon EKS Add-on](#) in the Kasten documentation.
- **Additional information** – If your Amazon EKS cluster is version Kubernetes 1.23 or later, you must have the Amazon EBS CSI driver installed on your cluster with a default StorageClass.

HA Proxy

- **Publisher** – HA Proxy
- **Name** – haproxy-technologies_kubernetes-ingress-ee
- **Namespace** – haproxy-controller
- **Service account name** – customer defined
- **AWS managed IAM policy** – [AWSLicenseManagerConsumptionPolicy](#)
- **Command to create required IAM role** – The following command requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one, or to create one, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#). Replace **my-cluster** with the name of your cluster and **my-haproxy-role** with the name for your role. This command requires that you have [eksctl \(p. 13\)](#) installed on your device. If you need to use a different tool to create the role and annotate the Kubernetes service account, see [the section called "Configuring role and service account" \(p. 466\)](#).

```
eksctl create iamserviceaccount --name service-account-name --namespace haproxy-  
controller --cluster my-cluster --role-name my-haproxy-role \  
    --role-only --attach-policy-arn arn:aws:iam::aws:policy/service-role/  
AWSLicenseManagerConsumptionPolicy --approve
```

```
--role-only --attach-policy-arn arn:aws:iam::aws:policy/service-role/  
AWSLicenseManagerConsumptionPolicy --approve
```

- **Custom IAM permissions** – Custom permissions aren't used with this add-on.
- **Setup and usage instructions** – See [Install HAProxy Enterprise Kubernetes Ingress Controller on Amazon EKS from AWS](#) in the HAProxy documentation.

Managing Amazon EKS add-ons

Amazon EKS add-ons are a curated set of add-on software for Amazon EKS clusters. All Amazon EKS add-ons:

- include the latest security patches and bug fixes.
- are validated by AWS to work with Amazon EKS.
- reduce the amount of work required to manage the add-on software.

The AWS Management Console notifies you when a new version is available for an Amazon EKS add-on. You can simply initiate the update, and Amazon EKS updates the add-on software for you.

For a list of available add-ons, see [the section called "Available Amazon EKS add-ons from Amazon EKS" \(p. 386\)](#). For more information about Kubernetes field management, see [the section called "Kubernetes field management" \(p. 406\)](#)

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Getting started with Amazon EKS \(p. 6\)](#).
- If you're creating an add-on that uses a Kubernetes service account and IAM role, then you need to have an AWS Identity and Access Management (IAM) OpenID Connect (OIDC) provider for your cluster. To determine whether you have one for your cluster, or to create one, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#).

Creating an add-on

You can create an Amazon EKS add-on using eksctl, the AWS Management Console, or the AWS CLI. If the add-on requires an IAM role, see the details for the specific add-on in [the section called "Available Amazon EKS add-ons from Amazon EKS" \(p. 386\)](#) for details about creating the role.

eksctl

Prerequisite

Version 0.160.0 or later of the eksctl command line tool installed on your device or AWS CloudShell. To install or update eksctl, see [Installing or updating eksctl \(p. 13\)](#).

To create an Amazon EKS add-on using eksctl

1. View the names of add-ons available for a cluster version. Replace **1.28** with the version of your cluster.

```
eksctl utils describe-addon-versions --kubernetes-version 1.28 | grep AddonName
```

An example output is as follows.

```
"AddonName": "aws-ebs-csi-driver",  
          "AddonName": "coredns",
```

```
"AddonName": "kube-proxy",
"AddonName": "vpc-cni",
"AddonName": "adot",
"AddonName": "dynatrace_dynatrace-operator",
"AddonName": "upbound_universal-crossplane",
"AddonName": "teleport_teleport",
"AddonName": "factorhouse_kpow",
[...]
```

- View the versions available for the add-on that you would like to create. Replace **1.28** with the version of your cluster. Replace **name-of-addon** with the name of the add-on you want to view the versions for. The name must be one of the names returned in the previous steps.

```
eksctl utils describe-addon-versions --kubernetes-version 1.28 --name name-of-addon
| grep AddonVersion
```

The following output is an example of what is returned for the add-on named vpc-cni. You can see that the add-on has several available versions.

```
"AddonVersions": [
    "AddonVersion": "v1.12.0-eksbuild.1",
    "AddonVersion": "v1.11.4-eksbuild.1",
    "AddonVersion": "v1.10.4-eksbuild.1",
    "AddonVersion": "v1.9.3-eksbuild.1",
```

- Determine whether the add-on you want to create is an Amazon EKS or AWS Marketplace add-on. The AWS Marketplace has third party add-ons that require you to complete additional steps to create the add-on.

```
eksctl utils describe-addon-versions --kubernetes-version 1.28 --name name-of-addon
| grep ProductUrl
```

If no output is returned, then the add-on is an Amazon EKS. If output is returned, then the add-on is an AWS Marketplace add-on. The following output is for an add-on named teleport_teleport.

```
"ProductUrl": "https://aws.amazon.com/marketplace/pp?sku=3bda70bb-566f-4976-806c-f96faef18b26"
```

You can learn more about the add-on in the AWS Marketplace with the returned URL. If the add-on requires a subscription, you can subscribe to the add-on through the AWS Marketplace. If you're going to create an add-on from the AWS Marketplace, then the [IAM principal](#) that you're using to create the add-on must have permission to create the [AWSServiceRoleForAWSLicenseManagerRole](#) service-linked role. For more information about assigning permissions to an IAM entity, see [Adding and removing IAM identity permissions](#) in the IAM User Guide.

- Create an Amazon EKS add-on. Copy the command that follows to your device. Make the following modifications to the command as needed and then run the modified command:
 - Replace **my-cluster** with the name of your cluster.
 - Replace **name-of-addon** with the name of the add-on that you want to create.
 - If you want a version of the add-on that's earlier than the latest version, then replace **Latest** with the version number returned in the output of a previous step that you want to use.
 - If the add-on uses a service account role, replace **11122223333** with your account ID and replace **role-name** with the name of the role. For instructions on creating a role for your service account, see the [documentation \(p. 386\)](#) for the add-on that you're creating.

Specifying a service account role requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one for your cluster, or to create one, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#).

If the add-on doesn't use a service account role, delete **--service-account-role-arn arn:aws:iam::111122223333:role/role-name**.

- This example command overwrites the configuration of any existing self-managed version of the add-on, if there is one. If you don't want to overwrite the configuration of an existing self-managed add-on, remove the **--force** option. If you remove the option, and the Amazon EKS add-on needs to overwrite the configuration of an existing self-managed add-on, then creation of the Amazon EKS add-on fails with an error message to help you resolve the conflict. Before specifying this option, make sure that the Amazon EKS add-on doesn't manage settings that you need to manage, because those settings are overwritten with this option.

```
eksctl create addon --cluster my-cluster --name name-of-addon --version latest \  
--service-account-role-arn arn:aws:iam::111122223333:role/role-name --force
```

You can see a list of all available options for the command.

```
eksctl create addon --help
```

For more information about available options see [Addons](#) in the eksctl documentation.
AWS Management Console

To create an Amazon EKS add-on using the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, select **Clusters**, and then select the name of the cluster that you want to create the add-on for.
3. Choose the **Add-ons** tab.
4. Select **Get more add-ons**.
5. Choose the add-ons that you want to add to your cluster. You can add as many **Amazon EKS add-ons** and **AWS Marketplace add-ons** as you require. If you're selecting **add-ons** that appear in the **AWS Marketplace** section, then the **IAM principal** that you're using to create the add-on must have permissions to read entitlements for the add-on from the AWS LicenseManager. AWS LicenseManager requires [AWSServiceRoleForAWSLicenseManagerRole](#) service-linked role (SLR) that allows AWS resources to manage licenses on your behalf. The SLR is a one time requirement, per account, and you will not have to create separate SLR's for each add-on nor each cluster. For more information about assigning permissions to an **IAM principal** see [Adding and removing IAM identity permissions](#) in the IAM User Guide. If the **AWS Marketplace add-ons** that you want to install isn't listed, you can search for available **AWS Marketplace add-ons** by entering text in the search box. You can also search by **category**, **vendor**, or **pricing model** and then choose the add-ons from the search results. Once you've selected the add-ons that you want to install, choose **Next**.
6. On the **Configure selected add-ons settings** page:
 - For **Version**, select the version that you want to install. We recommend the version marked **latest**, unless the individual add-on that you're creating recommends a different version. To determine whether an add-on has a recommended version, see the [documentation \(p. 386\)](#) for the add-on that you're creating.
 - If all of the add-ons that you selected have **Requires subscription** under **Status**, select **Next**. You can't [configure those add-ons \(p. 400\)](#) further until you've subscribed to them after your cluster is created. For the add-ons that don't have **Requires subscription** under **Status**:

- For **Select IAM role**, accept the default option, unless the add-on requires IAM permissions. If the add-on requires AWS permissions, you can select **Inherit from node** or an existing role that you created for use with the add-on. If there's no role to select, then you don't have an existing role. Regardless of which option you choose, see the [documentation \(p. 386\)](#) for the add-on that you're creating to create an IAM policy and attach it to a role. Selecting an IAM role requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one for your cluster, or to create one, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#).
 - Choose **Optional configuration settings**.
 - If the add-on requires configuration, enter it in the **Configuration values** box. To determine whether the add-on requires configuration information, see the [documentation \(p. 386\)](#) for the add-on that you're creating.
 - Select one of the available options for **Conflict resolution method**.
 - Choose **Next**.
7. On the **Review and add** page, choose **Create**. After the add-on installation is complete, you see your installed add-ons.
 8. If any of the add-ons that you installed require a subscription, complete the following steps:
 1. Choose the **Subscribe** button in the lower right corner for the add-on. You're taken to the page for the add-on in the AWS Marketplace. Read the information about the add-on such as its **Product Overview** and **Pricing Information**.
 2. Select the **Continue to Subscribe** button on the top right of the add-on page.
 3. Read through the **Terms and Conditions**. If you agree to them, choose **Accept Terms**. It may take several minutes to process the subscription. While the subscription is processing, the **Return to Amazon EKS Console** button is grayed out.
 4. Once the subscription has finished processing, the **Return to Amazon EKS Console** button is no longer grayed out. Choose the button to go back to the Amazon EKS console **Add-ons** tab for your cluster.
 5. For the add-on that you subscribed to, choose **Remove and reinstall** and then choose **Reinstall add-on**. Installation of the add-on can take several minutes. When Installation is complete, you can configure the add-on.

AWS CLI

Prerequisite

Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.

To create an Amazon EKS add-on using the AWS CLI

1. Determine which add-ons are available. You can see all available add-ons, their type, and their publisher. You can also see the URL for add-ons that are available through the AWS Marketplace. Replace **1.28** with the version of your cluster.

```
aws eks describe-addon-versions --kubernetes-version 1.28 \
    --query 'addons[].{MarketplaceProductId: marketplaceInformation.productId,
    Name: addonName, Owner: owner Publisher: publisher, Type: type}' --output table
```

An example output is as follows.

DescribeAddonVersions				Name
	MarketplaceProductUrl	Owner	Publisher	Type
None		aws	eks	storage
None		aws	eks	networking
None		aws	eks	networking
None		aws	eks	networking
None		aws	eks	observability
https://aws.amazon.com/marketplace/pp/prodview-brb73nceicv7u	dynatrace_dynatrace-operator	aws-marketplace	dynatrace	monitoring
https://aws.amazon.com/marketplace/pp/prodview-uhc2iwi5xysoc	upbound_universal-crossplane	aws-marketplace	upbound	infra-management
https://aws.amazon.com/marketplace/pp/prodview-hd2ydsrggy4li	teleport_teleport	aws-marketplace	teleport	policy-management
https://aws.amazon.com/marketplace/pp/prodview-vgghgqdsplhvc	factorhouse_kpow	aws-marketplace	factorhouse	monitoring
[...]	[...]	[...]	[...]	[...]

Your output might be different. In this example output, there are three different add-ons available of type networking and five add-ons with a publisher of type eks. The add-ons with aws-marketplace in the Owner column may require a subscription before you can install them. You can visit the URL to learn more about the add-on and to subscribe to it.

2. You can see which versions are available for each add-on. Replace **1.28** with the version of your cluster and replace **vpc-cni** with the name of an add-on returned in the previous step.

```
aws eks describe-addon-versions --kubernetes-version 1.28 --addon-name vpc-cni \
--query 'addons[].addonVersions[].[Version: addonVersion, Defaultversion: \
compatibilities[0].defaultVersion]' --output table
```

An example output is as follows.

DescribeAddonVersions	
Defaultversion	Version
False	v1.12.0-eksbuild.1

True	v1.11.4-eksbuild.1
False	v1.10.4-eksbuild.1
False	v1.9.3-eksbuild.1

The version with True in the Defaultversion column is the version that the add-on is created with, by default.

3. (Optional) Find the configuration options for your chosen add-on by running the following command:

```
aws eks describe-addon-configuration --addon-name vpc-cni --addon-version v1.12.0-eksbuild.1
```

```
{
  "addonName": "vpc-cni",
  "addonVersion": "v1.12.0-eksbuild.1",
  "configurationSchema": "{\"$ref\": \"#/definitions/VpcCni\", \"$schema\": \"http://json-schema.org/draft-06/schema#\", \"definitions\": {\"Cri\": {\"additionalProperties\": false, \"properties\": {\"hostPath\": {\"$ref\": \"#/definitions/HostPath\"}}}, \"Env\": {\"additionalProperties\": false, \"properties\": {\"ADDITIONAL_ENI_TAGS\": {\"type\": \"string\"}, \"AWS_VPC_CNI_NODE_PORT_SUPPORT\": {\"format\": \"boolean\"}, \"AWS_VPC_ENI_MTU\": {\"format\": \"integer\"}, \"type\": \"string\"}, \"AWS_VPC_K8S_CNI_CONFIGURE_RPFFILTER\": {\"format\": \"boolean\"}, \"type\": \"string\"}, \"AWS_VPC_K8S_CNI_CUSTOM_NETWORK_CFG\": {\"format\": \"boolean\"}, \"type\": \"string\"}, \"AWS_VPC_K8S_CNI_EXTERNALSNAT\": {\"format\": \"boolean\"}, \"type\": \"string\"}, \"AWS_VPC_K8S_CNI_LOGLEVEL\": {\"type\": \"string\"}, \"AWS_VPC_K8S_CNI_LOGFILE\": {\"type\": \"string\"}, \"AWS_VPC_K8S_CNI_RANDOMIZESNAT\": {\"type\": \"string\"}, \"AWS_VPC_K8S_CNI_VETHPREFIX\": {\"type\": \"string\"}, \"AWS_VPC_K8S_PLUGIN_LOG_FILE\": {\"type\": \"string\"}, \"AWS_VPC_K8S_PLUGIN_LOG_LEVEL\": {\"type\": \"string\"}, \"DISABLE_INTROSPECTION\": {\"format\": \"boolean\"}, \"type\": \"string\"}, \"DISABLE_METRICS\": {\"format\": \"boolean\"}, \"type\": \"string\"}, \"DISABLE_NETWORK_RESOURCE_PROVISIONING\": {\"format\": \"boolean\"}, \"type\": \"string\"}, \"ENABLE_POD_ENI\": {\"format\": \"boolean\"}, \"type\": \"string\"}, \"ENABLE_PREFIX_DELEGATION\": {\"format\": \"boolean\"}, \"type\": \"string\"}, \"WARM_ENI_TARGET\": {\"format\": \"integer\"}, \"type\": \"string\"}, \"WARM_PREFIX_TARGET\": {\"format\": \"integer\"}, \"type\": \"string\"}], \"title\": \"Env\", \"type\": \"object\"}, \"HostPath\": {\"additionalProperties\": false, \"properties\": {\"path\": {\"type\": \"string\"}}, \"title\": \"HostPath\"}, \"type\": \"object\"}, \"Limits\": {\"additionalProperties\": false, \"properties\": {\"cpu\": {\"type\": \"string\"}, \"memory\": {\"type\": \"string\"}}, \"title\": \"Limits\"}, \"type\": \"object\"}, \"Resources\": {\"additionalProperties\": false, \"properties\": {\"limits\": {\"$ref\": \"#/definitions/Limits\"}, \"requests\": {\"$ref\": \"#/definitions/Limits\"}}, \"title\": \"Resources\"}, \"type\": \"object\"}, \"VpcCni\": {\"additionalProperties\": false, \"properties\": {\"cri\": {\"$ref\": \"#/definitions/Cri\"}, \"env\": {\"$ref\": \"#/definitions/Env\"}, \"resources\": {\"$ref\": \"#/definitions/Resources\"}}, \"title\": \"VpcCni\"}, \"type\": \"object\"}}}}
```

The output is a standard JSON schema.

Here is an example of valid configuration values, in JSON format, that works with the schema above.

```
{
  "resources": {
    "limits": {
      "cpu": "100m"
    }
  }
}
```

}

Here is an example of valid configuration values, in YAML format, that works with the schema above.

```
resources:
  limits:
    cpu: 100m
```

4. Create an Amazon EKS add-on. Copy the command that follows to your device. Make the following modifications to the command as needed and then run the modified command:
 - Replace *my-cluster* with the name of your cluster.
 - Replace *vpc-cni* with an add-on name returned in the output of the previous step that you want to create.
 - Replace *version-number* with the version returned in the output of the previous step that you want to use.
 - If the add-on uses a Kubernetes service account and IAM role, replace *111122223333* with your account ID and *role-name* with the name of an existing IAM role that you've created. For instructions on creating the role, see the [documentation \(p. 386\)](#) for the add-on that you're creating. Specifying a service account role requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one for your cluster, or to create one, see the [section called "Creating an IAM OIDC provider" \(p. 465\)](#).

If the add-on doesn't use a Kubernetes service account and IAM role, delete `--service-account-role-arn arn:aws:iam::111122223333:role/role-name`.

- These example commands overwrites the `--configuration-values` option of any existing self-managed version of the add-on, if there is one. Replace this with the desired configuration values, such as a string or a file input. If you don't want to provide configuration values, then delete the `--configuration-values` option. If you don't want the AWS CLI to overwrite the configuration of an existing self-managed add-on, remove the `--resolve-conflicts OVERWRITE` option. If you remove the option, and the Amazon EKS add-on needs to overwrite the configuration of an existing self-managed add-on, then creation of the Amazon EKS add-on fails with an error message to help you resolve the conflict. Before specifying this option, make sure that the Amazon EKS add-on doesn't manage settings that you need to manage, because those settings are overwritten with this option.

```
aws eks create-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version version-number \
  --service-account-role-arn arn:aws:iam::111122223333:role/role-name \
  --configuration-values '{"resources":{"limits":{"cpu":"100m"}}}' --resolve-conflicts OVERWRITE
```

```
aws eks create-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version version-number \
  --service-account-role-arn arn:aws:iam::111122223333:role/role-name \
  --configuration-values 'file://example.yaml' --resolve-conflicts OVERWRITE
```

For a full list of available options, see [create-addon](#) in the Amazon EKS Command Line Reference. If the add-on that you created has aws-marketplace listed in the Owner column of a previous step, then creation may fail, and you may receive an error message similar to the following error.

```
{
  "addon": {
```

```

"addonName": "addon-name",
"clusterName": "my-cluster",
"status": "CREATE_FAILED",
"addonVersion": "version",
"health": {
    "issues": [
        {
            "code": "AddonSubscriptionNeeded",
            "message": "You are currently not subscribed to this add-on. To subscribe, visit the AWS Marketplace console, agree to the seller EULA, select the pricing type if required, then re-install the add-on"
        }
    ]
}

```

If you receive an error similar to the error in the previous output, visit the URL in the output of a previous step to subscribe to the add-on. Once subscribed, run the `create-addon` command again.

Updating an add-on

Amazon EKS doesn't automatically update an add-on when new versions are released or after you update your cluster to a new Kubernetes minor version. To update an add-on for an existing cluster, you must initiate the update. After you initiate the update, Amazon EKS updates the add-on for you. Before updating an add-on, review the current documentation for the add-on. For a list of available add-ons, see [the section called "Available Amazon EKS add-ons from Amazon EKS" \(p. 386\)](#). If the add-on requires an IAM role, see the details for the specific add-on in [the section called "Available Amazon EKS add-ons from Amazon EKS" \(p. 386\)](#) for details about creating the role.

You can update an Amazon EKS add-on using `eksctl`, the AWS Management Console, or the AWS CLI.

`eksctl`

Prerequisite

Version 0.160.0 or later of the `eksctl` command line tool installed on your device or AWS CloudShell. To install or update `eksctl`, see [Installing or updating eksctl \(p. 13\)](#).

To update an Amazon EKS add-on using `eksctl`

- Determine the current add-ons and add-on versions installed on your cluster. Replace `my-cluster` with the name of your cluster.

```
eksctl get addon --cluster my-cluster
```

An example output is as follows.

NAME	VERSION	STATUS	ISSUES	IAMROLE	UPDATE AVAILABLE
coredns	v1.8.7-eksbuild.2	ACTIVE	0		
kube-proxy	v1.23.7-eksbuild.1	ACTIVE	0		v1.23.8-eksbuild.2
vpc-cni	v1.10.4-eksbuild.1	ACTIVE	0		v1.12.0-
					eksbuild.1,v1.11.4-eksbuild.1,v1.11.3-eksbuild.1,v1.11.2-eksbuild.1,v1.11.0-eksbuild.1

Your output might look different, depending on which add-ons and versions that you have on your cluster. You can see that in the previous example output, two existing add-ons on the cluster have newer versions available in the UPDATE AVAILABLE column.

- Update the add-on.

1. Copy the command that follows to your device. Make the following modifications to the command as needed:

- Replace *my-cluster* with the name of your cluster.
- Replace *region* with the AWS Region that your cluster is in.
- Replace *vpc-cni* with the name of an add-on returned in the output of the previous step that you want to update.
- If you want to update to a version earlier than the latest available version, then replace *latest* with the version number returned in the output of the previous step that you want to use. Some add-ons have recommended versions. For more information, see the [documentation \(p. 386\)](#) for the add-on that you're updating.
- If the add-on uses a Kubernetes service account and IAM role, replace **111122223333** with your account ID and *role-name* with the name of an existing IAM role that you've created. For instructions on creating the role, see the [documentation \(p. 386\)](#) for the add-on that you're creating. Specifying a service account role requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one for your cluster, or to create one, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#).

If the add-on doesn't use a Kubernetes service account and IAM role, delete the **serviceAccountRoleARN: arn:aws:iam::111122223333:role/*role-name*** line.

- The *preserve* option preserves existing values for the add-on. If you have set custom values for add-on settings, and you don't use this option, Amazon EKS overwrites your values with its default values. If you use this option, then we recommend that you test any field and value changes on a non-production cluster before updating the add-on on your production cluster. If you change this value to *overwrite*, all settings are changed to Amazon EKS default values. If you've set custom values for any settings, they might be overwritten with Amazon EKS default values. If you change this value to *none*, Amazon EKS doesn't change the value of any settings, but the update might fail. If the update fails, you receive an error message to help you resolve the conflict.

```
cat >update-addon.yaml <<EOF
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
  name: my-cluster
  region: region

addons:
- name: vpc-cni
  version: latest
  serviceAccountRoleARN: arn:aws:iam::111122223333:role/role-name
  resolveConflicts: preserve
EOF
```

2. Run the modified command to create the update-addon.yaml file.
3. Apply the config file to your cluster.

```
eksctl update addon -f update-addon.yaml
```

For more information about updating add-ons, see [Addons](#) in the eksctl documentation.

AWS Management Console

To update an Amazon EKS add-on using the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, select **Clusters**, and then select the name of the cluster that you want to configure the add-on for.
3. Choose the **Add-ons** tab.
4. Select the box in the top right of the add-on box and then choose **Edit**.
5. On the **Configure name of addon** page:
 - Select the **Version** that you'd like to use. The add-on might have a recommended version. For more information, see the [documentation \(p. 386\)](#) for the add-on that you're updating.
 - For **Select IAM role**, you can select **Inherit from node** or an existing role that you created for use with the add-on. If there's no role to select, then you don't have an existing role. Regardless of which option you choose, see the [documentation \(p. 386\)](#) for the add-on that you're creating to create an IAM policy and attach it to a role. Selecting an IAM role requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one for your cluster, or to create one, see [the section called "Creating an IAM OIDC provider" \(p. 465\)](#).
 - For **Code editor**, enter any add-on specific configuration information. For more information, see the [documentation \(p. 386\)](#) for the add-on that you're updating.
 - For **Conflict resolution method**, select one of the options. If you have set custom values for add-on settings, we recommend the **Preserve** option. If you don't choose this option, Amazon EKS overwrites your values with its default values. If you use this option, then we recommend that you test any field and value changes on a non-production cluster before updating the add-on on your production cluster.
6. Choose **Update**.

AWS CLI

Prerequisite

Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.

To update an Amazon EKS add-on using the AWS CLI

1. See a list of installed add-ons. Replace `my-cluster` with the name of your cluster.

```
aws eks list-addons --cluster-name my-cluster
```

An example output is as follows.

```
{  
  "addons": [  
    "coredns",  
    "kube-proxy",  
    "vpc-cni"  
  ]}
```

}

- View the current version of the add-on that you want to update. Replace *my-cluster* with your cluster name and *vpc-cni* with the name of the add-on that you want to update.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni --query "addon.addonVersion" --output text
```

An example output is as follows.

```
v1.10.4-eksbuild.1
```

- You can see which versions of the add-on are available for your cluster's version. Replace *1.28* with your cluster's version and *vpc-cni* with the name of the add-on that you want to update.

```
aws eks describe-addon-versions --kubernetes-version 1.28 --addon-name vpc-cni \
--query 'addons[].addonVersions[].[{Version: addonVersion, Defaultversion: compatibilities[0].defaultVersion}]' --output table
```

An example output is as follows.

DescribeAddonVersions	
Defaultversion	Version
False	v1.12.0-eksbuild.1
True	v1.11.4-eksbuild.1
False	v1.10.4-eksbuild.1
False	v1.9.3-eksbuild.1

The version with True in the Defaultversion column is the version that the add-on is created with, by default.

- Update your add-on. Copy the command that follows to your device. Make the following modifications to the command, as needed, and then run the modified command.
 - Replace *my-cluster* with the name of your cluster.
 - Replace *vpc-cni* with the name of the add-on that you want to update that was returned in the output of a previous step.
 - Replace *version-number* with the version returned in the output of the previous step that you want to update to. Some add-ons have recommended versions. For more information, see the [documentation \(p. 386\)](#) for the add-on that you're updating.
 - If the add-on uses a Kubernetes service account and IAM role, replace *111122223333* with your account ID and *role-name* with the name of an existing IAM role that you've created. For instructions on creating the role, see the [documentation \(p. 386\)](#) for the add-on that you're creating. Specifying a service account role requires that you have an IAM OpenID Connect (OIDC) provider for your cluster. To determine whether you have one for your cluster, or to create one, see the section called "[Creating an IAM OIDC provider](#)" (p. 465).

If the add-on doesn't use a Kubernetes service account and IAM role, delete the **serviceAccountRoleARN: arn:aws:iam::111122223333:role/*role-name*** line.

- The **--resolve-conflicts *PRESERVE*** option preserves existing values for the add-on. If you have set custom values for add-on settings, and you don't use this option, Amazon EKS overwrites your values with its default values. If you use this option, then we recommend that you test any field and value changes on a non-production cluster before updating the add-on

on your production cluster. If you change this value to `overwrite`, all settings are changed to Amazon EKS default values. If you've set custom values for any settings, they might be overwritten with Amazon EKS default values. If you change this value to `none`, Amazon EKS doesn't change the value of any settings, but the update might fail. If the update fails, you receive an error message to help you resolve the conflict.

- If you want to remove all custom configuration then perform the update using the `--configuration-values '{}` option. This sets all custom configuration back to the default values. If you don't want to change your custom configuration, don't provide the `--configuration-values` flag. If you want to adjust a custom configuration then replace `{}` with the new parameters. To see a list of parameters, see [viewing configuration schema \(p. 398\)](#) step in the create an add-on section.

```
aws eks update-addon --cluster-name my-cluster --addon-name vpc-cni --addon-version version-number \
    --service-account-role-arn arn:aws:iam::111122223333:role/role-name \
    --configuration-values '{}' --resolve-conflicts PRESERVE
```

5. Check the status of the update. Replace `my-cluster` with the name of your cluster and `vpc-cni` with the name of the add-on you're updating.

```
aws eks describe-addon --cluster-name my-cluster --addon-name vpc-cni
```

An example output is as follows.

```
{  
  "addon": {  
    "addonName": "vpc-cni",  
    "clusterName": "my-cluster",  
    "status": "UPDATING",  
    [...]
```

The update is complete when the status is ACTIVE.

Deleting an add-on

When you delete an Amazon EKS add-on:

- There is no downtime for the functionality that the add-on provides.
- If the add-on has an IAM role associated with it, the IAM role isn't removed.
- Amazon EKS stops managing settings for the add-on.
- The console stops notifying you when new versions are available.
- You can't update the add-on using any AWS tools or APIs.
- You can choose to leave the add-on software on your cluster so that you can self-manage it, or you can remove the add-on software from your cluster. You should only remove the add-on software from your cluster if there are no resources on your cluster are dependent on the functionality that the add-on provides.

You can delete an Amazon EKS add-on from your cluster using `eksctl`, the AWS Management Console, or the AWS CLI.

eksctl

Prerequisite

Version 0.160.0 or later of the eksctl command line tool installed on your device or AWS CloudShell. To install or update eksctl, see [Installing or updating eksctl \(p. 13\)](#).

To delete an Amazon EKS add-on using eksctl

1. Determine the current add-ons installed on your cluster. Replace *my-cluster* with the name of your cluster.

```
eksctl get addon --cluster my-cluster
```

An example output is as follows.

NAME	VERSION	STATUS	ISSUES	IAMROLE	UPDATE AVAILABLE
coredns	v1.8.7-eksbuild.2	ACTIVE	0		
kube-proxy	v1.23.7-eksbuild.1	ACTIVE	0		
vpc-cni	v1.10.4-eksbuild.1	ACTIVE	0		
[...]					

Your output might look different, depending on which add-ons and versions that you have on your cluster.

2. Delete the add-on. Replace *my-cluster* with the name of your cluster and *name-of-addon* with the name of the add-on returned in the output of the previous step that you want to remove. If you remove the **--preserve** option, in addition to Amazon EKS no longer managing the add-on, the add-on software is removed from your cluster.

```
eksctl delete addon --cluster my-cluster --name name-of-addon --preserve
```

AWS Management Console

To delete an Amazon EKS add-on using the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, select **Clusters**, and then select the name of the cluster that you want to remove the Amazon EKS add-on for.
3. Choose the **Add-ons** tab.
4. Select the check box in the upper right of the add-on box and then choose **Remove**. Select **Preserve on the cluster** if you want Amazon EKS to stop managing settings for the add-on, but want to retain the add-on software on your cluster so that you can self-manage all of the settings for the add-on. Type the add-on name and then select **Remove**.

AWS CLI

Prerequisite

Version 0.160.0 or later of the eksctl command line tool installed on your device or AWS CloudShell. To install or update eksctl, see [Installing or updating eksctl \(p. 13\)](#).

To delete an Amazon EKS add-on using the AWS CLI

1. See a list of installed add-ons. Replace *my-cluster* with the name of your cluster.

```
aws eks list-addons --cluster-name my-cluster
```

An example output is as follows.

```
{  
    "addons": [  
        "coredns",  
        "kube-proxy",  
        "vpc-cni",  
        "name-of-addon"  
    ]  
}
```

2. Delete the installed add-on. Replace *my-cluster* with the name of your cluster and *name-of-addon* with the name of the add-on that you want to remove. Removing *--preserve* removes the add-on software from your cluster.

```
aws eks delete-addon --cluster-name my-cluster --addon-name name-of-addon --preserve
```

The abbreviated example output is as follows.

```
{  
    "addon": {  
        "addonName": "name-of-addon",  
        "clusterName": "my-cluster",  
        "status": "DELETING",  
        [...]  
    }  
}
```

3. Check the status of the deletion. Replace *my-cluster* with the name of your cluster and *name-of-addon* with the name of the add-on that you're removing.

```
aws eks describe-addon --cluster-name my-cluster --addon-name name-of-addon
```

After the add-on is deleted, the example output is as follows.

```
An error occurred (ResourceNotFoundException) when calling the DescribeAddon  
operation: No addon: name-of-addon found in cluster: my-cluster
```

Kubernetes field management

Amazon EKS add-ons are installed to your cluster using standard, best practice configurations. For more information about adding an Amazon EKS add-on to your cluster, see [Amazon EKS add-ons \(p. 385\)](#).

You may want to customize the configuration of an Amazon EKS add-on to enable advanced features. Amazon EKS uses the Kubernetes server-side apply feature to enable management of an add-on by Amazon EKS without overwriting your configuration for settings that aren't managed by Amazon EKS. For more information, see [Server-Side Apply](#) in the Kubernetes documentation. To achieve this, Amazon EKS manages a minimum set of fields for every add-on that it installs. You can modify all fields that aren't managed by Amazon EKS, or another Kubernetes control plane process such as kube-controller-manager, without issue.

Important

Modifying a field managed by Amazon EKS prevents Amazon EKS from managing the add-on and may result in your changes being overwritten when an add-on is updated.

View field management status

You can use `kubectl` to see which fields are managed by Amazon EKS for any Amazon EKS add-on.

To see the management status of a field

1. Determine which add-on that you want to examine. To see all of the deployments and DaemonSets deployed to your cluster, see [View Kubernetes resources \(p. 529\)](#).
2. View the managed fields for an add-on by running the following command:

```
kubectl get type/add-on-name -n add-on-namespace -o yaml
```

For example, you can see the managed fields for the CoreDNS add-on with the following command.

```
kubectl get deployment/coredns -n kube-system -o yaml
```

Field management is listed in the following section in the returned output.

```
[...]
managedFields:
  - apiVersion: apps/v1
    fieldsType: FieldsV1
    fieldsV1:
[...]
```

Note

If you don't see `managedFields` in the output, add `--show-managed-fields` to the command and run it again. The version of `kubectl` that you're using determines whether managed fields are returned by default.

Understanding field management syntax in the Kubernetes API

When you view details for a Kubernetes object, both managed and unmanaged fields are returned in the output. Managed fields can be either of the following types:

- **Fully managed** – All keys for the field are managed by Amazon EKS. Modifications to any value causes a conflict.
- **Partially managed** – Some keys for the field are managed by Amazon EKS. Only modifications to the keys explicitly managed by Amazon EKS cause a conflict.

Both types of fields are tagged with `manager: eks`.

Each key is either a `.` representing the field itself, which always maps to an empty set, or a string that represents a sub-field or item. The output for field management consists of the following types of declarations:

- `f:name`, where `name` is the name of a field in a list.
- `k:keys`, where `keys` is a map of a list item's fields.
- `v:value`, where `value` is the exact JSON formatted value of a list item.
- `i:index`, where `index` is position of an item in the list.

The following portions of output for the CoreDNS add-on illustrate the previous declarations:

- **Fully managed fields** – If a managed field has an `f: (field)` specified, but no `k: (key)`, then the entire field is managed. Modifications to any values in this field cause a conflict.

In the following output, you can see that the container named `coredns` is managed by `eks`. The `args`, `image`, and `imagePullPolicy` sub-fields are also managed by `eks`. Modifications to any values in these fields cause a conflict.

```
[...]
f:containers:
  k:{"name":"coredns"}:
    .: {}
    f:args: {}
    f:image: {}
    f:imagePullPolicy: {}
[...]
manager: eks
[...]
```

- **Partially managed fields** – If a managed key has a value specified, the declared keys are managed for that field. Modifying the specified keys cause a conflict.

In the following output, you can see that `eks` manages the `config-volume` and `tmp` volumes set with the `name` key.

```
[...]
f:volumes:
  k:{"name":"config-volume"}:
    .: {}
    f:configMap:
      f:items: {}
      f:name: {}
    f:name: {}
  k:{"name":"tmp"}:
    .: {}
    f:name: {}
[...]
manager: eks
[...]
```

- **Adding keys to partially managed fields** – If only a specific key value is managed, you can safely add additional keys, such as arguments, to a field without causing a conflict. If you add additional keys, make sure that the field isn't managed first. Adding or modifying any value that is managed causes a conflict.

In the following output, you can see that both the `name` key and `name` field are managed. Adding or modifying any container name causes a conflict with this managed key.

```
[...]
f:containers:
  k:{"name":"coredns"}:
    [...]
      f:name: {}
    [...]
manager: eks
[...]
```

Verifying a container image during deployment

If you use [AWS Signer](#) and want to verify signed container images at the time of deployment, you can use one of the following solutions:

- [Gatekeeper and Ratify](#) – Use Gatekeeper as the admission controller and Ratify configured with an AWS Signer plugin as a web hook for validating signatures.
- [Kyverno](#) – A Kubernetes policy engine configured with an AWS Signer plugin for validating signatures.

Note

Before verifying container image signatures, configure the [Notation](#) trust store and trust policy, as required by your selected admission controller.

Machine learning training using Elastic Fabric Adapter

This topic describes how to integrate Elastic Fabric Adapter (EFA) with Pods deployed in your Amazon EKS cluster. Elastic Fabric Adapter (EFA) is a network interface for Amazon EC2 instances that enables you to run applications requiring high levels of inter-node communications at scale on AWS. Its custom-built operating system bypass hardware interface enhances the performance of inter-instance communications, which is critical to scaling these applications. With EFA, High Performance Computing (HPC) applications using the Message Passing Interface (MPI) and Machine Learning (ML) applications using NVIDIA Collective Communications Library (NCCL) can scale to thousands of CPUs or GPUs. As a result, you get the application performance of on-premises HPC clusters with the on-demand elasticity and flexibility of the AWS cloud. Integrating EFA with applications running on Amazon EKS clusters can reduce the time to complete large scale distributed training workloads without having to add additional instances to your cluster. For more information about EFA, [Elastic Fabric Adapter](#).

The EFA plugin described in this topic fully supports Amazon EC2 [P4d](#) instances, which represent the current state of the art in distributed machine learning in the cloud. Each p4d.24xlarge instance has eight NVIDIA A100 GPUs, and 400 Gbps GPUDirectRDMA over EFA. GPUDirectRDMA enables you to have direct GPU-to-GPU communication across nodes with CPU bypass, increasing collective communication bandwidth and lowering latency. Amazon EKS and EFA integration with P4d instances provides a seamless method to take advantage of the highest performing Amazon EC2 computing instance for distributed machine learning training.

Prerequisites

- An existing Amazon EKS cluster. If you don't have an existing cluster, use one of our [Getting started with Amazon EKS \(p. 6\)](#) guides to create one. Your cluster must be deployed in a VPC that has at least one private subnet with enough available IP addresses to deploy nodes in. The private subnet must have outbound internet access provided by an external device, such as a NAT gateway.

If you plan to use eksctl to create your node group, eksctl can also create a cluster for you.

- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.

- The `kubectl` command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use `kubectl` version 1.26, 1.27, or 1.28 with it. To install or upgrade `kubectl`, see [Installing or updating `kubectl` \(p. 6\)](#).
- You must have the Amazon VPC CNI plugin for Kubernetes version 1.7.10 or later installed before launching worker nodes that support multiple Elastic Fabric Adapters, such as the `p4d.24xlarge`. For more information about updating your Amazon VPC CNI plugin for Kubernetes version, see [the section called "Amazon VPC CNI plugin for Kubernetes" \(p. 266\)](#).

Create node group

The following procedure helps you create a node group with a `p4d.24xlarge` backed node group with EFA interfaces and GPUDirect RDMA, and run an example NVIDIA Collective Communications Library (NCCL) test for multi-node NCCL Performance using EFAs. The example can be used a template for distributed deep learning training on Amazon EKS using EFAs.

1. Determine which Amazon EC2 instance types that support EFA are available in the AWS Region that you want to deploy nodes in. Replace `region-code` with the AWS Region that you want to deploy your node group in.

```
aws ec2 describe-instance-types --region region-code --filters Name=network-infoefa-supported,Values=true \
--query "InstanceTypes[*].[InstanceType]" --output text
```

When you deploy nodes, the instance type that you want to deploy must be available in the AWS Region that your cluster is in.

2. Determine which Availability Zones that the instance type that you want to deploy is available in. In this tutorial, the `p4d.24xlarge` instance type is used and must be returned in the output for the AWS Region that you specified in the previous step. When you deploy nodes in a production cluster, replace `p4d.24xlarge` with any instance type returned in the previous step.

```
aws ec2 describe-instance-type-offerings --region region-code --location-type availability-zone --filters Name=instance-type,Values=p4d.24xlarge \
--query 'InstanceTypeOfferings[*].Location' --output text
```

An example output is as follows.

```
us-west-2a      us-west-2c      us-west-2b
```

Note the Availability Zones returned for use in later steps. When you deploy nodes to a cluster, your VPC must have subnets with available IP addresses in one of the Availability Zones returned in the output.

3. Create a node group using either `eksctl` or the AWS CLI and AWS CloudFormation.

`eksctl`

Prerequisite

Version 0.160.0 or later of the `eksctl` command line tool installed on your device or AWS CloudShell. To install or update `eksctl`, see [Installing or updating `eksctl` \(p. 13\)](#).

1. Copy the following contents to a file named `efa-cluster.yaml`. Replace the `example values` with your own. You can replace `p4d.24xlarge` with a different instance, but if you

do, make sure that the values for availabilityZones are Availability Zones that were returned for the instance type in step 1.

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-efa-cluster
  region: region-code
  version: "1.XX"

iam:
  withOIDC: true

availabilityZones: ["us-west-2a", "us-west-2c"]

managedNodeGroups:
- name: my-efa-ng
  instanceType: p4d.24xlarge
  minSize: 1
  desiredCapacity: 2
  maxSize: 3
  availabilityZones: ["us-west-2a"]
  volumeSize: 300
  privateNetworking: true
  efaEnabled: true
```

2. Create a managed node group in an existing cluster.

```
eksctl create nodegroup -f efa-cluster.yaml
```

If you don't have an existing cluster, you can run the following command to create a cluster and the node group.

```
eksctl create cluster -f efa-cluster.yaml
```

Note

Because the instance type used in this example has GPUs, eksctl automatically installs the NVIDIA Kubernetes device plugin on each instance for you.

AWS CLI and AWS CloudFormation

There are several requirements for EFA networking, including creating an EFA specific security group, creating an Amazon EC2 [placement group](#), and creating a launch template that specifies one or more EFA interfaces, and includes EFA driver installation as part of Amazon EC2 user data. To learn more about EFA requirements, see [Get started with EFA and MPI](#) in the Amazon EC2 User Guide for Linux Instances. The following steps create all of this for you. Replace all *example values* with your own.

1. Set a few variables used in later steps. Replace all of the *example values* with your own. Replace *my-cluster* with the name of your existing cluster. The value for `node_group_resources_name` is later used to create an AWS CloudFormation stack. The value for `node_group_name` is later used to create the node group in your cluster.

```
cluster_name="my-cluster"
cluster_region="region-code"
node_group_resources_name="my-efa-nodegroup-resources"
node_group_name="my-efa-nodegroup"
```

2. Identify a private subnet in your VPC that is in the same Availability Zone as the instance type that you want to deploy is available in.
 - a. Retrieve the version of your cluster and store it in a variable for use in a later step.

```
cluster_version=$(aws eks describe-cluster \
--name $cluster_name \
--query "cluster.version" \
--output text)
```

- b. Retrieve the VPC ID that your cluster is in and store it in a variable for use in a later step.

```
vpc_id=$(aws eks describe-cluster \
--name $cluster_name \
--query "cluster.resourcesVpcConfig.vpcId" \
--output text)
```

- c. Retrieve the ID of the control plane security group for your cluster and store it in a variable for use in a later step.

```
control_plane_security_group=$(aws eks describe-cluster \
--name $cluster_name \
--query "cluster.resourcesVpcConfig.clusterSecurityGroupId" \
--output text)
```

- d. Get the list of subnet IDs in your VPC that are in an Availability Zone returned in step 1.

```
aws ec2 describe-subnets \
--filters "Name=vpc-id,Values=$vpc_id" "Name=availability-zone,Values=us-west-2a" \
--query 'Subnets[*].SubnetId' \
--output text
```

If no output is returned, try a different Availability Zone returned in step 1. If none of your subnets are in an Availability Zone returned in step 1, then you need to create a subnet in an Availability Zone returned in step 1. If you have no room in your VPC to create another subnet, then you may need to create a new cluster in a new VPC.

- e. Determine whether the subnet is a private subnet by checking the route table for the subnet.

```
aws ec2 describe-route-tables \
--filter Name=association.subnet-id,Values=subnet-0d403852a65210a29 \
--query "RouteTables[] .Routes[] .GatewayId" \
--output text
```

An example output is as follows.

```
local
```

If the output is **local igw-02adc64c1b72722e2**, then the subnet is a public subnet. You must select a private subnet in an Availability Zone returned in step 1. Once you've identified a private subnet, note its ID for use in a later step.

- f. Set a variable with the private subnet ID from the previous step for use in later steps.

```
subnet_id=your-subnet-id
```

3. Download the AWS CloudFormation template.

```
curl -O https://raw.githubusercontent.com/aws-samples/aws-efa-eks/main/cloudformation/efa-p4d-managed-nodegroup.yaml
```

4. Copy the following text to your computer. Replace *p4d.24xlarge* with an instance type from step 1. Replace *subnet-0d403852a65210a29* with the ID of the private subnet that you identified in step 2.b.v. Replace *path-to-downloaded-cfn-template* with the path to the efa-p4d-managed-nodegroup.yaml that you downloaded in the previous step. Replace *your-public-key-name* with the name of your public key. Once you've made the replacements, run the modified command.

```
aws cloudformation create-stack \
--stack-name ${node_group_resources_name} \
--capabilities CAPABILITY_IAM \
--template-body file://${path-to-downloaded-cfn-template} \
--parameters \
  ParameterKey=ClusterName,ParameterValue=${cluster_name} \
  ParameterKey=ClusterControlPlaneSecurityGroup,ParameterValue=
${control_plane_security_group} \
  ParameterKey=VpcId,ParameterValue=${vpc_id} \
  ParameterKey=SubnetId,ParameterValue=${subnet_id} \
  ParameterKey=NodeGroupName,ParameterValue=${node_group_name} \
  ParameterKey=NodeImageIdSSMParam,ParameterValue=/aws/service/eks/
optimized-ami/${cluster_version}/amazon-linux-2-gpu/recommended/image_id \
  ParameterKey=KeyName,ParameterValue=your-public-key-name \
  ParameterKey=NodeInstanceType,ParameterValue=p4d.24xlarge
```

5. Determine when the stack that you deployed in the previous step is deployed.

```
aws cloudformation wait stack-create-complete --stack-name
$node_group_resources_name
```

There is no output from the previous command, but your shell prompt doesn't return until the stack is created.

6. Create your node group using the resources created by the AWS CloudFormation stack in the previous step.
 - a. Retrieve information from the deployed AWS CloudFormation stack and store it in variables.

```
node_instance_role=$(aws cloudformation describe-stacks \
--stack-name $node_group_resources_name \
--query='Stacks[0].Outputs[?OutputKey==`NodeInstanceRole`].OutputValue' \
--output text)
launch_template=$(aws cloudformation describe-stacks \
--stack-name $node_group_resources_name \
--query='Stacks[0].Outputs[?OutputKey==`LaunchTemplateID`].OutputValue' \
--output text)
```

- b. Create a managed node group that uses the launch template and node IAM role that were created in the previous step.

```
aws eks create-nodegroup \
--cluster-name $cluster_name \
--nodegroup-name $node_group_name \
--node-role $node_instance_role \
--subnets $subnet_id \
--launch-template id=$launch_template,version=1
```

- c. Confirm that the nodes were created.

```
aws eks describe-nodegroup \
--cluster-name ${cluster_name} \
--nodegroup-name ${node_group_name} | jq -r .nodegroup.status
```

Don't continue until the status returned from the previous command is ACTIVE. It can take several minutes for the nodes to become ready.

7. If you chose a GPU instance type, you must deploy the [NVIDIA device plugin for Kubernetes](#). Replace `vX.X.X` with your desired [NVIDIA/k8s-device-plugin](#) version before running the following command.

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-
plugin/vX.X.X/nvidia-device-plugin.yaml
```

4. Deploy the EFA Kubernetes device plugin.

The EFA Kubernetes device plugin detects and advertises EFA interfaces as allocatable resources to Kubernetes. An application can consume the extended resource type `vpc.amazonaws.com/efa` in a Pod request spec just like CPU and memory. For more information, see [Consuming extended resources](#) in the Kubernetes documentation. Once requested, the plugin automatically assigns and mounts an EFA interface to the Pod. Using the device plugin simplifies EFA setup and does not require a Pod to run in privileged mode.

```
kubectl apply -f https://raw.githubusercontent.com/aws-samples/aws-efa-eks/main/
manifest/efa-k8s-device-plugin.yaml
```

(Optional) Deploy a sample EFA compatible application

Deploy the Kubeflow MPI Operator

For the NCCL tests you can apply the Kubeflow MPI Operator. The MPI Operator makes it easy to run Allreduce-style distributed training on Kubernetes. For more information, see [MPI Operator](#) on GitHub.

```
kubectl apply -f https://raw.githubusercontent.com/kubeflow/mpi-operator/master/deploy/
v2beta1/mpi-operator.yaml
```

Run the multi-node NCCL Performance Test to verify GPUDirectRDMA/EFA

To verify NCCL Performance with GPUDirectRDMA over EFA, run the standard NCCL Performance test. For more information, see the official [NCCL-Tests](#) repo on GitHub. You can use the sample [Dockerfile](#) that comes with this test already built for both [NVIDIA CUDA](#) 11.2 and the latest version of EFA.

Alternately, you can download an AWS Docker image available from an [Amazon ECR repo](#).

Important

An important consideration required for adopting EFA with Kubernetes is configuring and managing Huge Pages as a resource in the cluster. For more information, see [Manage Huge Pages](#) in the Kubernetes documentation. Amazon EC2 instances with the EFA driver installed pre-allocate 5128 2M Huge Pages, which you can request as resources to consume in your job specifications.

Complete the following steps to run a two node NCCL Performance Test. In the example NCCL test job, each worker requests eight GPUs, 5210Mi of hugepages-2Mi, four EFAs, and 8000Mi of memory, which effectively means each worker consumes all the resources of a p4d.24xlarge instance.

1. Create the NCCL-tests job.

```
kubectl apply -f https://raw.githubusercontent.com/aws-samples/aws-efa-eks/main/examples/simple/nccl-efa-tests.yaml
```

An example output is as follows.

```
mpijob.kubeflow.org/nccl-tests-efa created
```

2. View your running Pods.

```
kubectl get pods
```

An example output is as follows.

NAME	READY	STATUS	RESTARTS	AGE
nccl-tests-efa-launcher- <i>nbql9</i>	0/1	Init:0/1	0	2m49s
nccl-tests-efa-worker-0	1/1	Running	0	2m49s
nccl-tests-efa-worker-1	1/1	Running	0	2m49s

The MPI Operator creates a launcher Pod and 2 worker Pods (one on each node).

3. View the log for the efa-launcher Pod. Replace *wzr8j* with the value from your output.

```
kubectl logs -f nccl-tests-efa-launcher-nbql9
```

For more examples, see the Amazon EKS [EFA samples](#) repository on GitHub.

Machine learning inference using AWS Inferentia

This topic describes how to create an Amazon EKS cluster with nodes running [Amazon EC2 Inf1](#) instances and (optionally) deploy a sample application. Amazon EC2 Inf1 instances are powered by [AWS Inferentia](#) chips, which are custom built by AWS to provide high performance and lowest cost inference in the cloud. Machine learning models are deployed to containers using [AWS Neuron](#), a specialized software development kit (SDK) consisting of a compiler, runtime, and profiling tools that optimize the machine learning inference performance of Inferentia chips. AWS Neuron supports popular machine learning frameworks such as TensorFlow, PyTorch, and MXNet.

Note

Neuron device logical IDs must be contiguous. If a Pod requesting multiple Neuron devices is scheduled on an `inf1.6xlarge` or `inf1.24xlarge` instance type (which have more than one Neuron device), that Pod will fail to start if the Kubernetes scheduler selects non-contiguous device IDs. For more information, see [Device logical IDs must be contiguous](#) on GitHub.

Prerequisites

- Have `eksctl` installed on your computer. If you don't have it installed, see [Installing or updating eksctl \(p. 13\)](#) for installation instructions.
- Have `kubectl` installed on your computer. For more information, see [Installing or updating kubectl \(p. 6\)](#).
- (Optional) Have `python3` installed on your computer. If you don't have it installed, then see [Python downloads](#) for installation instructions.

Create a cluster

To create a cluster with Inf1 Amazon EC2 instance nodes

1. Create a cluster with Inf1 Amazon EC2 instance nodes. You can replace `inf1.2xlarge` with any [Inf1 instance type](#). The `eksctl` utility detects that you are launching a node group with an Inf1 instance type and will start your nodes using one of the Amazon EKS optimized accelerated Amazon Linux AMIs.

Note

You can't use [IAM roles for service accounts \(p. 464\)](#) with TensorFlow Serving.

```
eksctl create cluster \
--name inferentia \
--region region-code \
--nodegroup-name ng-inf1 \
--node-type inf1.2xlarge \
--nodes 2 \
--nodes-min 1 \
--nodes-max 4 \
--ssh-access \
--ssh-public-key your-key \
--with-oidc
```

Note

Note the value of the following line of the output. It's used in a later (optional) step.

```
[9] adding identity "arn:aws:iam::11122223333:role/
eksctl-inferentia-nodegroup-ng-in-NodeInstanceRole-FI7HIYS3BS09" to auth
ConfigMap
```

When launching a node group with Inf1 instances, `eksctl` automatically installs the AWS Neuron Kubernetes device plugin. This plugin advertises Neuron devices as a system resource to the Kubernetes scheduler, which can be requested by a container. In addition to the default Amazon EKS node IAM policies, the Amazon S3 read only access policy is added so that the sample application, covered in a later step, can load a trained model from Amazon S3.

2. Make sure that all Pods have started correctly.

```
kubectl get pods -n kube-system
```

Abbreviated output:

NAME	READY	STATUS	RESTARTS	AGE
[...]				
neuron-device-plugin-daemonset- 6djhfp	1/1	Running	0	5m
neuron-device-plugin-daemonset- hwjsj	1/1	Running	0	5m

(Optional) Deploy a TensorFlow Serving application image

A trained model must be compiled to an Inferentia target before it can be deployed on Inferentia instances. To continue, you will need a [Neuron optimized TensorFlow](#) model saved in Amazon S3. If you don't already have a SavedModel, please follow the tutorial for [creating a Neuron compatible ResNet50 model](#) and upload the resulting SavedModel to S3. ResNet-50 is a popular machine learning model

used for image recognition tasks. For more information about compiling Neuron models, see [The AWS Inferentia Chip With DLAMI](#) in the AWS Deep Learning AMI Developer Guide.

The sample deployment manifest manages a pre-built inference serving container for TensorFlow provided by AWS Deep Learning Containers. Inside the container is the AWS Neuron Runtime and the TensorFlow Serving application. A complete list of pre-built Deep Learning Containers optimized for Neuron is maintained on GitHub under [Available Images](#). At start-up, the DLC will fetch your model from Amazon S3, launch Neuron TensorFlow Serving with the saved model, and wait for prediction requests.

The number of Neuron devices allocated to your serving application can be adjusted by changing the `aws.amazon.com/neuron` resource in the deployment yaml. Please note that communication between TensorFlow Serving and the Neuron runtime happens over GRPC, which requires passing the `IPC_LOCK` capability to the container.

1. Add the `AmazonS3ReadOnlyAccess` IAM policy to the node instance role that was created in step 1 of [Create a cluster \(p. 416\)](#). This is necessary so that the sample application can load a trained model from Amazon S3.

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess \
--role-name eksctl-inferentia-nodegroup-ing-in-NodeInstanceRole-FI7HIYS3BS09
```

2. Create a file named `rn50_deployment.yaml` with the following contents. Update the region-code and model path to match your desired settings. The model name is for identification purposes when a client makes a request to the TensorFlow server. This example uses a model name to match a sample ResNet50 client script that will be used in a later step for sending prediction requests.

```
aws ecr list-images --repository-name neuron-rtd --registry-id 790709498068 --
region us-west-2
```

```
kind: Deployment
apiVersion: apps/v1
metadata:
  name: eks-neuron-test
  labels:
    app: eks-neuron-test
    role: master
spec:
  replicas: 2
  selector:
    matchLabels:
      app: eks-neuron-test
      role: master
  template:
    metadata:
      labels:
        app: eks-neuron-test
        role: master
    spec:
      containers:
        - name: eks-neuron-test
          image: 763104351884.dkr.ecr.us-east-1.amazonaws.com/tensorflow-inference-
neuron:1.15.4-neuron-py37-ubuntu18.04
          command:
            - /usr/local/bin/entrypoint.sh
          args:
            - --port=8500
            - --rest_api_port=9000
            - --model_name=resnet50_neuron
            - --model_base_path=s3://your-bucket-of-models/resnet50_neuron/
  ports:
```

```
- containerPort: 8500
- containerPort: 9000
imagePullPolicy: IfNotPresent
env:
- name: AWS_REGION
  value: "us-east-1"
- name: S3_USE_HTTPS
  value: "1"
- name: S3_VERIFY_SSL
  value: "0"
- name: S3_ENDPOINT
  value: s3.us-east-1.amazonaws.com
- name: AWS_LOG_LEVEL
  value: "3"
resources:
limits:
  cpu: 4
  memory: 4Gi
  aws.amazon.com/neuron: 1
requests:
  cpu: "1"
  memory: 1Gi
securityContext:
capabilities:
  add:
    - IPC_LOCK
```

3. Deploy the model.

```
kubectl apply -f rn50_deployment.yaml
```

4. Create a file named `rn50_service.yaml` with the following contents. The HTTP and gRPC ports are opened for accepting prediction requests.

```
kind: Service
apiVersion: v1
metadata:
  name: eks-neuron-test
  labels:
    app: eks-neuron-test
spec:
  type: ClusterIP
  ports:
    - name: http-tf-serving
      port: 8500
      targetPort: 8500
    - name: grpc-tf-serving
      port: 9000
      targetPort: 9000
  selector:
    app: eks-neuron-test
    role: master
```

5. Create a Kubernetes service for your TensorFlow model Serving application.

```
kubectl apply -f rn50_service.yaml
```

(Optional) Make predictions against your TensorFlow Serving service

1. To test locally, forward the gRPC port to the eks-neuron-test service.

```
kubectl port-forward service/eks-neuron-test 8500:8500 &
```

2. Create a Python script called tensorflow-model-server-infer.py with the following content. This script runs inference via gRPC, which is service framework.

```
import numpy as np
import grpc
import tensorflow as tf
from tensorflow.keras.preprocessing import image
from tensorflow.keras.applications.resnet50 import preprocess_input
from tensorflow_serving.apis import predict_pb2
from tensorflow_serving.apis import prediction_service_pb2_grpc
from tensorflow.keras.applications.resnet50 import decode_predictions

if __name__ == '__main__':
    channel = grpc.insecure_channel('localhost:8500')
    stub = prediction_service_pb2_grpc.PredictionServiceStub(channel)
    img_file = tf.keras.utils.get_file(
        './kitten_small.jpg',
        "https://raw.githubusercontent.com/awslabs/mxnet-model-server/master/docs/images/kitten_small.jpg")
    img = image.load_img(img_file, target_size=(224, 224))
    img_array = preprocess_input(image.img_to_array(img)[None, ...])
    request = predict_pb2.PredictRequest()
    request.model_spec.name = 'resnet50_inf1'
    request.inputs['input'].CopyFrom(
        tf.make_tensor_proto(img_array, shape=img_array.shape))
    result = stub.Predict(request)
    prediction = tf.make_ndarray(result.outputs['output'])
    print(decode_predictions(prediction))
```

3. Run the script to submit predictions to your service.

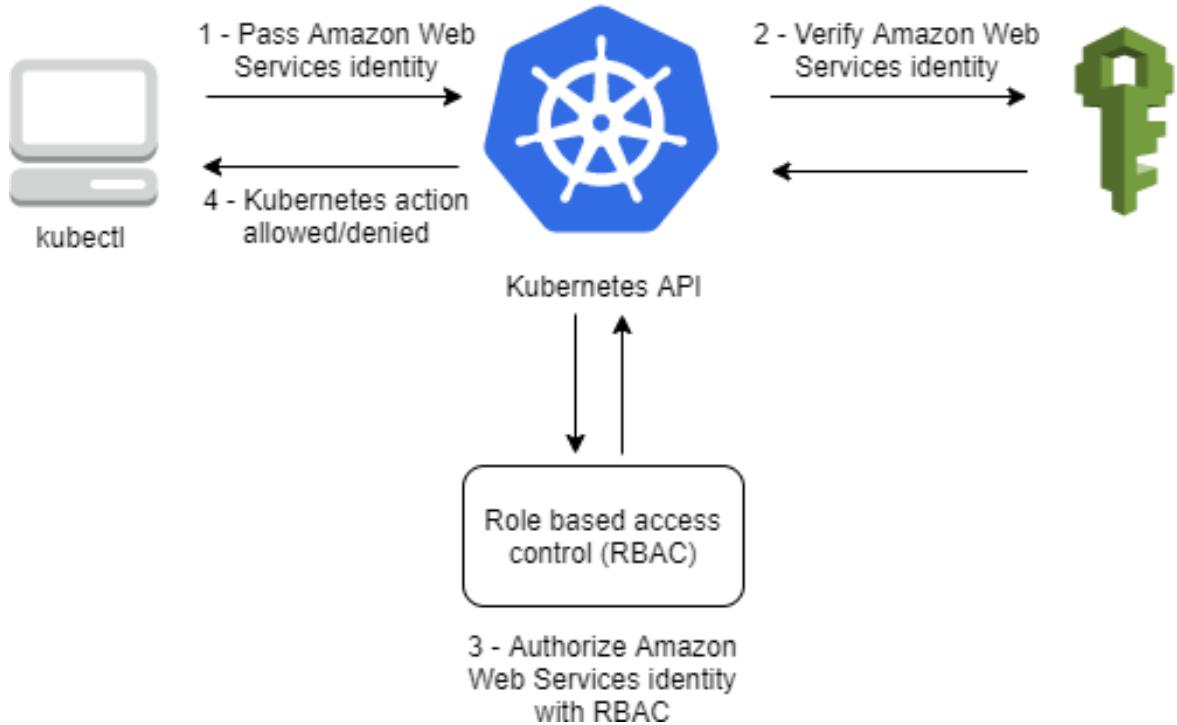
```
python3 tensorflow-model-server-infer.py
```

An example output is as follows.

```
[[u'n02123045', u'tabby', 0.68817204), (u'n02127052', u'lynx', 0.12701613),
(u'n02123159', u'tiger_cat', 0.08736559), (u'n02124075', u'Egyptian_cat',
0.063844085), (u'n02128757', u'snow_leopard', 0.009240591)]]
```

Cluster authentication

Amazon EKS uses IAM to provide authentication to your Kubernetes cluster (through the `aws_eks get-token` command, available in version 1.16.156 or later of the AWS CLI, or the [AWS IAM Authenticator for Kubernetes](#)), but it still relies on native Kubernetes [Role Based Access Control](#) (RBAC) for authorization. This means that IAM is only used for authentication of valid IAM entities. All permissions for interacting with your Amazon EKS cluster's Kubernetes API is managed through the native Kubernetes RBAC system. The following picture shows this relationship.



Note

Amazon EKS uses the authentication token to make the `sts:GetCallerIdentity` call. As a result, AWS CloudTrail events with the name `GetCallerIdentity` from the source `sts.amazonaws.com` can have Amazon EKS service IP addresses for their source IP address.

Topics

- [Enabling IAM principal access to your cluster \(p. 420\)](#)
- [Authenticating users for your cluster from an OpenID Connect identity provider \(p. 427\)](#)
- [Creating or updating a kubeconfig file for an Amazon EKS cluster \(p. 431\)](#)
- [Installing aws-iam-authenticator \(p. 436\)](#)
- [Default Amazon EKS created Kubernetes roles and users \(p. 440\)](#)

Enabling IAM principal access to your cluster

Access to your cluster using [IAM principals](#) is enabled by the [AWS IAM Authenticator for Kubernetes](#), which runs on the Amazon EKS control plane. The authenticator gets its configuration information from the `aws-auth` ConfigMap. For all `aws-auth` ConfigMap settings, see [Full Configuration Format](#) on GitHub.

Add IAM principals to your Amazon EKS cluster

When you create an Amazon EKS cluster, the [IAM principal](#) that creates the cluster is automatically granted system:masters permissions in the cluster's role-based access control (RBAC) configuration in the Amazon EKS control plane. This principal doesn't appear in any visible configuration, so make sure to keep track of which principal originally created the cluster. To grant additional IAM principals the ability to interact with your cluster, edit the aws-auth ConfigMap within Kubernetes and create a Kubernetes rolebinding or clusterrolebinding with the name of a group that you specify in the aws-auth ConfigMap.

Note

For more information about Kubernetes role-based access control (RBAC) configuration, see [Using RBAC Authorization](#) in the Kubernetes documentation.

To add an IAM principal to an Amazon EKS cluster

1. Determine which credentials kubectl is using to access your cluster. On your computer, you can see which credentials kubectl uses with the following command. Replace `~/.kube/config` with the path to your kubeconfig file if you don't use the default path.

```
cat ~/.kube/config
```

An example output is as follows.

```
[...]
contexts:
- context:
    cluster: my-cluster.region-code.eksctl.io
    user: admin@my-cluster.region-code.eksctl.io
    name: admin@my-cluster.region-code.eksctl.io
current-context: admin@my-cluster.region-code.eksctl.io
[...]
```

In the previous example output, the credentials for a user named `admin` are configured for a cluster named `my-cluster`. If this is the user that created the cluster, then it already has access to your cluster. If it's not the user that created the cluster, then you need to complete the remaining steps to enable cluster access for other IAM principals. [IAM best practices](#) recommend that you grant permissions to roles instead of users. You can see which other principals currently have access to your cluster with the following command:

```
kubectl describe -n kube-system configmap/aws-auth
```

An example output is as follows.

```
Name:      aws-auth
Namespace: kube-system
Labels:    <none>
Annotations: <none>

Data
=====
mapRoles:
-----
- groups:
  - system:bootstrappers
  - system:nodes
  rolearn: arn:aws:iam::111122223333:role/my-node-role
  username: system:node:{EC2PrivateDNSName}
```

```
BinaryData
=====
Events: <none>
```

The previous example is a default aws-auth ConfigMap. Only the node instance role has access to the cluster.

2. Make sure that you have existing Kubernetes roles and rolebindings or clusterroles and clusterrolebindings that you can map IAM principals to. For more information about these resources, see [Using RBAC Authorization](#) in the Kubernetes documentation.
 1. View your existing Kubernetes roles or clusterroles. Roles are scoped to a namespace, but clusterroles are scoped to the cluster.

```
kubectl get roles -A
```

```
kubectl get clusterroles
```

2. View the details of any role or clusterrole returned in the previous output and confirm that it has the permissions (rules) that you want your IAM principals to have in your cluster.

Replace *role-name* with a role name returned in the output from the previous command. Replace *kube-system* with the namespace of the role.

```
kubectl describe role role-name -n kube-system
```

Replace *cluster-role-name* with a clusterrole name returned in the output from the previous command.

```
kubectl describe clusterrole cluster-role-name
```

3. View your existing Kubernetes rolebindings or clusterrolebindings. Rolebindings are scoped to a namespace, but clusterrolebindings are scoped to the cluster.

```
kubectl get rolebindings -A
```

```
kubectl get clusterrolebindings
```

4. View the details of any rolebinding or clusterrolebinding and confirm that it has a role or clusterrole from the previous step listed as a roleRef and a group name listed for subjects.

Replace *role-binding-name* with a rolebinding name returned in the output from the previous command. Replace *kube-system* with the namespace of the rolebinding.

```
kubectl describe rolebinding role-binding-name -n kube-system
```

An example output is as follows.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: eks-console-dashboard-restricted-access-role-binding
```

```
namespace: default
subjects:
- kind: Group
  name: eks-console-dashboard-restricted-access-group
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: eks-console-dashboard-restricted-access-role
  apiGroup: rbac.authorization.k8s.io
```

Replace `cluster-role-binding-name` with a `clusterrolebinding` name returned in the output from the previous command.

```
kubectl describe clusterrolebinding cluster-role-binding-name
```

An example output is as follows.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: eks-console-dashboard-full-access-binding
subjects:
- kind: Group
  name: eks-console-dashboard-full-access-group
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: eks-console-dashboard-full-access-clusterrole
  apiGroup: rbac.authorization.k8s.io
```

3. Edit the `aws-auth` ConfigMap. You can use a tool such as `eksctl` to update the ConfigMap or you can update it manually by editing it.

Important

We recommend using `eksctl`, or another tool, to edit the ConfigMap. For information about other tools you can use, see [Use tools to make changes to the `aws-authConfigMap`](#) in the Amazon EKS best practices guides. An improperly formatted `aws-auth` ConfigMap can cause you to lose access to your cluster.

`eksctl`

Prerequisite

Version 0.160.0 or later of the `eksctl` command line tool installed on your device or AWS CloudShell. To install or update `eksctl`, see [Installing or updating `eksctl` \(p. 13\)](#).

1. View the current mappings in the ConfigMap. Replace `my-cluster` with the name of your cluster. Replace `region-code` with the AWS Region that your cluster is in.

```
eksctl get iamidentitymapping --cluster my-cluster --region=region-code
```

An example output is as follows.

ARN	USERNAME	GROUPS
ACCOUNT		
arn:aws:iam::111122223333:role/ <code>eksctl-my-cluster-my-nodegroup-NodeInstanceRole-1XLS7754U3ZPA</code>	system:node:{{EC2PrivateDNSName}}	
	system:bootstrappers,system:nodes	

2. Add a mapping for a role. Replace `my-role` with your role name. Replace `eks-console-dashboard-full-access-group` with the name of the group specified in your Kubernetes RoleBinding or ClusterRoleBinding object. Replace `111122223333` with your account ID. You can replace `admin` with any name you choose.

```
eksctl create iamidentitymapping --cluster my-cluster --region=region-code \
--arn arn:aws:iam::111122223333:role/my-role --username admin --group eks-
console-dashboard-full-access-group \
--no-duplicate-arns
```

Important

The role ARN can't include a path such as `role/my-team/developers/my-role`.

The format of the ARN must be `arn:aws:iam::111122223333:role/my-role`.

In this example, `my-team/developers/` needs to be removed.

An example output is as follows.

```
[...]
2022-05-09 14:51:20 [#] adding identity "arn:aws:iam::111122223333:role/my-role"
to auth ConfigMap
```

3. Add a mapping for a user. [IAM best practices](#) recommend that you grant permissions to roles instead of users. Replace `my-user` with your user name. Replace `eks-console-dashboard-restricted-access-group` with the name of the group specified in your Kubernetes RoleBinding or ClusterRoleBinding object. Replace `111122223333` with your account ID. You can replace `my-user` with any name you choose.

```
eksctl create iamidentitymapping --cluster my-cluster --region=region-code \
--arn arn:aws:iam::111122223333:user/my-user --username my-user --group eks-
console-dashboard-restricted-access-group \
--no-duplicate-arns
```

An example output is as follows.

```
[...]
2022-05-09 14:53:48 [#] adding identity "arn:aws:iam::111122223333:user/my-user"
to auth ConfigMap
```

4. View the mappings in the ConfigMap again.

```
eksctl get iamidentitymapping --cluster my-cluster --region=region-code
```

An example output is as follows.

ARN	USERNAME	ACCOUNT	GROUPS
<code>arn:aws:iam::111122223333:role/eksctl-my-cluster-my-nodegroup-NodeInstanceRole-1XLS7754U3ZPA</code>	<code>system:node:{EC2PrivateDNSName}</code>	<code>system:bootstrappers,system:nodes</code>	<code>eks-console-dashboard-full-access-group</code>
<code>arn:aws:iam::111122223333:role/admin</code>	<code>my-role</code>		<code>eks-console-dashboard-restricted-access-group</code>
<code>arn:aws:iam::111122223333:user/my-user</code>	<code>my-user</code>		<code>eks-console-dashboard-restricted-access-group</code>

Edit ConfigMap manually

1. Open the ConfigMap for editing.

```
kubectl edit -n kube-system configmap/aws-auth
```

Note

If you receive an error stating "Error from server (NotFound): configmaps \"aws-auth\" not found", then use the procedure in [Apply the aws-authConfigMap to your cluster \(p. 426\)](#) to apply the stock ConfigMap.

2. Add your IAM principals to the ConfigMap. An IAM group isn't an IAM principal, so it can't be added to the ConfigMap.

- **To add an IAM role (for example, for federated users):** Add the role details to the mapRoles section of the ConfigMap, under data. Add this section if it does not already exist in the file. Each entry supports the following parameters:
 - **rolearn:** The ARN of the IAM role to add. This value can't include a path. For example, you can't specify an ARN such as `arn:aws:iam::111122223333:role/my-team/developers/role-name`. The ARN needs to be `arn:aws:iam::111122223333:role/role-name` instead.
 - **username:** The user name within Kubernetes to map to the IAM role.
 - **groups:** The group or list of Kubernetes groups to map the role to. The group can be a default group, or a group specified in a clusterrolebinding or rolebinding. For more information, see [Default roles and role bindings](#) in the Kubernetes documentation.
- **To add an IAM user:** [IAM best practices](#) recommend that you grant permissions to roles instead of users. Add the user details to the mapUsers section of the ConfigMap, under data. Add this section if it does not already exist in the file. Each entry supports the following parameters:
 - **userarn:** The ARN of the IAM user to add.
 - **username:** The user name within Kubernetes to map to the IAM user.
 - **groups:** The group, or list of Kubernetes groups to map the user to. The group can be a default group, or a group specified in a clusterrolebinding or rolebinding. For more information, see [Default roles and role bindings](#) in the Kubernetes documentation.

For example, the following YAML block contains:

- A mapRoles section that maps the IAM node instance to Kubernetes groups so that nodes can register themselves with the cluster and the my-console-viewer-role IAM role that is mapped to a Kubernetes group that can view all Kubernetes resources for all clusters. For a list of the IAM and Kubernetes group permissions required for the my-console-viewer-role IAM role, see [Required permissions \(p. 529\)](#).
- A mapUsers section that maps the admin IAM user from the default AWS account to the system:masters Kubernetes group and the my-user user from a different AWS account that is mapped to a Kubernetes group that can view Kubernetes resources for a specific namespace. For a list of the IAM and Kubernetes group permissions required for the my-user IAM user, see [Required permissions \(p. 529\)](#).

Add or remove lines as necessary and replace all *example values* with your own values.

```
# Please edit the object below. Lines beginning with a '#' will be ignored,  
# and an empty file will abort the edit. If an error occurs while saving this  
file will be  
# reopened with the relevant failures.  
#  
apiVersion: v1
```

```

data:
  mapRoles: |
    - groups:
      - system:bootstrappers
      - system:nodes
      rolearn: arn:aws:iam::111122223333:role/my-role
      username: system:node:{{EC2PrivateDNSName}}
    - groups:
      - eks-console-dashboard-full-access-group
      rolearn: arn:aws:iam::111122223333:role/my-console-viewer-role
      username: my-console-viewer-role
  mapUsers: |
    - groups:
      - system:masters
      userarn: arn:aws:iam::111122223333:user/admin
      username: admin
    - groups:
      - eks-console-dashboard-restricted-access-group
      userarn: arn:aws:iam::444455556666:user/my-user
      username: my-user

```

3. Save the file and exit your text editor.

Apply the aws-authConfigMap to your cluster

The aws-auth ConfigMap is automatically created and applied to your cluster when you create a managed node group or when you create a node group using eksctl. It is initially created to allow nodes to join your cluster, but you also use this ConfigMap to add role-based access control (RBAC) access to IAM principals. If you've launched self-managed nodes and haven't applied the aws-auth ConfigMap to your cluster, you can do so with the following procedure.

To apply the aws-authConfigMap to your cluster

1. Check to see if you've already applied the aws-auth ConfigMap.

```
kubectl describe configmap -n kube-system aws-auth
```

If you receive an error stating "Error from server (NotFound): configmaps "aws-auth" not found", then proceed with the following steps to apply the stock ConfigMap.

2. Download, edit, and apply the AWS authenticator configuration map.
 - a. Download the configuration map.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/clouformation/2020-10-29/
aws-auth-cm.yaml
```

- b. In the aws-auth-cm.yaml file, set the rolearn to the Amazon Resource Name (ARN) of the IAM role associated with your nodes. You can do this with a text editor, or by replacing *my-node-instance-role* and running the following command:

```
sed -i.bak -e 's|<ARN of instance role (not instance profile)>|my-node-instance-role' aws-auth-cm.yaml
```

Don't modify any other lines in this file.

Important

The role ARN can't include a path such as `role/my-team/developers/my-role`. The format of the ARN must be `arn:aws:iam::1112222333:role/my-role`. In this example, `my-team/developers/` needs to be removed.

You can inspect the AWS CloudFormation stack outputs for your node groups and look for the following values:

- **InstanceRoleARN** – For node groups that were created with `eksctl`
 - **NodeInstanceRole** – For node groups that were created with Amazon EKS vended AWS CloudFormation templates in the AWS Management Console
- c. Apply the configuration. This command may take a few minutes to finish.

```
kubectl apply -f aws-auth-cm.yaml
```

Note

If you receive any authorization or resource type errors, see [Unauthorized or access denied \(kubectl\) \(p. 563\)](#) in the troubleshooting topic.

3. Watch the status of your nodes and wait for them to reach the Ready status.

```
kubectl get nodes --watch
```

Enter Ctrl+C to return to a shell prompt.

Authenticating users for your cluster from an OpenID Connect identity provider

Amazon EKS supports using OpenID Connect (OIDC) identity providers as a method to authenticate users to your cluster. OIDC identity providers can be used with, or as an alternative to AWS Identity and Access Management (IAM). For more information about using IAM, see [Enabling IAM principal access to your cluster \(p. 420\)](#). After configuring authentication to your cluster, you can create Kubernetes roles and clusterroles to assign permissions to the roles, and then bind the roles to the identities using Kubernetes rolebindings and clusterrolebindings. For more information, see [Using RBAC Authorization](#) in the Kubernetes documentation.

Considerations

- You can associate one OIDC identity provider to your cluster.
- Kubernetes doesn't provide an OIDC identity provider. You can use an existing public OIDC identity provider, or you can run your own identity provider. For a list of certified providers, see [OpenID Certification](#) on the OpenID site.
- The issuer URL of the OIDC identity provider must be publicly accessible, so that Amazon EKS can discover the signing keys. Amazon EKS does not support OIDC identity providers with self-signed certificates.
- You can't disable the AWS IAM authenticator on your cluster, because it is still required for joining nodes to a cluster. For more information, see [AWS IAM Authenticator for Kubernetes](#) on GitHub.
- An Amazon EKS cluster must still be created by an AWS [IAM principal](#), rather than an OIDC identity provider user. This is because the cluster creator interacts with the Amazon EKS APIs, rather than the Kubernetes APIs.

- OIDC identity provider-authenticated users are listed in the cluster's audit log if CloudWatch logs are turned on for the control plane. For more information, see [Enabling and disabling control plane logs \(p. 537\)](#).
- You can't sign in to the AWS Management Console with an account from an OIDC provider. You can only [view Kubernetes resources \(p. 529\)](#) in the console by signing into the AWS Management Console with an AWS Identity and Access Management account.

Associate an OIDC identity provider

Before you can associate an OIDC identity provider with your cluster, you need the following information from your provider:

Issuer URL

The URL of the OIDC identity provider that allows the API server to discover public signing keys for verifying tokens. The URL must begin with `https://` and should correspond to the `iss` claim in the provider's OIDC ID tokens. In accordance with the OIDC standard, path components are allowed but query parameters are not. Typically the URL consists of only a host name, like `https://server.example.org` or `https://example.com`. This URL should point to the level below `.well-known/openid-configuration` and must be publicly accessible over the internet.

Client ID (also known as *audience*)

The ID for the client application that makes authentication requests to the OIDC identity provider.

You can associate an identity provider using `eksctl` or the AWS Management Console.

`eksctl`

To associate an OIDC identity provider to your cluster using `eksctl`

- Create a file named `associate-identity-provider.yaml` with the following contents. Replace the `example values` with your own. The values in the `identityProviders` section are obtained from your OIDC identity provider. Values are only required for the `name`, `type`, `issuerUrl`, and `clientId` settings under `identityProviders`.

```
---
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-cluster
  region: your-region-code

identityProviders:
  - name: my-provider
    type: oidc
    issuerUrl: https://example.com
    clientId: kubernetes
    usernameClaim: email
    usernamePrefix: my-username-prefix
    groupsClaim: my-claim
    groupsPrefix: my-groups-prefix
    requiredClaims:
      string: string
    tags:
      env: dev
```

Important

Don't specify system:, or any portion of that string, for groupsPrefix or usernamePrefix.

2. Create the provider.

```
eksctl associate identityprovider -f associate-identity-provider.yaml
```

3. To use kubectl to work with your cluster and OIDC identity provider, see [Using kubectl](#) in the Kubernetes documentation.

AWS Management Console

To associate an OIDC identity provider to your cluster using the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Select your cluster.
3. Select the **Configuration** tab, and then select the **Authentication** tab.
4. On the **OIDC Identity Providers** page, select **Associate Identity Provider**.
5. On the **Associate OIDC Identity Provider** page, enter or select the following options, and then select **Associate**.
 - For **Name**, enter a unique name for the provider.
 - For **Issuer URL**, enter the URL for your provider. This URL must be accessible over the internet.
 - For **Client ID**, enter the OIDC identity provider's client ID (also known as **audience**).
 - For **Username claim**, enter the claim to use as the username.
 - For **Groups claim**, enter the claim to use as the user's group.
 - (Optional) Select **Advanced options**, enter or select the following information.
 - **Username prefix** – Enter a prefix to prepend to username claims. The prefix is prepended to username claims to prevent clashes with existing names. If you do not provide a value, and the username is a value other than email, the prefix defaults to the value for **Issuer URL**. You can use the value – to disable all prefixing. Don't specify system: or any portion of that string.
 - **Groups prefix** – Enter a prefix to prepend to groups claims. The prefix is prepended to group claims to prevent clashes with existing names (such as `system: groups`). For example, the value `oidc:` creates group names like `oidc:engineering` and `oidc:infra`. Don't specify system: or any portion of that string..
 - **Required claims** – Select **Add claim** and enter one or more key value pairs that describe required claims in the client ID token. The pairs describe required claims in the ID Token. If set, each claim is verified to be present in the ID token with a matching value.
6. To use kubectl to work with your cluster and OIDC identity provider, see [Using kubectl](#) in the Kubernetes documentation.

Disassociate an OIDC identity provider from your cluster

If you disassociate an OIDC identity provider from your cluster, users included in the provider can no longer access the cluster. However, you can still access the cluster with [IAM principals](#).

To disassociate an OIDC identity provider from your cluster using the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the **OIDC Identity Providers** section, select **Disassociate**, enter the identity provider name, and then select **Disassociate**.

Example IAM policy

If you want to prevent an OIDC identity provider from being associated with a cluster, create and associate the following IAM policy to the IAM accounts of your Amazon EKS administrators. For more information, see [Creating IAM policies](#) and [Adding IAM identity permissions](#) in the IAM User Guide and [Actions, resources, and condition keys for Amazon Elastic Kubernetes Service](#) in the Service Authorization Reference.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "denyOIDC",
            "Effect": "Deny",
            "Action": [
                "eks:AssociateIdentityProviderConfig"
            ],
            "Resource": "arn:aws:eks:us-west-2.amazonaws.com:111122223333:cluster/*"
        },
        {
            "Sid": "eksAdmin",
            "Effect": "Allow",
            "Action": [
                "eks:)"
            ],
            "Resource": "*"
        }
    ]
}
```

The following example policy allows OIDC identity provider association if the `clientID` is `kubernetes` and the `issuerUrl` is `https://cognito-idp.us-west-2amazonaws.com/*`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCognitoOnly",
            "Effect": "Deny",
            "Action": "eks:AssociateIdentityProviderConfig",
            "Resource": "arn:aws:eks:us-west-2:111122223333:cluster/my-instance",
            "Condition": {
                "StringNotLikeIfExists": {
                    "eks:issuerUrl": "https://cognito-idp.us-west-2.amazonaws.com/*"
                }
            }
        },
        {
            "Sid": "DenyOtherClients",
            "Effect": "Deny",
            "Action": "eks:AssociateIdentityProviderConfig",
            "Resource": "arn:aws:eks:us-west-2:111122223333:cluster/my-instance",
            "Condition": {
                "StringNotLikeIfExists": {
                    "eks:clientID": "kubernetes"
                }
            }
        }
    ]
}
```

```

        "Condition": {
            "StringNotEquals": {
                "eks:clientId": "kubernetes"
            }
        },
    {
        "Sid": "AllowOthers",
        "Effect": "Allow",
        "Action": "eks:*",
        "Resource": "*"
    }
]
}

```

Partner validated OIDC identity providers

Amazon EKS maintains relationships with a network of partners that offer support for compatible OIDC identity providers. Refer to the following partners' documentation for details on how to integrate the identity provider with Amazon EKS.

Partner	Product	Documentation
Pingidentity	PingOne for Enterprise	Installation instructions

Amazon EKS aims to give you a wide selection of options to cover all use cases. If you develop a commercially supported OIDC compatible identity provider that is not listed here, then contact our partner team at aws-container-partners@amazon.com for more information.

Creating or updating a kubeconfig file for an Amazon EKS cluster

In this topic, you create a kubeconfig file for your cluster (or update an existing one).

The `kubectl` command-line tool uses configuration information in kubeconfig files to communicate with the API server of a cluster. For more information, see [Organizing Cluster Access Using kubeconfig Files](#) in the Kubernetes documentation. This topic provides two procedures to create or update a kubeconfig file for your Amazon EKS cluster:

- Creating it automatically with the AWS CLI `update-kubeconfig` command.
- Creating it manually using the AWS CLI or the `aws-iam-authenticator`.

Amazon EKS uses the `aws eks get-token` command, available in version 1.16.156 or later of the AWS CLI or the [AWS IAM Authenticator for Kubernetes](#) with `kubectl` for cluster authentication. If you have installed the AWS CLI on your system, then by default the AWS IAM Authenticator for Kubernetes uses the same credentials that are returned with the following command:

```
aws sts get-caller-identity
```

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Getting started with Amazon EKS \(p. 6\)](#).

- The `kubectl` command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use `kubectl` version 1.26, 1.27, or 1.28 with it. To install or upgrade `kubectl`, see [Installing or updating `kubectl` \(p. 6\)](#).

Create kubeconfig file automatically

Prerequisites

- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such `yum`, `apt-get`, or `Homebrew` for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with `aws configure`](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.
- Permission to use the `eks :DescribeCluster` API action for the cluster that you specify. For more information, see [Amazon EKS identity-based policy examples \(p. 485\)](#).

To create your kubeconfig file with the AWS CLI

1. Create or update a kubeconfig file for your cluster. Replace `region-code` with the AWS Region that your cluster is in and replace `my-cluster` with the name of your cluster.

```
aws eks update-kubeconfig --region region-code --name my-cluster
```

By default, the resulting configuration file is created at the default kubeconfig path (`.kube`) in your home directory or merged with an existing config file at that location. You can specify another path with the `--kubeconfig` option.

You can specify an IAM role ARN with the `--role-arn` option to use for authentication when you issue `kubectl` commands. Otherwise, the [IAM principal](#) in your default AWS CLI or SDK credential chain is used. You can view your default AWS CLI or SDK identity by running the `aws sts get-caller-identity` command.

For all available options, run the `aws eks update-kubeconfig help` command or see [update-kubeconfig](#) in the *AWS CLI Command Reference*.

2. Test your configuration.

```
kubectl get svc
```

An example output is as follows.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
svc/kubernetes	ClusterIP	10.100.0.1	<none>	443/TCP	1m

If you receive any authorization or resource type errors, see [Unauthorized or access denied \(kubectl\) \(p. 563\)](#) in the troubleshooting topic.

Create kubeconfig file manually

To create your kubeconfig file manually

1. Set values for a few variables by replacing the *example values* with your own and then running the modified commands.

```
export region_code=region-code
export cluster_name=my-cluster
export account_id=111122223333
```

2. Retrieve the endpoint for your cluster and store the value in a variable.

```
cluster_endpoint=$(aws eks describe-cluster \
--region $region_code \
--name $cluster_name \
--query "cluster.endpoint" \
--output text)
```

3. Retrieve the Base64-encoded certificate data required to communicate with your cluster and store the value in a variable.

```
certificate_data=$(aws eks describe-cluster \
--region $region_code \
--name $cluster_name \
--query "cluster.certificateAuthority.data" \
--output text)
```

4. Create the default `~/.kube` directory if it doesn't already exist.

```
mkdir -p ~/.kube
```

5. Run one of the following commands for your preferred client token method (AWS CLI or AWS IAM authenticator for Kubernetes) to create the config file in the `~/.kube` directory. You can specify the following before running one of the commands by modifying the command to include the following:

- **An IAM role** – Remove the # at the start of the lines under `args::`. Replace `my-role` with the name of the IAM role that you want to perform cluster operations with instead of the default AWS credential provider chain. For more information, see [Set up kubectl to use authentication tokens provided by AWS IAM Authenticator for Kubernetes](#) on GitHub.
- **An AWS CLI named profile** – Remove the # at the start of the `env:` line, and remove # at the start of the lines under it. Replace `aws-profile` with the name of the profile to use. If you don't specify a profile, then the default profile is used. For additional information, see [Specifying Credentials & Using AWS Profiles](#) on GitHub.

AWS CLI

Prerequisite

Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed

in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.

```
#!/bin/bash
read -r -d '' KUBECONFIG <<EOF
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: $certificate_data
    server: $cluster_endpoint
  name: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
contexts:
- context:
    cluster: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
    user: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
  name: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
current-context: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
kind: Config
preferences: {}
users:
- name: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
  user:
    exec:
      apiVersion: client.authentication.k8s.io/v1beta1
      command: aws
      args:
        - --region
        - $region_code
        - eks
        - get-token
        - --cluster-name
        - $cluster_name
        # - --role
        # - "arn:aws:iam::$account_id:role/my-role"
    # env:
    # - name: "AWS_PROFILE"
    #   value: "aws-profile"
EOF
echo "${KUBECONFIG}" > ~/.kube/config
```

AWS IAM Authenticator for Kubernetes

Prerequisite

Version 0.5.9 or later of the AWS IAM Authenticator for Kubernetes installed on your device. To install it, see [Installing aws-iam-authenticator \(p. 436\)](#).

```
#!/bin/bash
read -r -d '' KUBECONFIG <<EOF
apiVersion: v1
clusters:
- cluster:
    server: $cluster_endpoint
    certificate-authority-data: $certificate_data
  name: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
contexts:
- context:
    cluster: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
    user: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
  name: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
current-context: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
kind: Config
preferences: {}
```

```

users:
- name: arn:aws:eks:$region_code:$account_id:cluster/$cluster_name
user:
  exec:
    apiVersion: client.authentication.k8s.io/v1beta1
    command: aws-iam-authenticator
    args:
      - "token"
      - "-i"
      - "$cluster_name"
      # - "--role"
      # - "arn:aws:iam::$account_id:role/my-role"
  # env:
  # - name: AWS_PROFILE
  #   value: aws-profile
EOF
echo "${KUBECONFIG}" > ~/.kube/config

```

6. Add the file path to your KUBECONFIG environment variable so that kubectl knows where to look for your cluster configuration.

- For Bash shells on macOS or Linux:

```
export KUBECONFIG=$KUBECONFIG:~/kube/config
```

- For PowerShell on Windows:

```
$ENV:KUBECONFIG="{0};{1}" -f $ENV:KUBECONFIG, "$ENV:UserProfile\.kube\config"
```

7. (Optional) Add the configuration to your shell initialization file so that it is configured when you open a shell.

- For Bash shells on macOS:

```
echo 'export KUBECONFIG=$KUBECONFIG:~/kube/config' >> ~/.bash_profile
```

- For Bash shells on Linux:

```
echo 'export KUBECONFIG=$KUBECONFIG:~/kube/config' >> ~/.bashrc
```

- For PowerShell on Windows:

```
[System.Environment]::SetEnvironmentVariable('KUBECONFIG', $ENV:KUBECONFIG, 'Machine')
```

8. Test your configuration.

```
kubectl get svc
```

An example output is as follows.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
svc/kubernetes	ClusterIP	10.100.0.1	<none>	443/TCP	1m

If you receive any authorization or resource type errors, see [Unauthorized or access denied \(kubectl\) \(p. 563\)](#) in the troubleshooting topic.

Installing aws-iam-authenticator

Amazon EKS uses IAM to provide authentication to your Kubernetes cluster through the [AWS IAM authenticator for Kubernetes](#). You can configure the stock `kubectl` client to work with Amazon EKS by installing the AWS IAM authenticator for Kubernetes and [modifying your `kubectl` configuration file \(p. 431\)](#) to use it for authentication.

Note

If you're running the AWS CLI version 1.16.156 or later, then you don't need to install the authenticator. Instead, you can use the [aws_eks_get-token](#) command. For more information, see [Create kubeconfig file manually \(p. 433\)](#).

If you're unable to use the AWS CLI version 1.16.156 or later to create the `kubeconfig` file, then you can install the AWS IAM authenticator for Kubernetes on macOS, Linux, or Windows.

macOS

To install aws-iam-authenticator with Homebrew

The easiest way to install the `aws-iam-authenticator` is with [Homebrew](#).

1. If you do not already have [Homebrew](#) installed on your Mac, install it with the following command.

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install.sh)"
```

2. Install the `aws-iam-authenticator` with the following command.

```
brew install aws-iam-authenticator
```

3. Test that the `aws-iam-authenticator` binary works.

```
aws-iam-authenticator help
```

To install aws-iam-authenticator on macOS

You can also install the `aws-iam-authenticator` by following these steps.

1. Download the `aws-iam-authenticator` binary from GitHub for your hardware platform. The first command downloads the `amd64` release. The second command downloads the `arm64` release.

```
curl -Lo aws-iam-authenticator https://github.com/kubernetes-sigs/aws-iam-authenticator/releases/download/v0.5.9/aws-iam-authenticator_0.5.9_darwin_amd64
```

```
curl -Lo aws-iam-authenticator https://github.com/kubernetes-sigs/aws-iam-authenticator/releases/download/v0.5.9/aws-iam-authenticator_0.5.9_darwin_arm64
```

2. (Optional) Verify the downloaded binary with the SHA-256 checksum for the file.

- a. Download the SHA-256 checksum file.

```
curl -Lo aws-iam-authenticator.txt https://github.com/kubernetes-sigs/aws-iam-authenticator/releases/download/v0.5.9/authenticator_0.5.9_checksums.txt
```

- b. View the checksum for the authenticator binary that you downloaded. The first command returns the amd64 checksum. The second command returns the arm64 checksum.

```
awk '/aws-iam-authenticator_0.5.9_darwin_amd64/ {print $1}' aws-iam-authenticator.txt
```

```
awk '/aws-iam-authenticator_0.5.9_darwin_arm64/ {print $1}' aws-iam-authenticator.txt
```

An example output is as follows.

```
7656bd290a7e9cb588df1d9cc43fab7f2447b88ed4f41d3f5092fd114b0939
```

- c. Determine the SHA-256 checksum for your downloaded binary.

```
openssl sha1 -sha256 aws-iam-authenticator
```

An example output is as follows.

```
SHA256(aws-iam-authenticator)= 7656bd290a7e9cb588df1d9cc43fab7f2447b88ed4f41d3f5092fd114b0939
```

The returned output should match the output returned in the previous step.

3. Apply execute permissions to the binary.

```
chmod +x ./aws-iam-authenticator
```

4. Copy the binary to a folder in your \$PATH. We recommend creating a \$HOME/bin/aws-iam-authenticator and ensuring that \$HOME/bin comes first in your \$PATH.

```
mkdir -p $HOME/bin && cp ./aws-iam-authenticator $HOME/bin/aws-iam-authenticator && export PATH=$HOME/bin:$PATH
```

5. Add \$HOME/bin to your PATH environment variable.

```
echo 'export PATH=$HOME/bin:$PATH' >> ~/.bash_profile
```

6. Test that the aws-iam-authenticator binary works.

```
aws-iam-authenticator help
```

Linux

To install aws-iam-authenticator on Linux

1. Download the aws-iam-authenticator binary from GitHub for your hardware platform. The first command downloads the amd64 release. The second command downloads the arm64 release.

```
curl -Lo aws-iam-authenticator https://github.com/kubernetes-sigs/aws-iam-authenticator/releases/download/v0.5.9/aws-iam-authenticator_0.5.9_linux_amd64
```

```
curl -Lo aws-iam-authenticator https://github.com/kubernetes-sigs/aws-iam-authenticator/releases/download/v0.5.9/aws-iam-authenticator_0.5.9_linux_arm64
```

2. (Optional) Verify the downloaded binary with the SHA-256 checksum for the file.

- a. Download the SHA-256 checksum file.

```
curl -Lo aws-iam-authenticator.txt https://github.com/kubernetes-sigs/aws-iam-authenticator/releases/download/v0.5.9/authenticator_0.5.9_checksums.txt
```

- b. View the checksum for the authenticator binary that you downloaded. The first command returns the amd64 checksum. The second command returns the arm64 checksum.

```
awk '/aws-iam-authenticator_0.5.9_linux_amd64/ {print $1}' aws-iam-authenticator.txt
```

```
awk '/aws-iam-authenticator_0.5.9_linux_arm64/ {print $1}' aws-iam-authenticator.txt
```

An example output is as follows.

```
b192431c22d720c38adbf53b016c33ab17105944ee73b25f485aa52c9e9297a7
```

- c. Determine the SHA-256 checksum for your downloaded binary.

```
openssl sha1 -sha256 aws-iam-authenticator
```

An example output is as follows.

```
SHA256(aws-iam-authenticator)= b192431c22d720c38adbf53b016c33ab17105944ee73b25f485aa52c9e9297a7
```

The returned output should match the output returned in the previous step.

3. Apply execute permissions to the binary.

```
chmod +x ./aws-iam-authenticator
```

4. Copy the binary to a folder in your \$PATH. We recommend creating a \$HOME/bin/aws-iam-authenticator and ensuring that \$HOME/bin comes first in your \$PATH.

```
mkdir -p $HOME/bin && cp ./aws-iam-authenticator $HOME/bin/aws-iam-authenticator && export PATH=$HOME/bin:$PATH
```

5. Add \$HOME/bin to your PATH environment variable.

```
echo 'export PATH=$HOME/bin:$PATH' >> ~/.bashrc
```

6. Test that the aws-iam-authenticator binary works.

```
aws-iam-authenticator help
```

Windows

To install aws-iam-authenticator on Windows with Chocolatey

1. If you do not already have Chocolatey installed on your Windows system, see [Installing chocolatey](#).
2. Open a PowerShell terminal window and install the aws-iam-authenticator package with the following command:

```
choco install -y aws-iam-authenticator
```

3. Test that the aws-iam-authenticator binary works.

```
aws-iam-authenticator help
```

To install aws-iam-authenticator on Windows

1. Open a PowerShell terminal window and download the aws-iam-authenticator binary from GitHub.

```
curl -Lo aws-iam-authenticator.exe https://github.com/kubernetes-sigs/aws-iam-authenticator/releases/download/v0.5.9/aws-iam-authenticator_0.5.9_windows_amd64.exe
```

2. (Optional) Verify the downloaded binary with the SHA-256 checksum for the file.
 - a. Download the SHA-256 checksum file.

```
curl -Lo aws-iam-authenticator.txt https://github.com/kubernetes-sigs/aws-iam-authenticator/releases/download/v0.5.9/authenticator_0.5.9_checksums.txt
```

- b. View the checksum for the authenticator binary that you downloaded.

```
$checksum = Get-Content aws-iam-authenticator.txt  
$checksum[3]
```

An example output is as follows.

```
b7345e06c5f1d31b9459a38bafffe0744343711cb5042cb31ff1e072d870c42f9 aws-iam-authenticator_0.5.9_windows_amd64.exe
```

- c. Determine the SHA-256 checksum for your downloaded binary.

```
Get-Filehash aws-iam-authenticator.exe
```

An example output is as follows.

Algorithm	Hash	
Path	-----	
-----	----	
SHA256	B7345E06C5F1D31B9459A38BAFFE0744343711CB5042CB31FF1E072D870C42F9	/home/cloudshell-user/temp/aws-iam-authenticator

Though the returned output is uppercase, it should match the lowercase output returned in the previous step.

3. Copy the binary to a folder in your PATH. If you have an existing directory in your PATH that you use for command line utilities, copy the binary to that directory. Otherwise, complete the following steps.
 - a. Create a new directory for your command line binaries, such as C:\bin.
 - b. Copy the aws-iam-authenticator.exe binary to your new directory.
 - c. Edit your user or system PATH environment variable to add the new directory to your PATH.
 - d. Close your PowerShell terminal and open a new one to pick up the new PATH variable.
4. Test that the aws-iam-authenticator binary works.

```
aws-iam-authenticator help
```

If you have an existing Amazon EKS cluster, create a kubeconfig file for that cluster. For more information, see [Creating or updating a kubeconfig file for an Amazon EKS cluster \(p. 431\)](#). Otherwise, see [Creating an Amazon EKS cluster \(p. 25\)](#) to create a new Amazon EKS cluster.

Default Amazon EKS created Kubernetes roles and users

When you create a Kubernetes cluster, several default Kubernetes identities are created on that cluster for the proper functioning of Kubernetes. Amazon EKS creates Kubernetes identities for each of its default components. The identities provide Kubernetes role-based authorization control (RBAC) for the cluster components. For more information, see [Using RBAC Authorization](#) in the Kubernetes documentation.

When you install optional [add-ons \(p. 385\)](#) to your cluster, additional Kubernetes identities might be added to your cluster. For more information about identities not addressed by this topic, see the documentation for the add-on.

You can view the list of Amazon EKS created Kubernetes identities on your cluster using the AWS Management Console or kubectl command line tool. All of the user identities appear in the kube audit logs available to you through Amazon CloudWatch.

AWS Management Console

Prerequisite

The [IAM principal](#) that you use must have the permissions described in [the section called “Required permissions” \(p. 529\)](#).

To view Amazon EKS created identities using the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the **Clusters** list, choose the cluster that contains the identities that you want to view.
3. Choose the **Resources** tab.
4. Under **Resource types**, choose **Authorization**.
5. Choose, **ClusterRoles**, **ClusterRoleBindings**, **Roles**, or **RoleBindings**. All resources prefaced with **eks** are created by Amazon EKS. Additional Amazon EKS created identity resources are:

- The **ClusterRole** and **ClusterRoleBinding** named **aws-node**. The **aws-node** resources support the [Amazon VPC CNI plugin for Kubernetes \(p. 266\)](#), which Amazon EKS installs on all clusters.
- A **ClusterRole** named **vpc-resource-controller-role** and a **ClusterRoleBinding** named **vpc-resource-controller-rolebinding**. These resources support the [Amazon VPC resource controller](#), which Amazon EKS installs on all clusters.

In addition to the resources that you see in the console, the following special user identities exist on your cluster, though they're not visible in the cluster's configuration:

- **eks:cluster-bootstrap** – Used for `kubectl` operations during cluster bootstrap.
 - **eks:support-engineer** – Used for cluster management operations.
6. Choose a specific resource to view details about it. By default, you're shown information in **Structured view**. In the top-right corner of the details page you can choose **Raw view** to see all information for the resource.

Kubectl

Prerequisite

The entity that you use (AWS Identity and Access Management (IAM) or OpenID Connect (OIDC)) to list the Kubernetes resources on the cluster must be authenticated by IAM or your OIDC identity provider. The entity must be granted permissions to use the Kubernetes get and list verbs for the Role, ClusterRole, RoleBinding, and ClusterRoleBinding resources on your cluster that you want the entity to work with. For more information about granting IAM entities access to your cluster, see [the section called "Enabling IAM principal access" \(p. 420\)](#). For more information about granting entities authenticated by your own OIDC provider access to your cluster, see [the section called "OIDC identity provider authentication" \(p. 427\)](#).

To view Amazon EKS created identities using `kubectl`

Run the command for the type of resource that you want to see. All returned resources that are prefaced with **eks** are created by Amazon EKS. In addition to the resources returned in the output from the commands, the following special user identities exist on your cluster, though they're not visible in the cluster's configuration:

- **eks:cluster-bootstrap** – Used for `kubectl` operations during cluster bootstrap.
- **eks:support-engineer** – Used for cluster management operations.

ClusterRoles – ClusterRoles are scoped to your cluster, so any permission granted to a role applies to resources in any Kubernetes namespace on the cluster.

The following command returns all of the Amazon EKS created Kubernetes ClusterRoles on your cluster.

```
kubectl get clusterroles | grep eks
```

In addition to the ClusterRoles returned in the output that are prefaced with, the following ClusterRoles exist.

- **aws-node** – This ClusterRole supports the [Amazon VPC CNI plugin for Kubernetes \(p. 266\)](#), which Amazon EKS installs on all clusters.
- **vpc-resource-controller-role** – This ClusterRole supports the [Amazon VPC resource controller](#), which Amazon EKS installs on all clusters.

To see the specification for a ClusterRole, replace `eks:k8s-metrics` in the following command with a ClusterRole returned in the output of the previous command. The following example returns the specification for the `eks:k8s-metrics` ClusterRole.

```
kubectl describe clusterrole eks:k8s-metrics
```

An example output is as follows.

Name:	eks:k8s-metrics		
Labels:	<none>		
Annotations:	<none>		
PolicyRule:			
Resources	Non-Resource URLs	Resource Names	Verbs
-----	-----	-----	-----
endpoints	[/metrics]	[]	[get]
nodes	[]	[]	[list]
pods	[]	[]	[list]
deployments.apps	[]	[]	[list]

ClusterRoleBindings – ClusterRoleBindings are scoped to your cluster.

The following command returns all of the Amazon EKS created Kubernetes ClusterRoleBindings on your cluster.

```
kubectl get clusterrolebindings | grep eks
```

In addition to the ClusterRoleBindings returned in the output, the following ClusterRoleBindings exist.

- **aws-node** – This ClusterRoleBinding supports the [Amazon VPC CNI plugin for Kubernetes \(p. 266\)](#), which Amazon EKS installs on all clusters.
- **vpc-resource-controller-rolebinding** – This ClusterRoleBinding supports the [Amazon VPC resource controller](#), which Amazon EKS installs on all clusters.

To see the specification for a ClusterRoleBinding, replace `eks:k8s-metrics` in the following command with a ClusterRoleBinding returned in the output of the previous command. The following example returns the specification for the `eks:k8s-metrics` ClusterRoleBinding.

```
kubectl describe clusterrolebinding eks:k8s-metrics
```

An example output is as follows.

Name:	eks:k8s-metrics	
Labels:	<none>	
Annotations:	<none>	
Role:		
Kind:	ClusterRole	
Name:	eks:k8s-metrics	
Subjects:		
Kind	Name	Namespace
----	----	-----
User	eks:k8s-metrics	

Roles – Roles are scoped to a Kubernetes namespace. All Amazon EKS created Roles are scoped to the `kube-system` namespace.

The following command returns all of the Amazon EKS created Kubernetes Roles on your cluster.

```
kubectl get roles -n kube-system | grep eks
```

To see the specification for a Role, replace `eks:k8s-metrics` in the following command with the name of a Role returned in the output of the previous command. The following example returns the specification for the `eks:k8s-metrics` Role.

```
kubectl describe role eks:k8s-metrics -n kube-system
```

An example output is as follows.

```
Name:      eks:k8s-metrics
Labels:    <none>
Annotations: <none>
PolicyRule:
  Resources      Non-Resource URLs  Resource Names      Verbs
  -----          -----           -----           -----
  daemonsets.apps  []                [aws-node]        [get]
  deployments.apps  []              [vpc-resource-controller]  [get]
```

RoleBindings – RoleBindings are scoped to a Kubernetes namespace. All Amazon EKS created RoleBindings are scoped to the `kube-system` namespace.

The following command returns all of the Amazon EKS created Kubernetes RoleBindings on your cluster.

```
kubectl get rolebindings -n kube-system | grep eks
```

To see the specification for a RoleBinding, replace `eks:k8s-metrics` in the following command with a RoleBinding returned in the output of the previous command. The following example returns the specification for the `eks:k8s-metrics` RoleBinding.

```
kubectl describe rolebinding eks:k8s-metrics -n kube-system
```

An example output is as follows.

```
Name:      eks:k8s-metrics
Labels:    <none>
Annotations: <none>
Role:
  Kind:  Role
  Name:  eks:k8s-metrics
Subjects:
  Kind  Name          Namespace
  ----  ---           -----
  User  eks:k8s-metrics
```

Cluster management

This chapter includes the following topics to help you manage your cluster. You can also view information about your [Kubernetes resources \(p. 529\)](#) with the AWS Management Console.

- The Kubernetes Dashboard is a general purpose, web-based UI for Kubernetes clusters. It allows users to manage applications running in the cluster and troubleshoot them, as well as manage the cluster itself. For more information, see The [Kubernetes Dashboard](#) GitHub repository.
- [Installing the Kubernetes Metrics Server \(p. 450\)](#) – The Kubernetes Metrics Server is an aggregator of resource usage data in your cluster. It isn't deployed by default in your cluster, but is used by Kubernetes add-ons, such as the Kubernetes Dashboard and [Horizontal Pod Autoscaler \(p. 367\)](#). In this topic you learn how to install the Metrics Server.
- [Using Helm with Amazon EKS \(p. 450\)](#) – The Helm package manager for Kubernetes helps you install and manage applications on your Kubernetes cluster. This topic helps you install and run the Helm binaries so that you can install and manage charts using the Helm CLI on your local computer.
- [Tagging your Amazon EKS resources \(p. 451\)](#) – To help you manage your Amazon EKS resources, you can assign your own metadata to each resource in the form of *tags*. This topic describes tags and shows you how to create them.
- [Amazon EKS service quotas \(p. 455\)](#) – Your AWS account has default quotas, formerly referred to as limits, for each AWS service. Learn about the quotas for Amazon EKS and how to increase them.

Cost monitoring

Amazon EKS supports Kubecost, which you can use to monitor your costs broken down by Kubernetes resources including Pods, nodes, namespaces, and labels. As a Kubernetes platform administrator and finance leader, you can use Kubecost to visualize a breakdown of Amazon EKS charges, allocate costs, and charge back organizational units such as application teams. You can provide your internal teams and business units with transparent and accurate cost data based on their actual AWS bill. Moreover, you can also get customized recommendations for cost optimization based on their infrastructure environment and usage patterns within their clusters. For more information about Kubecost, see the [Kubecost](#) documentation.

Amazon EKS provides an AWS optimized bundle of Kubecost for cluster cost visibility. You can use your existing AWS support agreements to obtain support.

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Getting started with Amazon EKS \(p. 6\)](#). The cluster must have Amazon EC2 nodes because you can't run Kubecost on Fargate nodes.
- The `kubectl` command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use `kubectl` version 1.26, 1.27, or 1.28 with it. To install or upgrade `kubectl`, see [Installing or updating kubectl \(p. 6\)](#).
- Helm version 3.9.0 or later configured on your device or AWS CloudShell. To install or update Helm, see [the section called "Using Helm" \(p. 450\)](#).
- If your cluster is version 1.23 or later, you must have the [the section called "Amazon EBS CSI driver" \(p. 228\)](#) installed on your cluster.

To install Kubecost

1. Install Kubecost with the following command. You can replace **1.96.0** with a later version. You can see the available versions at [kubecost/cost-analyzer](#) in the Amazon ECR Public Gallery.

```
helm upgrade -i kubecost oci://public.ecr.aws/kubecost/cost-analyzer --version 1.96.0 \
--namespace kubecost --create-namespace \
-f https://raw.githubusercontent.com/kubecost/cost-analyzer-helm-chart/develop/
cost-analyzer/values-eks-cost-monitoring.yaml
```

Kubecost releases new versions regularly. You can update your version using [helm upgrade](#). By default, the installation includes a local [Prometheus](#) server and [kube-state-metrics](#). You can customize your deployment to use [Amazon Managed Service for Prometheus](#) by following the documentation in [Integrating with Amazon EKS cost monitoring](#). For a list of all other settings that you can configure, see the [sample configuration file](#) on GitHub.

2. Make sure the required Pods are running.

```
kubectl get pods -n kubecost
```

An example output is as follows.

NAME	READY	STATUS	RESTARTS	AGE
kubecost-cost-analyzer- b9788c99f-5vj5b	2/2	Running	0	3h27m
kubecost-kube-state-metrics- 99bb8c55b-bn2br	1/1	Running	0	3h27m
kubecost-prometheus-server- 7d9967bfc8-9c8p7	2/2	Running	0	3h27m

3. On your device, enable port-forwarding to expose the Kubecost dashboard.

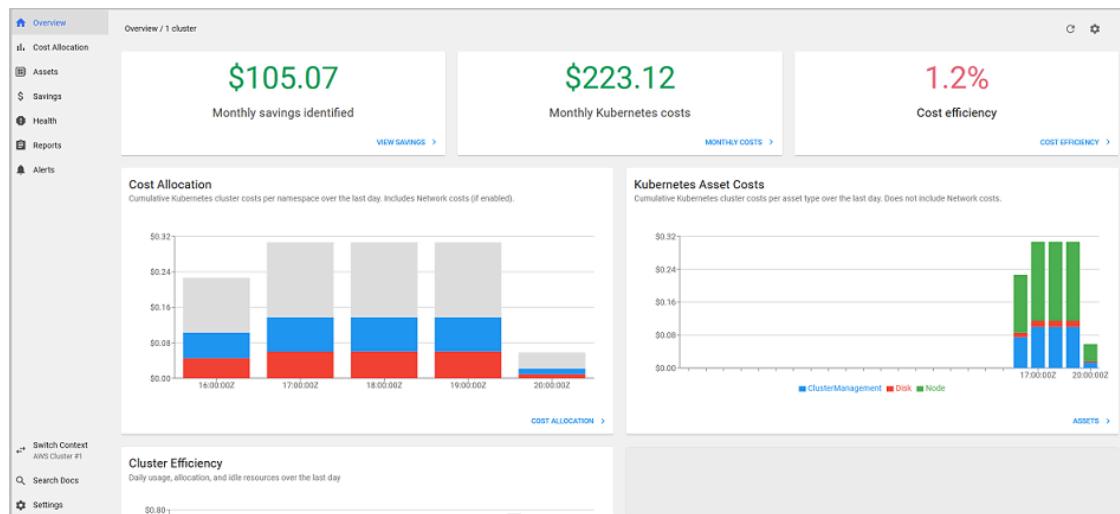
```
kubectl port-forward --namespace kubecost deployment/kubecost-cost-analyzer 9090
```

Alternatively, you can use the [AWS Load Balancer Controller \(p. 333\)](#) to expose Kubecost and use Amazon Cognito for authentication, authorization, and user management. For more information, see [How to use Application Load Balancer and Amazon Cognito to authenticate users for your Kubernetes web apps](#).

4. On the same device that you completed the previous step on, open a web browser and enter the following address.

```
http://localhost:9090
```

You see the Kubecost Overview page in your browser. It might take 5–10 minutes for Kubecost to gather metrics. You can see your Amazon EKS spend, including cumulative cluster costs, associated Kubernetes asset costs, and monthly aggregated spend.



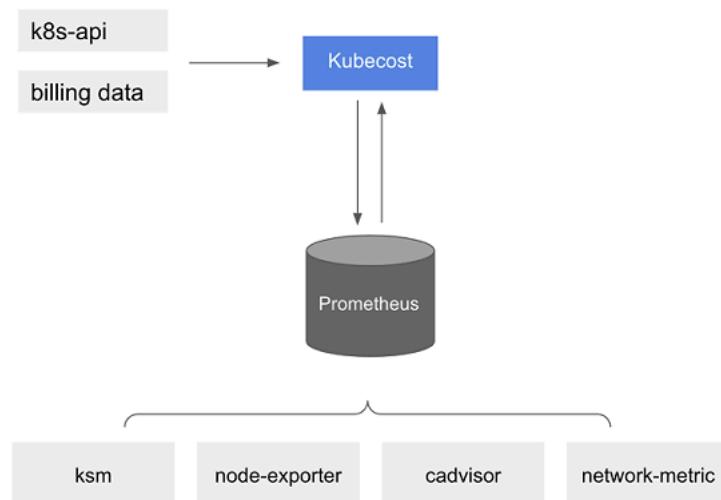
- To track costs at a cluster level, tag your Amazon EKS resources for billing. For more information, see [the section called "Tagging your resources for billing" \(p. 453\)](#).

You can also view the following information by selecting it in the left pane of the dashboard:

- Cost allocation** – View monthly Amazon EKS costs and cumulative costs for each of your namespaces and other dimensions over the past seven days. This is helpful for understanding which parts of your application are contributing to Amazon EKS spend.
- Assets** – View the costs of the AWS infrastructure assets that are associated with your Amazon EKS resources.

Additional features

- Export cost metrics** – Amazon EKS optimized cost monitoring is deployed with Kubecost and Prometheus, which is an open-source monitoring system and time series database. Kubecost reads metric from Prometheus and then performs cost allocation calculations and writes the metrics back to Prometheus. The Kubecost front-end reads metrics from Prometheus and shows them on the Kubecost user interface. The architecture is illustrated in the following diagram.



With [Prometheus](#) pre-installed, you can write queries to ingest Kubecost data into your current business intelligence system for further analysis. You can also use it as a data source for your current [Grafana](#) dashboard to display Amazon EKS cluster costs that your internal teams are familiar with. To learn more about how to write Prometheus queries, see the [Prometheus Configuration](#) readme file on GitHub or use the example Grafana JSON models in the [Kubecost Github repository](#) as references.

- **AWS Cost and Usage Report integration** – To perform cost allocation calculations for your Amazon EKS cluster, Kubecost retrieves the public pricing information of AWS services and AWS resources from the AWS Price List API. You can also integrate Kubecost with [AWS Cost and Usage Report](#) to enhance the accuracy of the pricing information specific to your AWS account. This information includes enterprise discount programs, reserved instance usage, savings plans, and spot usage. To learn more about how the AWS Cost and Usage Report integration works, see [AWS Cloud Integration](#) in the Kubecost documentation.

Remove Kubecost

You can remove Kubecost from your cluster with the following commands.

```
helm uninstall kubecost --namespace kubecost
kubectl delete ns kubecost
```

Frequently asked questions

See the following common questions and answers about using Kubecost with Amazon EKS.

What is the difference between the custom bundle of Kubecost and the free version of Kubecost (also known as OpenCost)?

AWS and Kubecost collaborated to offer a customized version of Kubecost. This version includes a subset of commercial features at no additional charge. See the following table for features that are included with in the custom bundle of Kubecost.

Feature	Kubecost free tier	Amazon EKS optimized Kubecost custom bundle	Kubecost Enterprise
Deployment	User hosted	User hosted	User hosted or Kubecost hosted (SaaS)
Number of clusters supported	Unlimited	Unlimited	Unlimited
Databases supported	Local Prometheus	Local Prometheus or Amazon Managed Service for Prometheus	Prometheus, Amazon Managed Service for Prometheus, Cortex, or Thanos
Database retention support	15 days	Unlimited historical data	Unlimited historical data
Kubecost API retention (ETL)	15 days	15 days	Unlimited historical data
Cluster cost visibility	Single clusters	Unified multi-cluster	Unified multi-cluster

Feature	Kubecost free tier	Amazon EKS optimized Kubecost custom bundle	Kubecost Enterprise
Hybrid cloud visibility	-	Amazon EKS and Amazon EKS Anywhere clusters	Multi-cloud and hybrid-cloud support
Alerts and recurring reports	-	Efficiency alerts, budget alerts, spend change alerts, and more supported	Efficiency alerts, budget alerts, spend change alerts, and more supported
Saved reports	-	Reports using 15 days data	Reports using unlimited historical data
Cloud billing integration	Required for each individual cluster	Custom pricing support for AWS (including multiple clusters and multiple accounts)	Custom pricing support for AWS (including multiple clusters and multiple accounts)
Savings recommendations	Single cluster insights	Single cluster insights	Multi-cluster insights
Governance: Audits	-	-	Audit historical cost events
Single sign-on (SSO) support	-	Amazon Cognito supported	Okta, Auth0, PingID, Keycloak
Role-based access control (RBAC) with SAML 2.0	-	-	Okta, Auth0, PingID, Keycloak
Enterprise training and onboarding	-	-	Full-service training and FinOps onboarding

What is the Kubecost API retention (ETL) feature?

The Kubecost ETL feature aggregates and organizes metrics to surface cost visibility at various levels of granularity (such as namespace-level, pod-level, and deployment-level). For the custom Kubecost bundle, customers get data and insights from metrics for the last 15 days.

What is the alerts and recurring reports feature? What alerts and reports does it include?

Kubecost alerts allow teams to receive updates on real-time Kubernetes spend as well as cloud spend. Recurring reports enable teams to receive customized views of historical Kubernetes and cloud spend. Both are configurable using the Kubecost UI or Helm values. They support email, Slack, and Microsoft Teams.

What do saved reports include?

Kubecost saved reports are predefined views of cost and efficiency metrics. They include cost by cluster, namespace, label, and more.

What is cloud billing integration?

Integration with AWS billing APIs allows Kubecost to display out-of-cluster costs (such as Amazon S3). Additionally, it allows Kubecost to reconcile Kubecost's in-cluster predictions with actual billing data to account for spot usage, savings plans, and enterprise discounts.

What do savings recommendations include?

Kubecost provides insights and automation to help users optimize their Kubernetes infrastructure and spend.

Is there a charge for this functionality?

No. You can use this version of Kubecost at no additional charge. If you want additional Kubecost capabilities that aren't included in this bundle, you can buy an enterprise license of Kubecost through the AWS Marketplace, or from Kubecost directly.

Is support available?

Yes. You can open a support case with the AWS Support team at [Contact AWS](#).

Do I need a license to use Kubecost features provided by the Amazon EKS integration?

No.

Can I integrate Kubecost with AWS Cost and Usage Report for more accurate reporting?

Yes. You can configure Kubecost to ingest data from AWS Cost and Usage Report to get accurate cost visibility, including discounts, Spot pricing, reserved instance pricing, and others. For more information, see [AWS Cloud Integration](#) in the Kubecost documentation.

Does this version support cost management of self-managed Kubernetes clusters on Amazon EC2?

No. This version is only compatible with Amazon EKS clusters.

Can Kubecost track costs for Amazon EKS on AWS Fargate?

Kubecost provides best effort to show cluster cost visibility for Amazon EKS on Fargate, but with lower accuracy than with Amazon EKS on Amazon EC2. This is primarily due to the difference in how you're billed for your usage. With Amazon EKS on Fargate, you're billed for consumed resources. With Amazon EKS on Amazon EC2 nodes, you're billed for provisioned resources. Kubecost calculates the cost of an Amazon EC2 node based on the node specification, which includes CPU, RAM, and ephemeral storage. With Fargate, costs are calculated based on the requested resources for the Fargate Pods.

How can I get updates and new versions of Kubecost?

You can upgrade your Kubecost version using standard Helm upgrade procedures. The latest versions are in the [Amazon ECR Public Gallery](#).

Is the kubectl-cost CLI supported? How do I install it?

Yes. Kubectl-cost is an open source tool by Kubecost (Apache 2.0 License) that provides CLI access to Kubernetes cost allocation metrics. To install kubectl-cost, see [Installation](#) on GitHub.

Is the Kubecost user interface supported? How do I access it?

Kubecost provides a web dashboard that you can access through kubectl port forwarding, an ingress, or a load balancer. You can also use the AWS Load Balancer Controller to expose Kubecost and use Amazon Cognito for authentication, authorization, and user management. For more information, see [How to use Application Load Balancer and Amazon Cognito to authenticate users for your Kubernetes web apps](#) on the AWS blog.

Is Amazon EKS Anywhere supported?

No.

Installing the Kubernetes Metrics Server

The Kubernetes Metrics Server is an aggregator of resource usage data in your cluster, and it isn't deployed by default in Amazon EKS clusters. For more information, see [Kubernetes Metrics Server](#) on GitHub. The Metrics Server is commonly used by other Kubernetes add ons, such as the [Horizontal Pod Autoscaler \(p. 367\)](#) or the [Kubernetes Dashboard \(p. 444\)](#). For more information, see [Resource metrics pipeline](#) in the Kubernetes documentation. This topic explains how to deploy the Kubernetes Metrics Server on your Amazon EKS cluster.

Important

The metrics are meant for point-in-time analysis and aren't an accurate source for historical analysis. They can't be used as a monitoring solution or for other non-auto scaling purposes. For information about monitoring tools, see [Observability in Amazon EKS \(p. 534\)](#).

Deploy the Metrics Server

1. Deploy the Metrics Server with the following command:

```
kubectl apply -f https://github.com/kubernetes-sigs/metrics-server/releases/latest/download/components.yaml
```

2. Verify that the `metrics-server` deployment is running the desired number of Pods with the following command.

```
kubectl get deployment metrics-server -n kube-system
```

An example output is as follows.

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
metrics-server	1/1	1	1	6m

Using Helm with Amazon EKS

The Helm package manager for Kubernetes helps you install and manage applications on your Kubernetes cluster. For more information, see the [Helm documentation](#). This topic helps you install and run the Helm binaries so that you can install and manage charts using the Helm CLI on your local system.

Important

Before you can install Helm charts on your Amazon EKS cluster, you must configure `kubectl` to work for Amazon EKS. If you have not already done this, see [Creating or updating a kubeconfig file for an Amazon EKS cluster \(p. 431\)](#) before proceeding. If the following command succeeds for your cluster, you're properly configured.

```
kubectl get svc
```

To install the Helm binaries on your local system

1. Run the appropriate command for your client operating system.

- If you're using macOS with [Homebrew](#), install the binaries with the following command.

```
brew install helm
```

- If you're using Windows with [Chocolatey](#), install the binaries with the following command.

```
choco install kubernetes-helm
```

- If you're using Linux, install the binaries with the following commands.

```
curl https://raw.githubusercontent.com/helm/helm/master/scripts/get-helm-3 >
get_helm.sh
chmod 700 get_helm.sh
./get_helm.sh
```

Note

If you get a message that openssl must first be installed, you can install it with the following command.

```
sudo yum install openssl
```

2. To pick up the new binary in your PATH, Close your current terminal window and open a new one.
3. See the version of Helm that you installed.

```
helm version --short | cut -d + -f 1
```

An example output is as follows.

```
v3.9.0
```

4. At this point, you can run any Helm commands (such as `helm install chart-name`) to install, modify, delete, or query Helm charts in your cluster. If you're new to Helm and don't have a specific chart to install, you can:
 - Experiment by installing an example chart. See [Install an example chart](#) in the Helm [Quickstart guide](#).
 - Create an example chart and push it to Amazon ECR. For more information, see [Pushing a Helm chart](#) in the [Amazon Elastic Container Registry User Guide](#).
 - Install an Amazon EKS chart from the [eks-charts](#) GitHub repo or from [ArtifactHub](#).

Tagging your Amazon EKS resources

You can use *tags* to help you manage your Amazon EKS resources. This topic provides an overview of the `tags` function and shows how you can create tags.

Topics

- [Tag basics \(p. 452\)](#)
- [Tagging your resources \(p. 452\)](#)
- [Tag restrictions \(p. 453\)](#)
- [Tagging your resources for billing \(p. 453\)](#)
- [Working with tags using the console \(p. 454\)](#)

- [Working with tags using the CLI, API, or eksctl \(p. 454\)](#)

Note

Tags are a type of metadata that's separate from Kubernetes labels and annotations. For more information about these other metadata types, see the following sections in the Kubernetes documentation:

- [Labels and Selectors](#)
- [Annotations](#)

Tag basics

A tag is a label that you assign to an AWS resource. Each tag consists of a *key* and an optional *value*.

With tags, you can categorize your AWS resources. For example, you can categorize resources by purpose, owner, or environment. When you have many resources of the same type, you can use the tags that you assigned to a specific resource to quickly identify that resource. For example, you can define a set of tags for your Amazon EKS clusters to help you track each cluster's owner and stack level. We recommend that you devise a consistent set of tag keys for each resource type. You can then search and filter the resources based on the tags that you add.

After you add a tag, you can edit tag keys and values or remove tags from a resource at any time. If you delete a resource, any tags for the resource are also deleted.

Tags don't have any semantic meaning to Amazon EKS and are interpreted strictly as a string of characters. You can set the value of a tag to an empty string. However, you can't set the value of a tag to null. If you add a tag that has the same key as an existing tag on that resource, the new value overwrites the earlier value.

If you use AWS Identity and Access Management (IAM), you can control which users in your AWS account have permission to manage tags.

Tagging your resources

The following Amazon EKS resources support tags:

- clusters
- managed node groups
- Fargate profiles

You can tag these resources using the following:

- If you're using the Amazon EKS console, you can apply tags to new or existing resources at any time. You can do this by using the **Tags** tab on the relevant resource page. For more information, see [Working with tags using the console \(p. 454\)](#).
- If you're using eksctl, you can apply tags to resources when they're created using the `--tags` option.
- If you're using the AWS CLI, the Amazon EKS API, or an AWS SDK, you can apply tags to new resources using the `tags` parameter on the relevant API action. You can apply tags to existing resources using the `TagResource` API action. For more information, see [TagResource](#).

When you use some resource-creating actions, you can also specify tags for the resource at the same time that you create it. If tags can't be applied while the resource is being created, the resource fails to

be created. This mechanism ensures that resources that you intend to tag are either created with the tags that you specify or not created at all. If you tag resources when you create them, you don't need to run custom tagging scripts after you create the resource.

Tags don't propagate to other resources that are associated with the resource that you create. For example, Fargate profile tags don't propagate to other resources that are associated with the Fargate profile, such as the Pods that are scheduled with it.

Tag restrictions

The following restrictions apply to tags:

- A maximum of 50 tags can be associated with a resource.
- Tag keys can't be repeated for one resource. Each tag key must be unique, and can only have one value.
- Keys can be up to 128 characters long in UTF-8.
- Values can be up to 256 characters long in UTF-8.
- If multiple AWS services and resources use your tagging schema, limit the types of characters you use. Some services might have restrictions on allowed characters. Generally, allowed characters are letters, numbers, spaces, and the following characters: + - = . _ : / @.
- Tag keys and values are case sensitive.
- Don't use aws :, AWS :, or any upper or lowercase combination of such as a prefix for either keys or values. These are reserved only for AWS use. You can't edit or delete tag keys or values with this prefix. Tags with this prefix don't count against your tags-per-resource limit.

Tagging your resources for billing

When you apply tags to Amazon EKS clusters, you can use them for cost allocation in your **Cost & Usage Reports**. The metering data in your **Cost & Usage Reports** shows usage across all of your Amazon EKS clusters. For more information, see [AWS cost and usage report](#) in the *AWS Billing User Guide*.

The AWS generated cost allocation tag, specifically `aws:eks:cluster-name`, lets you break down Amazon EC2 instance costs by individual Amazon EKS cluster in **Cost Explorer**. However, this tag doesn't capture the control plane expenses. The tag is automatically added to Amazon EC2 instances that participate in an Amazon EKS cluster. This behavior happens regardless of whether the instances are provisioned using Amazon EKS managed node groups, Karpenter, or directly with Amazon EC2. This specific tag doesn't count towards the 50 tags limit. To use the tag, the account owner must activate it in the AWS Billing console or by using the API. When an AWS Organizations management account owner activates the tag, it's also activated for all organization member accounts.

You can also organize your billing information based on resources that have the same tag key values. For example, you can tag several resources with a specific application name, and then organize your billing information. That way, you can see the total cost of that application across several services. For more information about setting up a cost allocation report with tags, see [The Monthly Cost Allocation Report](#) in the *AWS Billing User Guide*.

Note

If you just enabled reporting, data for the current month is available for viewing after 24 hours.

Cost Explorer is a reporting tool that's available as part of the AWS Free Tier. You can use **Cost Explorer** to view charts of your Amazon EKS resources from the last 13 months. You can also forecast how much you're likely to spend for the next three months. You can see patterns in how much you spend on AWS resources over time. For example, you can use it to identify areas that need further inquiry and see

trends that you can use to understand your costs. You also can specify time ranges for the data, and view time data by day or by month.

Working with tags using the console

Using the Amazon EKS console, you can manage the tags that are associated with new or existing clusters and managed node groups.

When you select a resource-specific page in the Amazon EKS console, the page displays a list of those resources. For example, if you select **Clusters** from the left navigation pane, the console displays a list of Amazon EKS clusters. When you select a resource from one of these lists (for example, a specific cluster) that supports tags, you can view and manage its tags on the **Tags** tab.

You can also use **Tag Editor** in the AWS Management Console, which provides a unified way to manage your tags. For more information, see [Tagging your AWS resources with Tag Editor](#) in the *AWS Tag Editor User Guide*.

Adding tags on a resource on creation

You can add tags to Amazon EKS clusters, managed node groups, and Fargate profiles when you create them. For more information, see [Creating an Amazon EKS cluster \(p. 25\)](#).

Adding and deleting tags on a resource

You can add or delete the tags that are associated with your clusters directly from the resource's page.

To add or delete a tag on an individual resource

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. On the navigation bar, select the AWS Region to use.
3. In the left navigation pane, choose **Clusters**.
4. Choose a specific cluster.
5. Choose the **Tags** tab, and then choose **Manage tags**.
6. On the **Manage tags** page, add or delete your tags as necessary.
 - To add a tag, choose **Add tag**. Then specify the key and value for each tag.
 - To delete a tag, choose **Remove tag**.
7. Repeat this process for each tag that you want to add or delete.
8. Choose **Update** to finish.

Working with tags using the CLI, API, or eksctl

Use the following AWS CLI commands or Amazon EKS API operations to add, update, list, and delete the tags for your resources. You can only use eksctl to add tags while simultaneously creating the new resources with one command.

Tagging support for Amazon EKS resources

Task	AWS CLI	AWS Tools for Windows PowerShell	API action
Add or overwrite one or more tags.	tag-resource	Add-EKSResourceTag	TagResource

Task	AWS CLI	AWS Tools for Windows PowerShell	API action
Delete one or more tags.	untag-resource	Remove-EKSResourceTag	UntagResource

The following examples show how to tag or untag resources using the AWS CLI.

Example 1: Tag an existing cluster

The following command tags an existing cluster.

```
aws eks tag-resource --resource-arn resource_ARN --tags team=devs
```

Example 2: Untag an existing cluster

The following command deletes a tag from an existing cluster.

```
aws eks untag-resource --resource-arn resource_ARN --tag-keys tag_key
```

Example 3: List tags for a resource

The following command lists the tags that are associated with an existing resource.

```
aws eks list-tags-for-resource --resource-arn resource_ARN
```

When you use some resource-creating actions, you can specify tags at the same time that you create the resource. The following actions support specifying a tag when you create a resource.

Task	AWS CLI	AWS Tools for Windows PowerShell	API action	eksctl
Create a cluster	create-cluster	New-EKSCluster	CreateCluster	create cluster
Create a managed node group*	create-nodegroup	New-EKSNodegroup	CreateNodegroup	create nodegroup
Create a Fargate profile	create-fargate-profile	New-EKSFargateProfile	CreateFargateProfile	create.html fargateprofile

* If you want to also tag the Amazon EC2 instances when you create a managed node group, create the managed node group using a launch template. For more information, see [Tagging Amazon EC2 instances \(p. 100\)](#). If your instances already exist, you can manually tag the instances. For more information, see [Tagging your resources](#) in the Amazon EC2 User Guide for Linux Instances.

Amazon EKS service quotas

Amazon EKS has integrated with Service Quotas, an AWS service that you can use to view and manage your quotas from a central location. For more information, see [What Is Service Quotas?](#) in the *Service Quotas User Guide*. With Service Quotas integration, you can quickly look up the value of your Amazon EKS and AWS Fargate service quotas using the AWS Management Console and AWS CLI.

AWS Management Console

To view Amazon EKS and Fargate service quotas using the AWS Management Console

1. Open the Service Quotas console at <https://console.aws.amazon.com/servicequotas/>.
2. In the left navigation pane, choose **AWS services**.
3. From the **AWS services** list, search for and select **Amazon Elastic Kubernetes Service (Amazon EKS) or AWS Fargate**.

In the **Service quotas** list, you can see the service quota name, applied value (if it's available), AWS default quota, and whether the quota value is adjustable.

4. To view additional information about a service quota, such as the description, choose the quota name.
5. (Optional) To request a quota increase, select the quota that you want to increase, select **Request quota increase**, enter or select the required information, and select **Request**.

To work more with service quotas using the AWS Management Console, see the [Service Quotas User Guide](#). To request a quota increase, see [Requesting a Quota Increase](#) in the [Service Quotas User Guide](#).

AWS CLI

To view Amazon EKS and Fargate service quotas using the AWS CLI

Run the following command to view your Amazon EKS quotas.

```
aws service-quotas list-aws-default-service-quotas \
--query 'Quotas[*]' \
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode} \
--service-code eks \
--output table
```

Run the following command to view your Fargate quotas.

```
aws service-quotas list-aws-default-service-quotas \
--query 'Quotas[*]' \
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode} \
--service-code fargate \
--output table
```

Note

The quota returned is the number of Amazon ECS tasks or Amazon EKS Pods that can run concurrently on Fargate in this account in the current AWS Region.

To work more with service quotas using the AWS CLI, see [service-quotas](#) in the [AWS CLI Command Reference](#). To request a quota increase, see the [request-service-quota-increase](#) command in the [AWS CLI Command Reference](#).

Service quotas

Name	Default	Adjust	Description
Clusters	Each supported Region: 100	Yes	The maximum number of EKS clusters in this account in the current Region.

Name	Default	Adjust	Description
Control plane security groups per cluster	Each supported Region: 4	No	The maximum number of control plane security groups per cluster (these are specified when you create the cluster).
Fargate profiles per cluster	Each supported Region: 10	Yes	The maximum number of Fargate profiles per cluster.
Label pairs per Fargate profile selector	Each supported Region: 5	Yes	The maximum number of label pairs per Fargate profile selector.
Managed node groups per cluster	Each supported Region: 30	Yes	The maximum number of managed node groups per cluster.
Nodes per managed node group	Each supported Region: 450	Yes	The maximum number of nodes per managed node group.
Public endpoint access CIDR ranges per cluster	Each supported Region: 40	No	The maximum number of public endpoint access CIDR ranges per cluster (these are specified when you create or update the cluster).
Registered clusters	Each supported Region: 10	Yes	The maximum number of registered clusters in this account in the current Region.
Selectors per Fargate profile	Each supported Region: 5	Yes	The maximum number of selectors per Fargate profile.

Note

The default values are the initial quotas set by AWS. These default values are separate from the actual applied quota values and maximum possible service quotas. For more information, see [Terminology in Service Quotas](#) in the *Service Quotas User Guide*.

These service quotas are listed under **Amazon Elastic Kubernetes Service (Amazon EKS)** in the Service Quotas console. To request a quota increase for values that are shown as adjustable, see [Requesting a quota increase](#) in the *Service Quotas User Guide*.

AWS Fargate service quotas

The **AWS Fargate** service in the Service Quotas console lists several service quotas. The following table only describes the quota that is applicable to Amazon EKS. You can configure alarms that alert you when your usage approaches a service quota. For more information, see [Creating a CloudWatch alarm to monitor Fargate resource usage metrics \(p. 144\)](#).

New AWS accounts might have lower initial quotas that can increase over time. Fargate constantly monitors the account usage within each AWS Region, and then automatically increases the quotas based

on the usage. You can also request a quota increase for values that are shown as adjustable. For more information, see [Requesting a quota increase](#) in the *Service Quotas User Guide*.

Name	Default	Adjustable	Description
Fargate On-Demand vCPU resource count	6	Yes	The number of Fargate vCPUs that can run concurrently as Fargate On-Demand in this account in the current Region.

Note

The default values are the initial quotas set by AWS. These default values are separate from the actual applied quota values and maximum possible service quotas. For more information, see [Terminology in Service Quotas](#) in the *Service Quotas User Guide*.

Note

Fargate additionally enforces Amazon ECS tasks and Amazon EKS Pods launch rate quotas. For more information, see [AWS Fargate throttling quotas](#) in the *Amazon Elastic Container Service User Guide for AWS Fargate*.

Security in Amazon EKS

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The [shared responsibility model](#) describes this as security of the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. For Amazon EKS, AWS is responsible for the Kubernetes control plane, which includes the control plane nodes and etcd database. Third-party auditors regularly test and verify the effectiveness of our security as part of the [AWS compliance programs](#). To learn about the compliance programs that apply to Amazon EKS, see [AWS Services in Scope by Compliance Program](#).
- **Security in the cloud** – Your responsibility includes the following areas.
 - The security configuration of the data plane, including the configuration of the security groups that allow traffic to pass from the Amazon EKS control plane into the customer VPC
 - The configuration of the nodes and the containers themselves
 - The node's operating system (including updates and security patches)
 - Other associated application software:
 - Setting up and managing network controls, such as firewall rules
 - Managing platform-level identity and access management, either with or in addition to IAM
 - The sensitivity of your data, your company's requirements, and applicable laws and regulations

This documentation helps you understand how to apply the shared responsibility model when using Amazon EKS. The following topics show you how to configure Amazon EKS to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon EKS resources.

Note

Linux containers are made up of control groups (cgroups) and namespaces that help limit what a container can access, but all containers share the same Linux kernel as the host Amazon EC2 instance. Running a container as the root user (UID 0) or granting a container access to host resources or namespaces such as the host network or host PID namespace are strongly discouraged, because doing so reduces the effectiveness of the isolation that containers provide.

Topics

- [Certificate signing \(p. 460\)](#)
- [Kubernetes service accounts \(p. 462\)](#)
- [Identity and access management for Amazon EKS \(p. 478\)](#)
- [Compliance validation for Amazon Elastic Kubernetes Service \(p. 519\)](#)
- [Resilience in Amazon EKS \(p. 520\)](#)
- [Infrastructure security in Amazon EKS \(p. 520\)](#)
- [Configuration and vulnerability analysis in Amazon EKS \(p. 521\)](#)
- [Security best practices for Amazon EKS \(p. 522\)](#)
- [Pod security policy \(p. 522\)](#)
- [Pod security policy \(PSP\) removal FAQ \(p. 525\)](#)

- [Using AWS Secrets Manager secrets with Kubernetes \(p. 527\)](#)
- [Amazon EKS Connector considerations \(p. 527\)](#)

Certificate signing

The Kubernetes Certificates API automates [X.509](#) credential provisioning. The API features a command line interface for Kubernetes API clients to request and obtain [X.509 certificates](#) from a Certificate Authority (CA). You can use the CertificateSigningRequest (CSR) resource to request that a denoted signer sign the certificate. Your requests are either approved or denied before they're signed. Kubernetes supports both built-in signers and custom signers with well-defined behaviors. This way, clients can predict what happens to their CSRs. To learn more about certificate signing, see [signing requests](#).

One of the built-in signers is `kubernetes.io/legacy-unknown`. The v1beta1 API of CSR resource honored this legacy-unknown signer. However, the stable v1 API of CSR doesn't allow the `signerName` to be set to `kubernetes.io/legacy-unknown`.

Amazon EKS version 1.21 and earlier allowed the `legacy-unknown` value as the `signerName` in v1beta1 CSR API. This API enables the Amazon EKS Certificate Authority (CA) to generate certificates. However, in Kubernetes version 1.22, the v1beta1 CSR API was replaced by the v1 CSR API. This API doesn't support the `signerName` of "legacy-unknown." If you want to use Amazon EKS CA for generating certificates on your clusters, you must use a custom signer. It was introduced in Amazon EKS version 1.22. To use the CSR v1 API version and generate a new certificate, you must migrate any existing manifests and API clients. Existing certificates that were created with the existing v1beta1 API are valid and function until the certificate expires. This includes the following:

- Trust distribution: None. There's no standard trust or distribution for this signer in a Kubernetes cluster.
- Permitted subjects: Any
- Permitted x509 extensions: Honors `subjectAltName` and `key usage` extensions and discards other extensions
- Permitted key usages: Must not include usages beyond ["key encipherment", "digital signature", "server auth"]

Note

Client certificate signing is not supported.

- Expiration/certificate lifetime: 1 year (default and maximum)
- CA bit allowed/disallowed: Not allowed

Example CSR generation with signerName

These steps shows how to generate a serving certificate for DNS name `myserver.default.svc` using `signerName: beta.eks.amazonaws.com/app-serving`. Use this as a guide for your own environment.

1. Run the `openssl genrsa -out myserver.key 2048` command to generate an RSA private key.

```
openssl genrsa -out myserver.key 2048
```

2. Run the following command to generate a certificate request.

```
openssl req -new -key myserver.key -out myserver.csr -subj "/CN=myserver.default.svc"
```

3. Generate a base64 value for the CSR request and store it in a variable for use in a later step.

```
base_64=$(cat myserver.csr | base64 -w 0 | tr -d "\n")
```

4. Run the following command to create a file named mycsr.yaml. In the following example, beta.eks.amazonaws.com/app-serving is the signerName.

```
cat >mycsr.yaml <<EOF
apiVersion: certificates.k8s.io/v1
kind: CertificateSigningRequest
metadata:
  name: myserver
spec:
  request: $base_64
  signerName: beta.eks.amazonaws.com/app-serving
  usages:
    - digital signature
    - key encipherment
    - server auth
EOF
```

5. Submit the CSR.

```
kubectl apply -f mycsr.yaml
```

6. Approve the serving certificate.

```
kubectl certificate approve myserver
```

7. Verify that the certificate was issued.

```
kubectl get csr myserver
```

An example output is as follows.

NAME	AGE	SIGNERNAME	REQUESTOR	CONDITION
myserver	3m20s	beta.eks.amazonaws.com/app-serving	kubernetes-admin	

Approved, Issued

8. Export the issued certificate.

```
kubectl get csr myserver -o jsonpath='{.status.certificate}' | base64 -d > myserver.crt
```

Certificate signing considerations before upgrading your cluster to Kubernetes 1.24

In Kubernetes 1.23 and earlier, kubelet serving certificates with unverifiable IP and DNS Subject Alternative Names (SANs) are automatically issued with unverifiable SANs. The SANs are omitted from the provisioned certificate. In 1.24 and later clusters, kubelet serving certificates aren't issued if a SAN can't be verified. This prevents the `kubectl exec` and `kubectl logs` commands from working.

Before upgrading your cluster to 1.24, determine whether your cluster has certificate signing requests (CSR) that haven't been approved by completing the following steps:

1. Run the following command.

```
kubectl get csr -A
```

An example output is as follows.

NAME	AGE	SIGNERNAME	REQUESTEDDURATION	REQUESTOR	CONDITION
csr-7znmf	90m	kubernetes.io/kubelet-serving		system:node:ip-192-168-42-149.region.compute.internal	<none>
		Approved		csr-9xx5q	90m kubernetes.io/kubelet-serving
				system:node:ip-192-168-65-38.region.compute.internal	<none>
		Approved, Issued			

If the returned output shows a CSR with a [kubernetes.io/kubelet-serving](#) signer that's Approved but not Issued for a node, then you need to approve the request.

- Manually approve the CSR. Replace `csr-7znmf` with your own value.

```
kubectl certificate approve csr-7znmf
```

To auto-approve CSRs in the future, we recommend that you write an approving controller that can automatically validate and approve CSRs that contain IP or DNS SANs that Amazon EKS can't verify.

Kubernetes service accounts

A Kubernetes service account provides an identity for processes that run in a Pod. For more information see [Managing Service Accounts](#) in the Kubernetes documentation. If your Pod needs access to AWS services, you can map the service account to an AWS Identity and Access Management identity to grant that access. For more information, see [IAM roles for service accounts \(p. 464\)](#).

Service account tokens

The [BoundServiceAccountTokenVolume](#) feature is enabled by default in Kubernetes versions. This feature improves the security of service account tokens by allowing workloads running on Kubernetes to request JSON web tokens that are audience, time, and key bound. Service account tokens have an expiration of one hour. In earlier Kubernetes versions, the tokens didn't have an expiration. This means that clients that rely on these tokens must refresh the tokens within an hour. The following [Kubernetes client SDKs](#) refresh tokens automatically within the required time frame:

- Go version 0.15.7 and later
- Python version 12.0.0 and later
- Java version 9.0.0 and later
- JavaScript version 0.10.3 and later
- Ruby master branch
- Haskell version 0.3.0.0
- C# version 7.0.5 and later

If your workload is using an earlier client version, then you must update it. To enable a smooth migration of clients to the newer time-bound service account tokens, Kubernetes adds an extended expiry period to the service account token over the default one hour. For Amazon EKS clusters, the extended expiry

period is 90 days. Your Amazon EKS cluster's Kubernetes API server rejects requests with tokens that are greater than 90 days old. We recommend that you check your applications and their dependencies to make sure that the Kubernetes client SDKs are the same or later than the versions listed previously.

When the API server receives requests with tokens that are greater than one hour old, it annotates the API audit log event with annotations.authentication.k8s.io/stale-token. The value of the annotation looks like the following example:

```
subject: system:serviceaccount:common:fluent-bit, seconds after warning threshold: 4185802.
```

If your cluster has [control plane logging \(p. 536\)](#) enabled, then the annotations are in the audit logs. You can use the following [CloudWatch Logs Insights](#) query to identify all the Pods in your Amazon EKS cluster that are using stale tokens:

```
fields @timestamp
| filter @logStream like /kube-apiserver-audit/
| filter @message like /seconds after warning threshold/
| parse @message "subject: *, seconds after warning threshold:*\\" as subject, elapsedtime
```

The subject refers to the service account that the Pod used. The elapsedtime indicates the elapsed time (in seconds) after reading the latest token. The requests to the API server are denied when the elapsedtime exceeds 90 days (7,776,000 seconds). You should proactively update your applications' Kubernetes client SDK to use one of the version listed previously that automatically refresh the token. If the service account token used is close to 90 days and you don't have sufficient time to update your client SDK versions before token expiration, then you can terminate existing Pods and create new ones. This results in refetching of the service account token, giving you an additional 90 days to update your client version SDKs.

If the Pod is part of a deployment, the suggested way to terminate Pods while keeping high availability is to perform a roll out with the following command. Replace *my-deployment* with the name of your deployment.

```
kubectl rollout restart deployment/my-deployment
```

Cluster add-ons

The following cluster add-ons have been updated to use the Kubernetes client SDKs that automatically refetch service account tokens. We recommend making sure that the listed versions, or later versions, are installed on your cluster.

- Amazon VPC CNI plugin for Kubernetes and metrics helper plugins version 1.8.0 and later. To check your current version or update it, see [Working with the Amazon VPC CNI plugin for Kubernetes Amazon EKS add-on \(p. 266\)](#) and [cni-metrics-helper](#).
- CoreDNS version 1.8.4 and later. To check your current version or update it, see [Working with the CoreDNS Amazon EKS add-on \(p. 341\)](#).
- AWS Load Balancer Controller version 2.0.0 and later. To check your current version or update it, see [Installing the AWS Load Balancer Controller add-on \(p. 333\)](#).
- A current kube-proxy version. To check your current version or update it, see [Updating the Kubernetes kube-proxy self-managed add-on \(p. 347\)](#).
- AWS for Fluent Bit version 2.25.0 or later. To update your current version, see [Releases](#) on GitHub.
- Fluentd image version [1.14.6-1.2](#) or later and Fluentd filter plugin for Kubernetes metadata version [2.11.1](#) or later.

IAM roles for service accounts

Applications in a Pod's containers can use an AWS SDK or the AWS CLI to make API requests to AWS services using AWS Identity and Access Management (IAM) permissions. Applications must sign their AWS API requests with AWS credentials. IAM roles for service accounts provide the ability to manage credentials for your applications, similar to the way that Amazon EC2 instance profiles provide credentials to Amazon EC2 instances. Instead of creating and distributing your AWS credentials to the containers or using the Amazon EC2 instance's role, you associate an IAM role with a Kubernetes service account and configure your Pods to use the service account. You can't use IAM roles for service accounts with [local clusters for Amazon EKS on AWS Outposts \(p. 590\)](#).

IAM roles for service accounts provide the following benefits:

- **Least privilege** – You can scope IAM permissions to a service account, and only Pods that use that service account have access to those permissions. This feature also eliminates the need for third-party solutions such as `kiam` or `kube2iam`.
- **Credential isolation** – A Pod's containers can only retrieve credentials for the IAM role that's associated with the service account that the container uses. A container never has access to credentials that are used by other containers in other Pods. When using IAM roles for service accounts, the Pod's containers also have the permissions assigned to the [Amazon EKS node IAM role \(p. 501\)](#), unless you block Pod access to the [Amazon EC2 Instance Metadata Service \(IMDS\)](#). For more information, see [Restrict access to the instance profile assigned to the worker node](#).
- **Auditability** – Access and event logging is available through AWS CloudTrail to help ensure retrospective auditing.

Enable IAM roles for service accounts by completing the following procedures:

1. [the section called "Creating an IAM OIDC provider" \(p. 465\)](#) – You only complete this procedure once for each cluster.
2. [the section called "Configuring role and service account" \(p. 466\)](#) – Complete this procedure for each unique set of permissions that you want an application to have.
3. [the section called "Configuring Pods" \(p. 472\)](#) – Complete this procedure for each Pod that needs access to AWS services.

IAM, Kubernetes, and OpenID Connect (OIDC) background information

In 2014, AWS Identity and Access Management added support for federated identities using OpenID Connect (OIDC). This feature allows you to authenticate AWS API calls with supported identity providers and receive a valid OIDC JSON web token (JWT). You can pass this token to the AWS STS `AssumeRoleWithWebIdentity` API operation and receive IAM temporary role credentials. You can use these credentials to interact with any AWS service, including Amazon S3 and DynamoDB.

Each JWT token is signed by a signing key pair. The keys are served on the OIDC provider managed by Amazon EKS and the private key rotates every 7 days. Amazon EKS keeps the public keys until they expire. If you connect external OIDC clients, be aware that you need to refresh the keys before the public key expires.

Kubernetes has long used service accounts as its own internal identity system. Pods can authenticate with the Kubernetes API server using an auto-mounted token (which was a non-OIDC JWT) that only the Kubernetes API server could validate. These legacy service account tokens don't expire, and rotating the signing key is a difficult process. In Kubernetes version 1.12, support was added for a new `ProjectedServiceAccountToken` feature. This feature is an OIDC JSON web token that also contains the service account identity and supports a configurable audience.

Amazon EKS hosts a public OIDC discovery endpoint for each cluster that contains the signing keys for the `ProjectedServiceAccountToken` JSON web tokens so external systems, such as IAM, can validate and accept the OIDC tokens that are issued by Kubernetes.

Creating an IAM OIDC provider for your cluster

Your cluster has an [OpenID Connect](#) (OIDC) issuer URL associated with it. To use AWS Identity and Access Management (IAM) roles for service accounts, an IAM OIDC provider must exist for your cluster's OIDC issuer URL.

Prerequisites

- An existing Amazon EKS cluster. To deploy one, see [Getting started with Amazon EKS \(p. 6\)](#).
- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.
- The `kubectl` command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use `kubectl` version 1.26, 1.27, or 1.28 with it. To install or upgrade `kubectl`, see [Installing or updating kubectl \(p. 6\)](#).
- An existing `kubectl config` file that contains your cluster configuration. To create a `kubectl config` file, see [Creating or updating a kubeconfig file for an Amazon EKS cluster \(p. 431\)](#).

You can create an IAM OIDC provider for your cluster using `eksctl` or the AWS Management Console.

`eksctl`

Prerequisite

Version 0.160.0 or later of the `eksctl` command line tool installed on your device or AWS CloudShell. To install or update `eksctl`, see [Installing or updating eksctl \(p. 13\)](#).

To create an IAM OIDC identity provider for your cluster with `eksctl`

1. Determine the OIDC issuer ID for your cluster.

Retrieve your cluster's OIDC issuer ID and store it in a variable. Replace `my-cluster` with your own value.

```
cluster_name=my-cluster
```

```
oidc_id=$(aws eks describe-cluster --name $cluster_name --query "cluster.identity.oidc.issuer" --output text | cut -d '/' -f 5)
```

```
echo $oidc_id
```

2. Determine whether an IAM OIDC provider with your cluster's issuer ID is already in your account.

```
aws iam list-open-id-connect-providers | grep $oidc_id | cut -d "/" -f4
```

If output is returned, then you already have an IAM OIDC provider for your cluster and you can skip the next step. If no output is returned, then you must create an IAM OIDC provider for your cluster.

3. Create an IAM OIDC identity provider for your cluster with the following command.

```
eksctl utils associate-iam-oidc-provider --cluster $cluster_name --approve
```

Note

If you enable the EKS VPC endpoint, the EKS OIDC service endpoint can't be accessed from inside that VPC. Consequently, your operations such as creating an OIDC provider with eksctl in the VPC will not work and will result in a timeout when attempting to request <https://oidc.eks.region.amazonaws.com>. An example error message follows:

```
** server can't find oidc.eks.region.amazonaws.com: NXDOMAIN
```

To complete this step, you can run the command outside the VPC, for example in AWS CloudShell or on a computer connected to the internet.

AWS Management Console

To create an IAM OIDC identity provider for your cluster with the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left pane, select **Clusters**, and then select the name of your cluster on the **Clusters** page.
3. In the **Details** section on the **Overview** tab, note the value of the **OpenID Connect provider URL**.
4. Open the IAM console at <https://console.aws.amazon.com/iam/>.
5. In the left navigation pane, choose **Identity Providers** under **Access management**. If a **Provider** is listed that matches the URL for your cluster, then you already have a provider for your cluster. If a provider isn't listed that matches the URL for your cluster, then you must create one.
6. To create a provider, choose **Add provider**.
7. For **Provider type**, select **OpenID Connect**.
8. For **Provider URL**, enter the OIDC provider URL for your cluster, and then choose **Get thumbprint**.
9. For **Audience**, enter **sts.amazonaws.com** and choose **Add provider**.

Next step

[the section called "Configuring role and service account" \(p. 466\)](#)

Configuring a Kubernetes service account to assume an IAM role

This topic covers how to configure a Kubernetes service account to assume an AWS Identity and Access Management (IAM) role. Any Pods that are configured to use the service account can then access any AWS service that the role has permissions to access.

Prerequisites

- An existing cluster. If you don't have one, you can create one by following one of the [Getting started with Amazon EKS \(p. 6\)](#) guides.

- An existing IAM OpenID Connect (OIDC) provider for your cluster. To learn if you already have one or how to create one, see [Creating an IAM OIDC provider for your cluster \(p. 465\)](#).
- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.
- The `kubectl` command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use `kubectl` version 1.26, 1.27, or 1.28 with it. To install or upgrade `kubectl`, see [Installing or updating kubectl \(p. 6\)](#).
- An existing `kubectl` config file that contains your cluster configuration. To create a `kubectl` config file, see [Creating or updating a kubeconfig file for an Amazon EKS cluster \(p. 431\)](#).

To associate an IAM role with a Kubernetes service account

1. If you want to associate an existing IAM policy to your IAM role, skip to the [next step \(p. 467\)](#).

Create an IAM policy. You can create your own policy, or copy an AWS managed policy that already grants some of the permissions that you need and customize it to your specific requirements. For more information, see [Creating IAM policies](#) in the *IAM User Guide*.

- a. Create a file that includes the permissions for the AWS services that you want your Pods to access. For a list of all actions for all AWS services, see the [Service Authorization Reference](#).

You can run the following command to create an example policy file that allows read-only access to an Amazon S3 bucket. You can optionally store configuration information or a bootstrap script in this bucket, and the containers in your Pod can read the file from the bucket and load it into your application. If you want to create this example policy, copy the following contents to your device. Replace `my-pod-secrets-bucket` with your bucket name and run the command.

```
cat >my-policy.json <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::my-pod-secrets-bucket"
        }
    ]
}
EOF
```

- b. Create the IAM policy.

```
aws iam create-policy --policy-name my-policy --policy-document file://my-policy.json
```

2. Create an IAM role and associate it with a Kubernetes service account. You can use either `eksctl` or the AWS CLI.

eksctl

Prerequisite

Version 0.160.0 or later of the eksctl command line tool installed on your device or AWS CloudShell. To install or update eksctl, see [Installing or updating eksctl \(p. 13\)](#).

Replace *my-service-account* with the name of the Kubernetes service account that you want eksctl to create and associate with an IAM role. Replace *default* with the namespace that you want eksctl to create the service account in. Replace *my-cluster* with the name of your cluster. Replace *my-role* with the name of the role that you want to associate the service account to. If it doesn't already exist, eksctl creates it for you. Replace *111122223333* with your account ID and *my-policy* with the name of an existing policy.

```
eksctl create iamserviceaccount --name my-service-account --namespace default --cluster my-cluster --role-name my-role \  
--attach-policy-arn arn:aws:iam::111122223333:policy/my-policy --approve
```

Important

- If the role or service account already exist, the previous command might fail. eksctl has different options that you can provide in those situations. For more information run `eksctl create iamserviceaccount --help`.
- Before [using the service account with a Pod \(p. 472\)](#), the service account that you specified or that eksctl created must be bound to an existing Kubernetes role, or clusterrole that includes the Kubernetes permissions that you require for the service account. For more information, see [Using RBAC Authorization](#) in the Kubernetes documentation.

AWS CLI

1. If you have an existing Kubernetes service account that you want to assume an IAM role, then you can skip this step.

Create a Kubernetes service account. Copy the following contents to your device. Replace *my-service-account* with your desired name and *default* with a different namespace, if necessary. If you change *default*, the namespace must already exist.

```
cat >my-service-account.yaml <<EOF  
apiVersion: v1  
kind: ServiceAccount  
metadata:  
  name: my-service-account  
  namespace: default  
EOF  
kubectl apply -f my-service-account.yaml
```

Important

Before [using the service account with a Pod \(p. 472\)](#), the service account that you created must be bound to an existing Kubernetes role, or clusterrole that includes the Kubernetes permissions that you require for the service account. For more information, see [Using RBAC Authorization](#) in the Kubernetes documentation.

2. Set your AWS account ID to an environment variable with the following command.

```
account_id=$(aws sts get-caller-identity --query "Account" --output text)
```

3. Set your cluster's OIDC identity provider to an environment variable with the following command. Replace *my-cluster* with the name of your cluster.

```
oidc_provider=$(aws eks describe-cluster --name my-cluster --region $AWS_REGION
--query "cluster.identity.oidc.issuer" --output text | sed -e "s/^https:\/\/\//")
```

4. Set variables for the namespace and name of the service account. Replace *my-service-account* with the Kubernetes service account that you want to assume the role. Replace *default* with the namespace of the service account.

```
export namespace=default
export service_account=my-service-account
```

5. Run the following command to create a trust policy file for the IAM role. If you want to allow all service accounts within a namespace to use the role, then copy the following contents to your device. Replace *StringEquals* with *StringLike* and replace *\$service_account* with *. You can add multiple entries in the *StringEquals* or *StringLike* conditions to allow multiple service accounts or namespaces to assume the role. To allow roles from a different AWS account than the account that your cluster is in to assume the role, see [the section called “Cross-account IAM permissions” \(p. 476\)](#) for more information.

```
cat >trust-relationship.json <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::$account_id:oidc-provider/$oidc_provider"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringEquals$namespace:$service_account"
                }
            }
        }
    ]
}
EOF
```

6. Create the role. Replace *my-role* with a name for your IAM role, and *my-role-description* with a description for your role.

```
aws iam create-role --role-name my-role --assume-role-policy-document
file:///trust-relationship.json --description "my-role-description"
```

7. Attach an IAM policy to your role. Replace *my-role* with the name of your IAM role and *my-policy* with the name of an existing policy that you created.

```
aws iam attach-role-policy --role-name my-role --policy-arn=arn:aws:iam::
$account_id:policy/my-policy
```

8. Annotate your service account with the Amazon Resource Name (ARN) of the IAM role that you want the service account to assume. Replace *my-role* with the name of your existing IAM role. Suppose that you allowed a role from a different AWS account than the account that your cluster is in to assume the role in a previous step. Then, make sure to specify the

AWS account and role from the other account. For more information, see [the section called "Cross-account IAM permissions" \(p. 476\)](#).

```
kubectl annotate serviceaccount -n $namespace $service_account eks.amazonaws.com/
role-arn=arn:aws:iam::$account_id:role/my-role
```

3. Confirm that the role and service account are configured correctly.

- a. Confirm that the IAM role's trust policy is configured correctly.

```
aws iam get-role --role-name my-role --query Role.AssumeRolePolicyDocument
```

An example output is as follows.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::111122223333:oidc-provider/
oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringEquals": {
                    "oidc.eks.region-code.amazonaws.com/
id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:default:my-
service-account",
                    "oidc.eks.region-code.amazonaws.com/
id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com"
                }
            }
        }
    ]
}
```

- b. Confirm that the policy that you attached to your role in a previous step is attached to the role.

```
aws iam list-attached-role-policies --role-name my-role --query
AttachedPolicies[].PolicyArn --output text
```

An example output is as follows.

```
arn:aws:iam::111122223333:policy/my-policy
```

- c. Set a variable to store the Amazon Resource Name (ARN) of the policy that you want to use. Replace **my-policy** with the name of the policy that you want to confirm permissions for.

```
export policy_arn=arn:aws:iam::111122223333:policy/my-policy
```

- d. View the default version of the policy.

```
aws iam get-policy --policy-arn $policy_arn
```

An example output is as follows.

```
{
```

```

    "Policy": [
        "PolicyName": "my-policy",
        "PolicyId": "EXAMPLEB10WGLDEXAMPLE",
        "Arn": "arn:aws:iam::111122223333:policy/my-policy",
        "Path": "/",
        "DefaultVersionId": "v1",
        [...]
    ]
}

```

- e. View the policy contents to make sure that the policy includes all the permissions that your Pod needs. If necessary, replace **1** in the following command with the version that's returned in the previous output.

```
aws iam get-policy-version --policy-arn $policy_arn --version-id v1
```

An example output is as follows.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::my-pod-secrets-bucket"
        }
    ]
}
```

If you created the example policy in a previous step, then your output is the same. If you created a different policy, then the **example** content is different.

- f. Confirm that the Kubernetes service account is annotated with the role.

```
kubectl describe serviceaccount my-service-account -n default
```

An example output is as follows.

```

Name:           my-service-account
Namespace:      default
Annotations:    eks.amazonaws.com/role-arn: arn:aws:iam::111122223333:role/my-role
Image pull secrets: <none>
Mountable secrets: my-service-account-token-qqjfl
Tokens:         my-service-account-token-qqjfl
[...]

```

4. (Optional) [the section called “Configuring AWS STS endpoint” \(p. 474\)](#). AWS recommends using a regional AWS STS endpoint instead of the global endpoint. This reduces latency, provides built-in redundancy, and increases session token validity.

Next step

[the section called “Configuring Pods” \(p. 472\)](#)

Configuring Pods to use a Kubernetes service account

If a Pod needs to access AWS services, then you must configure it to use a Kubernetes service account. The service account must be associated to an AWS Identity and Access Management (IAM) role that has permissions to access the AWS services.

Prerequisites

- An existing cluster. If you don't have one, you can create one using one of the [Getting started with Amazon EKS \(p. 6\)](#) guides.
- An existing IAM OpenID Connect (OIDC) provider for your cluster. To learn if you already have one or how to create one, see [Creating an IAM OIDC provider for your cluster \(p. 465\)](#).
- An existing Kubernetes service account that's associated with an IAM role. The service account must be annotated with the Amazon Resource Name (ARN) of the IAM role. The role must have an associated IAM policy that contains the permissions that you want your Pods to have to use AWS services. For more information about how to create the service account and role, and configure them, see [the section called "Configuring role and service account" \(p. 466\)](#).
- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.
- The kubectl command line tool is installed on your device or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use kubectl version 1.26, 1.27, or 1.28 with it. To install or upgrade kubectl, see [Installing or updating kubectl \(p. 6\)](#).
- An existing kubectl config file that contains your cluster configuration. To create a kubectl config file, see [Creating or updating a kubeconfig file for an Amazon EKS cluster \(p. 431\)](#).

To configure a Pod to use a service account

1. Use the following command to create a deployment manifest that you can deploy a Pod to confirm configuration with. The Pod uses an existing Kubernetes service account. The service account must be properly configured. For more information, see [the section called "Configuring role and service account" \(p. 466\)](#). Replace the *example values* with your own values.

```
cat >my-deployment.yaml <<EOF
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
spec:
  selector:
    matchLabels:
      app: my-app
  template:
    metadata:
      labels:
        app: my-app
    spec:
      serviceAccountName: my-service-account
      containers:
        - name: my-app
          image: public.ecr.aws/nginx/nginx:X.XX
EOF
```

EOF

2. Deploy the manifest to your cluster.

```
kubectl apply -f my-deployment.yaml
```

3. Confirm that the required environment variables exist for your Pod.

- a. View the Pods that were deployed with the deployment in the previous step.

```
kubectl get pods | grep my-app
```

An example output is as follows.

```
my-app-6f4dff6cb-76cv9  1/1      Running     0          3m28s
```

- b. View the ARN of the IAM role that the Pod is using.

```
kubectl describe pod my-app-6f4dff6cb-76cv9 | grep AWS_ROLE_ARN:
```

An example output is as follows.

```
AWS_ROLE_ARN:           arn:aws:iam::111122223333:role/my-role
```

The role ARN must match the role ARN that you annotated the existing service account with. For more about annotating the service account, see [the section called “Configuring role and service account” \(p. 466\)](#).

- c. Confirm that the Pod has a web identity token file mount.

```
kubectl describe pod my-app-6f4dff6cb-76cv9 | grep AWS_WEB_IDENTITY_TOKEN_FILE:
```

An example output is as follows.

```
AWS_WEB_IDENTITY_TOKEN_FILE: /var/run/secrets/eks.amazonaws.com/serviceaccount/token
```

The kubelet requests and stores the token on behalf of the Pod. By default, the kubelet refreshes the token if the token is older than 80 percent of its total time to live or older than 24 hours. You can modify the expiration duration for any account other than the default service account by using the settings in your Pod spec. For more information, see [Service Account Token Volume Projection](#) in the Kubernetes documentation.

The [Amazon EKS Pod Identity Webhook](#) on the cluster watches for Pods that use a service account with the following annotation:

```
eks.amazonaws.com/role-arn: arn:aws:iam::111122223333:role/my-role
```

The webhook applies the previous environment variables to those Pods. Your cluster doesn't need to use the webhook to configure the environment variables and token file mounts. You can manually configure Pods to have these environment variables. The [supported versions of the AWS SDK \(p. 478\)](#) look for these environment variables first in the credential chain provider. The role credentials are used for Pods that meet this criteria.

4. Confirm that your Pods can interact with the AWS services using the permissions that you assigned in the IAM policy attached to your role.

Note

When a Pod uses AWS credentials from an IAM role that's associated with a service account, the AWS CLI or other SDKs in the containers for that Pod use the credentials that are provided by that role. If you don't restrict access to the credentials that are provided to the [Amazon EKS node IAM role \(p. 501\)](#), the Pod still has access to these credentials. For more information, see [Restrict access to the instance profile assigned to the worker node](#).

If your Pods can't interact with the services as you expected, complete the following steps to confirm that everything is properly configured.

- a. Confirm that your Pods use an AWS SDK version that supports assuming an IAM role through an OpenID Connect web identity token file. For more information, see [the section called "Supported SDKs" \(p. 478\)](#).
- b. Confirm that the deployment is using the service account.

```
kubectl describe deployment my-app | grep "Service Account"
```

An example output is as follows.

```
Service Account: my-service-account
```

- c. If your Pods still can't access services, review the [steps \(p. 470\)](#) that are described in [the section called "Configuring role and service account" \(p. 466\)](#) to confirm that your role and service account are configured properly.

Configuring the AWS Security Token Service endpoint for a service account

If you're using a Kubernetes service account with [IAM roles for service accounts \(p. 464\)](#), then you can configure the type of AWS Security Token Service endpoint that's used by the service account if your cluster and platform version are the same or later than those listed in the following table. If your Kubernetes or platform version are earlier than those listed in the table, then your service accounts can only use the global endpoint.

Kubernetes version	Platform version	Default endpoint type
1.28	eks.1	Regional
1.27	eks.1	Regional
1.26	eks.1	Regional
1.25	eks.1	Regional
1.24	eks.2	Regional
1.23	eks.1	Regional

AWS recommends using the regional AWS STS endpoints instead of the global endpoint. This reduces latency, provides built-in redundancy, and increases session token validity. The AWS Security Token Service must be active in the AWS Region where the Pod is running. Moreover, your application must

have built-in redundancy for a different AWS Region in the event of a failure of the service in the AWS Region. For more information, see [Managing AWS STS in an AWS Region](#) in the IAM User Guide.

Prerequisites

- An existing cluster. If you don't have one, you can create one using one of the [Getting started with Amazon EKS \(p. 6\)](#) guides.
- An existing IAM OIDC provider for your cluster. For more information, see [Creating an IAM OIDC provider for your cluster \(p. 465\)](#).
- An existing Kubernetes service account configured for use with the [Amazon EKS IAM for service accounts \(p. 464\)](#) feature.

To configure the endpoint type used by a Kubernetes service account

The following examples all use the `aws-node` Kubernetes service account used by the [Amazon VPC CNI plugin \(p. 272\)](#). You can replace the *example values* with your own service accounts, Pods, namespaces, and other resources.

1. Select a Pod that uses a service account that you want to change the endpoint for. Determine which AWS Region that the Pod runs in. Replace `aws-node-6mfgv` with your Pod name and `kube-system` with your Pod's namespace.

```
kubectl describe pod aws-node-6mfgv -n kube-system |grep Node:
```

An example output is as follows.

```
ip-192-168-79-166.us-west-2/192.168.79.166
```

In the previous output, the Pod is running on a node in the us-west-2 AWS Region.

2. Determine the endpoint type that the Pod's service account is using.

```
kubectl describe pod aws-node-6mfgv -n kube-system |grep AWS_STS_REGIONAL_ENDPOINTS
```

An example output is as follows.

```
AWS_STS_REGIONAL_ENDPOINTS: regional
```

If the current endpoint is global, then `global` is returned in the output. If no output is returned, then the default endpoint type is in use and has not been overridden.

3. If your cluster or platform version are the same or later than those listed in the table, then you can change the endpoint type used by your service account from the default type to a different type with one of the following commands. Replace `aws-node` with the name of your service account and `kube-system` with the namespace for your service account.
 - If your default or current endpoint type is global and you want to change it to regional:

```
kubectl annotate serviceaccount -n kube-system aws-node eks.amazonaws.com/sts-regional-endpoints=true
```

If you are using [IAM roles for service accounts \(p. 464\)](#) to generate pre-signed S3 URLs in your application running in Pods' containers, the format of the URL for regional endpoints is similar to the following example:

```
https://bucket.s3.us-west-2.amazonaws.com/path?...&X-Amz-Credential=your-access-key-id/date/us-west-2/s3/aws4_request&...
```

- If your default or current endpoint type is regional and you want to change it to global:

```
kubectl annotate serviceaccount -n kube-system aws-node eks.amazonaws.com/sts-regional-endpoints=false
```

If your application is explicitly making requests to AWS STS global endpoints and you don't override the default behavior of using regional endpoints in Amazon EKS clusters, then requests will fail with an error. For more information, see [Pod containers receive the following error: An error occurred \(SignatureDoesNotMatch\) when calling the GetCallerIdentity operation: Credential should be scoped to a valid region \(p. 519\)](#).

If you're using [IAM roles for service accounts \(p. 464\)](#) to generate pre-signed S3 URLs in your application running in Pods' containers, the format of the URL for global endpoints is similar to the following example:

```
https://bucket.s3.amazonaws.com/path?...&X-Amz-Credential=your-access-key-id/date/us-west-2/s3/aws4_request&...
```

If you have automation that expects the pre-signed URL in a certain format or if your application or downstream dependencies that use pre-signed URLs have expectations for the AWS Region targeted, then make the necessary changes to use the appropriate AWS STS endpoint.

4. Delete and re-create any existing Pods that are associated with the service account to apply the credential environment variables. The mutating web hook doesn't apply them to Pods that are already running. You can replace `Pods`, `kube-system`, and `-l k8s-app=aws-node` with the information for the Pods that you set your annotation for.

```
kubectl delete Pods -n kube-system -l k8s-app=aws-node
```

5. Confirm that all Pods restarted.

```
kubectl get Pods -n kube-system -l k8s-app=aws-node
```

6. View the environment variables for one of the Pods. Verify that the `AWS_STS_REGIONAL_ENDPOINTS` value is what you set it to in a previous step.

```
kubectl describe pod aws-node-kzbtr -n kube-system |grep AWS_STS_REGIONAL_ENDPOINTS
```

An example output is as follows.

```
AWS_STS_REGIONAL_ENDPOINTS=regional
```

Cross-account IAM permissions

You can configure cross-account IAM permissions either by creating an identity provider from another account's cluster or by using chained AssumeRole operations. In the following examples, *Account A* owns an Amazon EKS cluster that supports IAM roles for service accounts. Pods that are running on that cluster must assume IAM permissions from *Account B*.

Example Create an identity provider from another account's cluster

Example

In this example, Account A provides Account B with the OpenID Connect (OIDC) issuer URL from their cluster. Account B follows the instructions in [Creating an IAM OIDC provider for your cluster \(p. 465\)](#) and [Configuring a Kubernetes service account to assume an IAM role \(p. 466\)](#) using the OIDC issuer URL from Account A's cluster. Then, a cluster administrator annotates the service account in Account A's cluster to use the role from Account B ([444455556666](#)).

```
apiVersion: v1
kind: ServiceAccount
metadata:
  annotations:
    eks.amazonaws.com/role-arn: arn:aws:iam::444455556666:role/account-b-role
```

Example Use chained AssumeRole operations

Example

In this example, Account B creates an IAM policy with the permissions to give to Pods in Account A's cluster. Account B ([444455556666](#)) attaches that policy to an IAM role with a trust relationship that allows AssumeRole permissions to Account A ([111122223333](#)).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {}
    }
  ]
}
```

Account A creates a role with a trust policy that gets credentials from the identity provider created with the cluster's OIDC issuer address.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::111122223333:oidc-provider/oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
      },
      "Action": "sts:AssumeRoleWithWebIdentity"
    }
  ]
}
```

Account A attaches a policy to that role with the following permissions to assume the role that Account B created.

```
{
  "Version": "2012-10-17",
```

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "arn:aws:iam::44445556666:role/account-b-role"
    }
]
```

The application code for Pods to assume Account B's role uses two profiles: `account_b_role` and `account_a_role`. The `account_b_role` profile uses the `account_a_role` profile as its source. For the AWS CLI, the `~/.aws/config` file is similar to the following.

```
[profile account_b_role]
source_profile = account_a_role
role_arn=arn:aws:iam::44445556666:role/account-b-role

[profile account_a_role]
web_identity_token_file = /var/run/secrets/eks.amazonaws.com/serviceaccount/token
role_arn=arn:aws:iam::111122223333:role/account-a-role
```

To specify chained profiles for other AWS SDKs, consult the documentation for the SDK that you're using. For more information, see [Tools to Build on AWS](#).

Using a supported AWS SDK

When using [the section called "IAM roles for service accounts" \(p. 464\)](#), the containers in your Pods must use an AWS SDK version that supports assuming an IAM role through an OpenID Connect web identity token file. Make sure that you're using the following versions, or later, for your AWS SDK:

- Java (Version 2) – [2.10.11](#)
- Java – [1.11.704](#)
- Go – [1.23.13](#)
- Python (Boto3) – [1.9.220](#)
- Python (botocore) – [1.12.200](#)
- AWS CLI – [1.16.232](#)
- Node – [2.525.0](#) and [3.27.0](#)
- Ruby – [3.58.0](#)
- C++ – [1.7.174](#)
- .NET – [3.3.659.1](#) – You must also include `AWSSDK.SecurityToken`.
- PHP – [3.110.7](#)

Many popular Kubernetes add-ons, such as the [Cluster Autoscaler](#), the [the section called "AWS Load Balancer Controller" \(p. 333\)](#), and the [Amazon VPC CNI plugin for Kubernetes \(p. 272\)](#) support IAM roles for service accounts.

To ensure that you're using a supported SDK, follow the installation instructions for your preferred SDK at [Tools to Build on AWS](#) when you build your containers.

Identity and access management for Amazon EKS

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and

authorized (have permissions) to use Amazon EKS resources. IAM is an AWS service that you can use with no additional charge.

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Amazon EKS.

Service user – If you use the Amazon EKS service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon EKS features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Amazon EKS, see [Troubleshooting IAM \(p. 517\)](#).

Service administrator – If you're in charge of Amazon EKS resources at your company, you probably have full access to Amazon EKS. It's your job to determine which Amazon EKS features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon EKS, see [How Amazon EKS works with IAM \(p. 482\)](#).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon EKS. To view example Amazon EKS identity-based policies that you can use in IAM, see [Amazon EKS identity-based policy examples \(p. 485\)](#).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see [How to sign in to your AWS account](#) in the [AWS Sign-In User Guide](#).

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see [Signing AWS API requests](#) in the [IAM User Guide](#).

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see [Multi-factor authentication](#) in the [AWS IAM Identity Center User Guide](#) and [Using multi-factor authentication \(MFA\) in AWS](#) in the [IAM User Guide](#).

AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the *AWS account root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list

of tasks that require you to sign in as the root user, see [Tasks that require root user credentials](#) in the *IAM User Guide*.

IAM users and groups

An [IAM user](#) is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see [Rotate access keys regularly for use cases that require long-term credentials](#) in the *IAM User Guide*.

An [IAM group](#) is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see [When to create an IAM user \(instead of a role\)](#) in the *IAM User Guide*.

IAM roles

An [IAM role](#) is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by [switching roles](#). You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see [Using IAM roles](#) in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see [Creating a role for a third-party Identity Provider](#) in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see [Permission sets](#) in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
- **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see [Actions, resources, and condition keys for Amazon Elastic Kubernetes Service](#) in the *Service Authorization Reference*.

- **Service role** – A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.
- **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.
- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see [When to create an IAM role \(instead of a user\)](#) in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see [Overview of JSON policies](#) in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM policies](#) in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see [Choosing between managed policies and inline policies](#) in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are *IAM role trust policies* and *Amazon S3 bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the

resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must [specify a principal](#) in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Access control lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see [Access control list \(ACL\) overview](#) in the *Amazon Simple Storage Service Developer Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the Principal field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see [Permissions boundaries for IAM entities](#) in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see [How SCPs work](#) in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see [Session policies](#) in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see [Policy evaluation logic](#) in the *IAM User Guide*.

How Amazon EKS works with IAM

Before you use IAM to manage access to Amazon EKS, you should understand what IAM features are available to use with Amazon EKS. To get a high-level view of how Amazon EKS and other AWS services work with IAM, see [AWS services that work with IAM](#) in the *IAM User Guide*.

Topics

- [Amazon EKS identity-based policies \(p. 483\)](#)

- [Amazon EKS resource-based policies \(p. 485\)](#)
- [Authorization based on Amazon EKS tags \(p. 485\)](#)
- [Amazon EKS IAM roles \(p. 485\)](#)

Amazon EKS identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. Amazon EKS supports specific actions, resources, and condition keys. To learn about all of the elements that you use in a JSON policy, see [IAM JSON policy elements reference](#) in the *IAM User Guide*.

Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The Action element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

Policy actions in Amazon EKS use the following prefix before the action: eks:. For example, to grant someone permission to get descriptive information about an Amazon EKS cluster, you include the `DescribeCluster` action in their policy. Policy statements must include either an Action or NotAction element.

To specify multiple actions in a single statement, separate them with commas as follows:

```
"Action": ["eks:action1", "eks:action2"]
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Describe`, include the following action:

```
"Action": "eks:Describe*"
```

To see a list of Amazon EKS actions, see [Actions defined by Amazon Elastic Kubernetes Service](#) in the *Service Authorization Reference*.

Resources

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The Resource JSON policy element specifies the object or objects to which the action applies. Statements must include either a Resource or a NotResource element. As a best practice, specify a resource using its [Amazon Resource Name \(ARN\)](#). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

The Amazon EKS cluster resource has the following ARN.

```
arn:aws:eks:region-code:account-id:cluster/cluster-name
```

For more information about the format of ARNs, see [Amazon resource names \(ARNs\) and AWS service namespaces](#).

For example, to specify the cluster with the name *my-cluster* in your statement, use the following ARN:

```
"Resource": "arn:aws:eks:region-code:111122223333:cluster/my-cluster"
```

To specify all clusters that belong to a specific account and AWS Region, use the wildcard (*):

```
"Resource": "arn:aws:eks:region-code:111122223333:cluster/*"
```

Some Amazon EKS actions, such as those for creating resources, can't be performed on a specific resource. In those cases, you must use the wildcard (*).

```
"Resource": "*"
```

To see a list of Amazon EKS resource types and their ARNs, see [Resources defined by Amazon Elastic Kubernetes Service](#) in the *Service Authorization Reference*. To learn which actions you can specify the ARN of each resource, see [Actions defined by Amazon Elastic Kubernetes Service](#).

Condition keys

Amazon EKS defines its own set of condition keys and also supports using some global condition keys. To see all AWS global condition keys, see [AWS Global Condition Context Keys](#) in the *IAM User Guide*.

You can set condition keys when associating an OpenID Connect provider to your cluster. For more information, see [Example IAM policy \(p. 430\)](#).

All Amazon EC2 actions support the aws :RequestedRegion and ec2 :Region condition keys. For more information, see [Example: Restricting Access to a Specific AWS Region](#).

For a list of Amazon EKS condition keys, see [Conditions defined by Amazon Elastic Kubernetes Service](#) in the *Service Authorization Reference*. To learn which actions and resources you can use a condition key with, see [Actions defined by Amazon Elastic Kubernetes Service](#).

Examples

To view examples of Amazon EKS identity-based policies, see [Amazon EKS identity-based policy examples \(p. 485\)](#).

When you create an Amazon EKS cluster, the [IAM principal](#) that creates the cluster is automatically granted system:masters permissions in the cluster's role-based access control (RBAC) configuration in the Amazon EKS control plane. This principal doesn't appear in any visible configuration, so make sure to keep track of which principal originally created the cluster. To grant additional IAM principals the ability to interact with your cluster, edit the aws-auth ConfigMap within Kubernetes and create a Kubernetes rolebinding or clusterrolebinding with the name of a group that you specify in the aws-auth ConfigMap.

For more information about working with the ConfigMap, see [Enabling IAM principal access to your cluster \(p. 420\)](#).

Amazon EKS resource-based policies

Amazon EKS does not support resource-based policies.

Authorization based on Amazon EKS tags

You can attach tags to Amazon EKS resources or pass tags in a request to Amazon EKS. To control access based on tags, you provide tag information in the [condition element](#) of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys. For more information about tagging Amazon EKS resources, see [Tagging your Amazon EKS resources \(p. 451\)](#). For more information about which actions that you can use tags in condition keys with, see [Actions defined by Amazon EKS](#) in the [Service Authorization Reference](#).

Amazon EKS IAM roles

An [IAM role](#) is an entity within your AWS account that has specific permissions.

Using temporary credentials with Amazon EKS

You can use temporary credentials to sign in with federation, assume an IAM role, or to assume a cross-account role. You obtain temporary security credentials by calling AWS STS API operations such as [AssumeRole](#) or [GetFederationToken](#).

Amazon EKS supports using temporary credentials.

Service-linked roles

[Service-linked roles](#) allow AWS services to access resources in other services to complete an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An administrator can view but can't edit the permissions for service-linked roles.

Amazon EKS supports service-linked roles. For details about creating or managing Amazon EKS service-linked roles, see [Using service-linked roles for Amazon EKS \(p. 490\)](#).

Service roles

This feature allows a service to assume a [service role](#) on your behalf. This role allows the service to access resources in other services to complete an action on your behalf. Service roles appear in your IAM account and are owned by the account. This means that an IAM administrator can change the permissions for this role. However, doing so might break the functionality of the service.

Amazon EKS supports service roles. For more information, see [Amazon EKS cluster IAM role \(p. 499\)](#) and [Amazon EKS node IAM role \(p. 501\)](#).

Choosing an IAM role in Amazon EKS

When you create a cluster resource in Amazon EKS, you must choose a role to allow Amazon EKS to access several other AWS resources on your behalf. If you have previously created a service role, then Amazon EKS provides you with a list of roles to choose from. It's important to choose a role that has the Amazon EKS managed policies attached to it. For more information, see [Check for an existing cluster role \(p. 499\)](#) and [Check for an existing node role \(p. 501\)](#).

Amazon EKS identity-based policy examples

By default, IAM users and roles don't have permission to create or modify Amazon EKS resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM

administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see [Creating policies on the JSON tab](#) in the *IAM User Guide*.

When you create an Amazon EKS cluster, the [IAM principal](#) that creates the cluster is automatically granted system:masters permissions in the cluster's role-based access control (RBAC) configuration in the Amazon EKS control plane. This principal doesn't appear in any visible configuration, so make sure to keep track of which principal originally created the cluster. To grant additional IAM principals the ability to interact with your cluster, edit the aws-auth ConfigMap within Kubernetes and create a Kubernetes rolebinding or clusterrolebinding with the name of a group that you specify in the aws-auth ConfigMap.

For more information about working with the ConfigMap, see [Enabling IAM principal access to your cluster \(p. 420\)](#).

Topics

- [Policy best practices \(p. 486\)](#)
- [Using the Amazon EKS console \(p. 487\)](#)
- [Allow IAM users to view their own permissions \(p. 487\)](#)
- [Create a Kubernetes cluster on the AWS Cloud \(p. 488\)](#)
- [Create a local Kubernetes cluster on an Outpost \(p. 489\)](#)
- [Update a Kubernetes cluster \(p. 490\)](#)
- [List or describe all clusters \(p. 490\)](#)

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon EKS resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see [AWS managed policies](#) or [AWS managed policies for job functions](#) in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see [Policies and permissions in IAM](#) in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see [IAM JSON policy elements: Condition](#) in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see [IAM Access Analyzer policy validation](#) in the *IAM User Guide*.

- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see [Configuring MFA-protected API access](#) in the *IAM User Guide*.

For more information about best practices in IAM, see [Security best practices in IAM](#) in the *IAM User Guide*.

Using the Amazon EKS console

To access the Amazon EKS console, an [IAM principal](#), must have a minimum set of permissions. These permissions allow the principal to list and view details about the Amazon EKS resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for principals with that policy attached to them.

To ensure that your IAM principals can still use the Amazon EKS console, create a policy with your own unique name, such as `AmazonEKSAdminPolicy`. Attach the policy to the principals. For more information, see [Adding and removing IAM identity permissions](#) in the *IAM User Guide*.

Important

The following example policy allows a principal to view information on the **Configuration** tab in the console. To view information on the **Overview** and **Resources** tabs in the AWS Management Console, the principal also needs Kubernetes permissions. For more information, see [Required permissions \(p. 529\)](#).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "eks:*"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "iam:PassRole",  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "iam:PassedToService": "eks.amazonaws.com"  
                }  
            }  
        }  
    ]  
}
```

You don't need to allow minimum console permissions for principals that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that you're trying to perform.

Allow IAM users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam>ListGroupsForUser",
                "iam>ListAttachedUserPolicies",
                "iam>ListUserPolicies",
                "iam GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam GetPolicy",
                "iam>ListAttachedGroupPolicies",
                "iam>ListGroupPolicies",
                "iam>ListPolicyVersions",
                "iam>ListPolicies",
                "iam>ListUsers"
            ],
            "Resource": "*"
        }
    ]
}

```

Create a Kubernetes cluster on the AWS Cloud

This example policy includes the minimum permissions required to create an Amazon EKS cluster named *my-cluster* in the *us-west-2* AWS Region. You can replace the AWS Region with the AWS Region that you want to create a cluster in. If you see a warning that says **The actions in your policy do not support resource-level permissions and require you to choose All resources** in the AWS Management Console, it can be safely ignored. If your account already has the *AWSServiceRoleForAmazonEKS* role, you can remove the *iam:CreateServiceLinkedRole* action from the policy. If you've ever created an Amazon EKS cluster in your account then this role already exists, unless you deleted it.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "eks>CreateCluster",
            "Resource": "arn:aws:eks:us-west-2:111122223333:cluster/my-cluster"
        },
        {
            "Effect": "Allow",
            "Action": "iam>CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::111122223333:role/aws-service-role/
eks.amazonaws.com/AWSServiceRoleForAmazonEKS",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "iam:AWSPropertyName": "eks"
                }
            }
        },
        {
            "Effect": "Allow",

```

```

        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::111122223333:role/cluster-role-name"
    }
}
]
```

Create a local Kubernetes cluster on an Outpost

This example policy includes the minimum permissions required to create an Amazon EKS local cluster named *my-cluster* on an Outpost in the *us-west-2* AWS Region. You can replace the AWS Region with the AWS Region that you want to create a cluster in. If you see a warning that says **The actions in your policy do not support resource-level permissions and require you to choose All resources** in the AWS Management Console, it can be safely ignored. If your account already has the AWSServiceRoleForAmazonEKSLocalOutpost role, you can remove the iam:CreateServiceLinkedRole action from the policy. If you've ever created an Amazon EKS local cluster on an Outpost in your account then this role already exists, unless you deleted it.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "eks:CreateCluster",
            "Resource": "arn:aws:eks:us-west-2:111122223333:cluster/my-cluster"
        },
        {
            "Action": [
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "iam:GetRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::111122223333:role/aws-service-role/outposts.eks-local.amazonaws.com/AWSServiceRoleForAmazonEKSLocalOutpost"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iam>ListAttachedRolePolicies"
            ],
            "Resource": "arn:aws:iam::111122223333:role/cluster-role-name"
        },
        {
            "Action": [
                "iam>CreateInstanceProfile",
                "iam:TagInstanceProfile",
                "iam>AddRoleToInstanceProfile",
                "iam:GetInstanceProfile",
                "iam>DeleteInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile"
            ],
            "Resource": "arn:aws:iam::*:instance-profile/eks-local-*",
            "Effect": "Allow"
        },
    ]
}
```

Update a Kubernetes cluster

This example policy includes the minimum permission required to update a cluster named `my-cluster` in the us-west-2 AWS Region.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "eks:UpdateClusterVersion",  
            "Resource": "arn:aws:eks:us-west-2:111122223333:cluster/my-cluster"  
        }  
    ]  
}
```

List or describe all clusters

This example policy includes the minimum permissions required to list and describe all clusters in your account. An [IAM principal](#) must be able to list and describe clusters to use the `update-kubeconfig` AWS CLI command.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "eks:DescribeCluster",  
                "eks>ListClusters"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Using service-linked roles for Amazon EKS

Amazon Elastic Kubernetes Service 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 Amazon EKS. Service-linked roles are predefined by Amazon EKS and include all the permissions that the service requires to call other AWS services on your behalf.

Topics

- [Using roles for Amazon EKS clusters \(p. 490\)](#)
- [Using roles for Amazon EKS node groups \(p. 492\)](#)
- [Using roles for Amazon EKS Fargate profiles \(p. 494\)](#)
- [Using roles to connect a Kubernetes cluster to Amazon EKS \(p. 496\)](#)
- [Using roles for Amazon EKS local clusters on Outpost \(p. 497\)](#)

Using roles for Amazon EKS clusters

Amazon Elastic Kubernetes Service 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 Amazon EKS. Service-linked roles are predefined by Amazon EKS and include all the permissions that the service requires to call other AWS services on your behalf.

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

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon EKS resources because you can't inadvertently remove permission to access the resources.

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

Service-linked role permissions for Amazon EKS

Amazon EKS uses the service-linked role named `AWSServiceRoleForAmazonEKS` – The role allows Amazon EKS to manage clusters in your account. The attached policies allow the role to manage the following resources: network interfaces, security groups, logs, and VPCs.

Note

The `AWSServiceRoleForAmazonEKS` service-linked role is distinct from the role required for cluster creation. For more information, see [Amazon EKS cluster IAM role \(p. 499\)](#).

The `AWSServiceRoleForAmazonEKS` service-linked role trusts the following services to assume the role:

- `eks.amazonaws.com`

The role permissions policy allows Amazon EKS to complete the following actions on the specified resources:

- [AmazonEKSServiceRolePolicy](#)

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 Amazon EKS

You don't need to manually create a service-linked role. When you create a cluster in the AWS Management Console, the AWS CLI, or the AWS API, Amazon EKS creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a cluster, Amazon EKS creates the service-linked role for you again.

Editing a service-linked role for Amazon EKS

Amazon EKS does not allow you to edit the `AWSServiceRoleForAmazonEKS` 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 Amazon EKS

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 your service-linked role before you can manually delete it.

Cleaning up a service-linked role

Before you can use IAM to delete a service-linked role, you must first delete any resources used by the role.

Note

If the Amazon EKS 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 delete Amazon EKS resources used by the `AWSServiceRoleForAmazonEKS` role.

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, choose **Clusters**.
3. If your cluster has any node groups or Fargate profiles, you must delete them before you can delete the cluster. For more information, see [Deleting a managed node group \(p. 107\)](#) and [Deleting a Fargate profile \(p. 139\)](#).
4. On the **Clusters** page, choose the cluster that you want to delete and choose **Delete**.
5. Type the name of the cluster in the deletion confirmation window, and then choose **Delete**.
6. Repeat this procedure for any other clusters in your account. Wait for all of the delete operations to finish.

Manually delete the service-linked role

Use the IAM console, the AWS CLI, or the AWS API to delete the `AWSServiceRoleForAmazonEKS` service-linked role. For more information, see [Deleting a service-linked role](#) in the *IAM User Guide*.

Supported regions for Amazon EKS service-linked roles

Amazon EKS supports using service-linked roles in all of the regions where the service is available. For more information, see [Amazon EKS endpoints and quotas](#).

Using roles for Amazon EKS node groups

Amazon EKS 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 Amazon EKS. Service-linked roles are predefined by Amazon EKS and include all the permissions that the service requires to call other AWS services on your behalf.

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

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon EKS resources because you can't inadvertently remove permission to access the resources.

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

Service-linked role permissions for Amazon EKS

Amazon EKS uses the service-linked role named `AWSServiceRoleForAmazonEKSNodegroup` – The role allows Amazon EKS to manage node groups in your account. The attached policies allow the role to manage the following resources: Auto Scaling groups, security groups, launch templates and IAM instance profiles..

The `AWSServiceRoleForAmazonEKSNodegroup` service-linked role trusts the following services to assume the role:

- `eks-nodegroup.amazonaws.com`

The role permissions policy allows Amazon EKS to complete the following actions on the specified resources:

- [AWSServiceRoleForAmazonEKSNodegroup](#)

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 Amazon EKS

You don't need to manually create a service-linked role. When you `CreateNodegroup` in the AWS Management Console, the AWS CLI, or the AWS API, Amazon EKS creates the service-linked role for you.

Important

This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. If you were using the Amazon EKS service before January 1, 2017, when it began supporting service-linked roles, then Amazon EKS created the `AWSServiceRoleForAmazonEKSNodegroup` role in your account. To learn more, see [A new role appeared in my IAM account](#).

Creating a service-linked role in Amazon EKS (AWS API)

You don't need to manually create a service-linked role. When you create a managed node group in the AWS Management Console, the AWS CLI, or the AWS API, Amazon EKS creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create another managed node group, Amazon EKS creates the service-linked role for you again.

Editing a service-linked role for Amazon EKS

Amazon EKS does not allow you to edit the `AWSServiceRoleForAmazonEKSNodegroup` 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 Amazon EKS

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 your service-linked role before you can manually delete it.

Cleaning up a service-linked role

Before you can use IAM to delete a service-linked role, you must first delete any resources used by the role.

Note

If the Amazon EKS 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 delete Amazon EKS resources used by the `AWSServiceRoleForAmazonEKSNodegroup` role.

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, choose **Clusters**.
3. Select the **Compute** tab.
4. In the **Node groups** section, choose the node group to delete.
5. Type the name of the node group in the deletion confirmation window, and then choose **Delete**.
6. Repeat this procedure for any other node groups in the cluster. Wait for all of the delete operations to finish.

Manually delete the service-linked role

Use the IAM console, the AWS CLI, or the AWS API to delete the `AWSServiceRoleForAmazonEKSNodegroup` service-linked role. For more information, see [Deleting a service-linked role](#) in the *IAM User Guide*.

Supported regions for Amazon EKS service-linked roles

Amazon EKS supports using service-linked roles in all of the regions where the service is available. For more information, see [Amazon EKS endpoints and quotas](#).

Using roles for Amazon EKS Fargate profiles

Amazon EKS 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 Amazon EKS. Service-linked roles are predefined by Amazon EKS and include all the permissions that the service requires to call other AWS services on your behalf.

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

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon EKS resources because you can't inadvertently remove permission to access the resources.

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

Service-linked role permissions for Amazon EKS

Amazon EKS uses the service-linked role named `AWSServiceRoleForAmazonEKSForFargate` – The role allows Amazon EKS Fargate to configure VPC networking required for Fargate Pods. The attached policies allow the role to create and delete elastic network interfaces and describe elastic network Interfaces and resources.

The `AWSServiceRoleForAmazonEKSForFargate` service-linked role trusts the following services to assume the role:

- `eks-fargate.amazonaws.com`

The role permissions policy allows Amazon EKS to complete the following actions on the specified resources:

- [AmazonEKSForFargateServiceRolePolicy](#)

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 Amazon EKS

You don't need to manually create a service-linked role. When you create a Fargate profile in the AWS Management Console, the AWS CLI, or the AWS API, Amazon EKS creates the service-linked role for you.

Important

This service-linked role can appear in your account if you completed an action in another service that uses the features supported by this role. If you were using the Amazon EKS service before December 13, 2019, when it began supporting service-linked roles, then Amazon EKS created the `AWSServiceRoleForAmazonEKSForFargate` role in your account. To learn more, see [A New role appeared in my IAM account](#).

Creating a service-linked role in Amazon EKS (AWS API)

You don't need to manually create a service-linked role. When you create a Fargate profile in the AWS Management Console, the AWS CLI, or the AWS API, Amazon EKS creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create another managed node group, Amazon EKS creates the service-linked role for you again.

Editing a service-linked role for Amazon EKS

Amazon EKS does not allow you to edit the `AWSServiceRoleForAmazonEKSForFargate` 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 Amazon EKS

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 your service-linked role before you manually delete it.

Cleaning up a service-linked role

Before you can use IAM to delete a service-linked role, you must first delete any resources used by the role.

Note

If the Amazon EKS 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 delete Amazon EKS resources used by the `AWSServiceRoleForAmazonEKSForFargate` role.

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, choose **Clusters**.
3. On the **Clusters** page, select your cluster.
4. Select the **Compute** tab.

5. If there are any Fargate profiles in the **Fargate profiles** section, select each one individually, and then choose **Delete**.
6. Type the name of the profile in the deletion confirmation window, and then choose **Delete**.
7. Repeat this procedure for any other Fargate profiles in the cluster and for any other clusters in your account.

Manually delete the service-linked role

Use the IAM console, the AWS CLI, or the AWS API to delete the `AWSServiceRoleForAmazonEKSForFargate` service-linked role. For more information, see [Deleting a service-linked role](#) in the *IAM User Guide*.

Supported regions for Amazon EKS service-linked roles

Amazon EKS supports using service-linked roles in all of the regions where the service is available. For more information, see [Amazon EKS endpoints and quotas](#).

Using roles to connect a Kubernetes cluster to Amazon EKS

Amazon EKS 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 Amazon EKS. Service-linked roles are predefined by Amazon EKS and include all the permissions that the service requires to call other AWS services on your behalf.

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

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon EKS resources because you can't inadvertently remove permission to access the resources.

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

Service-linked role permissions for Amazon EKS

Amazon EKS uses the service-linked role named `AWSServiceRoleForAmazonEKSConnector` – The role allows Amazon EKS to connect Kubernetes clusters. The attached policies allow the role to manage necessary resources to connect to your registered Kubernetes cluster.

The `AWSServiceRoleForAmazonEKSConnector` service-linked role trusts the following services to assume the role:

- `eks-connector.amazonaws.com`

The role permissions policy allows Amazon EKS to complete the following actions on the specified resources:

- [AmazonEKSConnectorServiceRolePolicy](#)

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 Amazon EKS

You don't need to manually create a service-linked role to connect a cluster. When you connect a cluster in the AWS Management Console, the AWS CLI, eksctl, or the AWS API, Amazon EKS creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you connect a cluster, Amazon EKS creates the service-linked role for you again.

Editing a service-linked role for Amazon EKS

Amazon EKS does not allow you to edit the `AWSServiceRoleForAmazonEKSConnector` 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 Amazon EKS

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 your service-linked role before you can manually delete it.

Cleaning up a service-linked role

Before you can use IAM to delete a service-linked role, you must first delete any resources used by the role.

Note

If the Amazon EKS 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 delete Amazon EKS resources used by the `AWSServiceRoleForAmazonEKSConnector` role.

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, choose **Clusters**.
3. On the **Clusters** page, select your cluster.
4. Select the **Deregister** tab and then select the **Ok** tab.

Manually delete the service-linked role

Use the IAM console, the AWS CLI, or the AWS API to delete the `AWSServiceRoleForAmazonEKSConnector` service-linked role. For more information, see [Deleting a service-linked role](#) in the *IAM User Guide*.

Using roles for Amazon EKS local clusters on Outpost

Amazon Elastic Kubernetes Service 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 Amazon EKS. Service-linked roles are predefined by Amazon EKS and include all the permissions that the service requires to call other AWS services on your behalf.

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

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon EKS resources because you can't inadvertently remove permission to access the resources.

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

Service-linked role permissions for Amazon EKS

Amazon EKS uses the service-linked role named `AWSServiceRoleForAmazonEKSLocalOutpost` – The role allows Amazon EKS to manage local clusters in your account. The attached policies allow the role to manage the following resources: network interfaces, security groups, logs, and Amazon EC2 instances.

Note

The `AWSServiceRoleForAmazonEKSLocalOutpost` service-linked role is distinct from the role required for cluster creation. For more information, see [Amazon EKS cluster IAM role \(p. 499\)](#).

The `AWSServiceRoleForAmazonEKSLocalOutpost` service-linked role trusts the following services to assume the role:

- `outposts.eks-local.amazonaws.com`

The role permissions policy allows Amazon EKS to complete the following actions on the specified resources:

- [AmazonEKSServiceRolePolicy](#)

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 Amazon EKS

You don't need to manually create a service-linked role. When you create a cluster in the AWS Management Console, the AWS CLI, or the AWS API, Amazon EKS creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a cluster, Amazon EKS creates the service-linked role for you again.

Editing a service-linked role for Amazon EKS

Amazon EKS does not allow you to edit the `AWSServiceRoleForAmazonEKSLocalOutpost` service-linked role. After you create a service-linked role, you can't 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 Amazon EKS

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 your service-linked role before you can manually delete it.

Cleaning up a service-linked role

Before you can use IAM to delete a service-linked role, you must first delete any resources used by the role.

Note

If the Amazon EKS 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 delete Amazon EKS resources used by the `AWSServiceRoleForAmazonEKSLocalOutpost` role.

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left navigation pane, choose Amazon EKS **Clusters**.
3. If your cluster has any node groups or Fargate profiles, you must delete them before you can delete the cluster. For more information, see [Deleting a managed node group \(p. 107\)](#) and [Deleting a Fargate profile \(p. 139\)](#).
4. On the **Clusters** page, choose the cluster that you want to delete and choose **Delete**.
5. Type the name of the cluster in the deletion confirmation window, and then choose **Delete**.
6. Repeat this procedure for any other clusters in your account. Wait for all of the delete operations to finish.

Manually delete the service-linked role

Use the IAM console, the AWS CLI, or the AWS API to delete the `AWSServiceRoleForAmazonEKSLocalOutpost` service-linked role. For more information, see [Deleting a service-linked role](#) in the *IAM User Guide*.

Supported regions for Amazon EKS service-linked roles

Amazon EKS supports using service-linked roles in all of the regions where the service is available. For more information, see [Amazon EKS endpoints and quotas](#).

Amazon EKS cluster IAM role

Kubernetes clusters managed by Amazon EKS make calls to other AWS services on your behalf to manage the resources that you use with the service. Before you can create Amazon EKS clusters, you must create an IAM role with the following IAM policies:

- [AmazonEKSClusterPolicy](#)

Note

Prior to April 16, 2020, [AmazonEKSServicePolicy](#) was also required and the suggested name was `eksServiceRole`. With the `AWSServiceRoleForAmazonEKS` service-linked role, that policy is no longer required for clusters created on or after April 16, 2020.

Check for an existing cluster role

You can use the following procedure to check and see if your account already has the Amazon EKS cluster role.

To check for the `eksClusterRole` in the IAM console

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the left navigation pane, choose **Roles**.
3. Search the list of roles for `eksClusterRole`. If a role that includes `eksClusterRole` doesn't exist, then see [Creating the Amazon EKS cluster role \(p. 500\)](#) to create the role. If a role that includes `eksClusterRole` does exist, then select the role to view the attached policies.

4. Choose **Permissions**.
5. Ensure that the **AmazonEKSClusterPolicy** managed policy is attached to the role. If the policy is attached, your Amazon EKS cluster role is properly configured.
6. Choose **Trust relationships**, and then choose **Edit trust policy**.
7. Verify that the trust relationship contains the following policy. If the trust relationship matches the following policy, choose **Cancel**. If the trust relationship doesn't match, copy the policy into the **Edit trust policy** window and choose **Update policy**.

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

Creating the Amazon EKS cluster role

You can use the AWS Management Console or the AWS CLI to create the cluster role.

AWS Management Console

To create your Amazon EKS cluster role in the IAM console

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.
2. Choose **Roles**, then **Create role**.
3. Under **Trusted entity type**, select **AWS service**.
4. From the **Use cases for other AWS services** dropdown list, choose **EKS**.
5. Choose **EKS - Cluster** for your use case, and then choose **Next**.
6. On the **Add permissions** tab, choose **Next**.
7. For **Role name**, enter a unique name for your role, such as **eksClusterRole**.
8. For **Description**, enter descriptive text such as **Amazon EKS - Cluster role**.
9. Choose **Create role**.

AWS CLI

1. Copy the following contents to a file named **cluster-trust-policy.json**.

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

}

2. Create the role. You can replace **eksClusterRole** with any name that you choose.

```
aws iam create-role \
--role-name eksClusterRole \
--assume-role-policy-document file://"cluster-trust-policy.json"
```

3. Attach the required IAM policy to the role.

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy \
--role-name eksClusterRole
```

Amazon EKS node IAM role

The Amazon EKS node kubelet daemon makes calls to AWS APIs on your behalf. Nodes receive permissions for these API calls through an IAM instance profile and associated policies. Before you can launch nodes and register them into a cluster, you must create an IAM role for those nodes to use when they are launched. This requirement applies to nodes launched with the Amazon EKS optimized AMI provided by Amazon, or with any other node AMIs that you intend to use.

Note

You can't use the same role that is used to create any clusters.

Before you create nodes, you must create an IAM role with the following IAM policies:

- [AmazonEKSWorkerNodePolicy](#)
- [AmazonEC2ContainerRegistryReadOnly](#)
- Either the [AmazonEKS_CNI_Policy](#) managed policy (if you created your cluster with the IPv4 family) or an [IPv6 policy that you create \(p. 276\)](#) (if you created your cluster with the IPv6 family). Rather than attaching the policy to this role however, we recommend that you attach the policy to a separate role used specifically for the Amazon VPC CNI add-on. For more information about creating a separate role for the Amazon VPC CNI add-on, see [the section called "Configure plugin for IAM account" \(p. 272\)](#).

Note

The Amazon EC2 node groups must have a different IAM role than the Fargate profile. For more information, see [Amazon EKS Pod execution IAM role \(p. 504\)](#).

Check for an existing node role

You can use the following procedure to check and see if your account already has the Amazon EKS node role.

To check for the eksNodeRole in the IAM console

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the left navigation pane, choose **Roles**.
3. Search the list of roles for eksNodeRole, AmazonEKSNodeRole, or NodeInstanceRole. If a role with one of those names doesn't exist, then see [Creating the Amazon EKS node IAM role \(p. 502\)](#) to create the role. If a role that contains eksNodeRole, AmazonEKSNodeRole, or NodeInstanceRole does exist, then select the role to view the attached policies.
4. Choose **Permissions**.

5. Ensure that the **AmazonEKSWorkerNodePolicy** and **AmazonEC2ContainerRegistryReadOnly** managed policies are attached to the role.

Note

If the **AmazonEKS_CNI_Policy** policy is attached to the role, we recommend removing it and attaching it to an IAM role that is mapped to the aws-node Kubernetes service account instead. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).

6. Choose **Trust relationships**, and then choose **Edit trust policy**.
7. Verify that the trust relationship contains the following policy. If the trust relationship matches the following policy, choose **Cancel**. If the trust relationship doesn't match, copy the policy into the **Edit trust policy** window and choose **Update policy**.

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

Creating the Amazon EKS node IAM role

You can create the node IAM role with the AWS Management Console or the AWS CLI.

AWS Management Console

To create your Amazon EKS node role in the IAM console

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the left navigation pane, choose **Roles**.
3. On the **Roles** page, choose **Create role**.
4. On the **Select trusted entity** page, do the following:
 - a. In the **Trusted entity type** section, choose **AWS service**.
 - b. Under **Use case**, choose **EC2**.
 - c. Choose **Next**.
5. On the **Add permissions** page, do the following:
 - a. In the **Filter policies** box, enter **AmazonEKSWorkerNodePolicy**.
 - b. Select the check box to the left of **AmazonEKSWorkerNodePolicy** in the search results.
 - c. Choose **Clear filters**.
 - d. In the **Filter policies** box, enter **AmazonEC2ContainerRegistryReadOnly**.
 - e. Select the check box to the left of **AmazonEC2ContainerRegistryReadOnly** in the search results.

Either the **AmazonEKS_CNI_Policy** managed policy, or an [IPv6 policy \(p. 276\)](#) that you create must also be attached to either this role or to a different role that's mapped to the aws-node Kubernetes service account. We recommend assigning the policy to the role associated to the Kubernetes service account instead of assigning it to this role. For more

information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).

- f. Choose **Next**.
6. On the **Name, review, and create** page, do the following:
 - a. For **Role name**, enter a unique name for your role, such as **AmazonEKSNodeRole**.
 - b. For **Description**, replace the current text with descriptive text such as **Amazon EKS - Node role**.
 - c. Under **Add tags (Optional)**, add metadata to the role by attaching tags as key-value pairs. For more information about using tags in IAM, see [Tagging IAM Entities](#) in the *IAM User Guide*.
 - d. Choose **Create role**.

AWS CLI

1. Run the following command to create the `node-role-trust-relationship.json` file.

```
cat >node-role-trust-relationship.json <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
```

2. Create the IAM role.

```
aws iam create-role \
--role-name AmazonEKSNodeRole \
--assume-role-policy-document file:///"node-role-trust-relationship.json"
```

3. Attach two required IAM managed policies to the IAM role.

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy \
--role-name AmazonEKSNodeRole
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly \
--role-name AmazonEKSNodeRole
```

4. Attach one of the following IAM policies to the IAM role depending on which IP family you created your cluster with. The policy must be attached to this role or to a role associated to the Kubernetes aws-node service account that's used for the Amazon VPC CNI plugin for Kubernetes. We recommend assigning the policy to the role associated to the Kubernetes service account. To assign the policy to the role associated to the Kubernetes service account, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).

- IPv4

```
aws iam attach-role-policy \
```

```
--policy-arn arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy \
--role-name AmazonEKSNodeRole
```

- IPv6

1. Copy the following text and save it to a file named `vpc-cni-ipv6-policy.json`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeInstances",
                "ec2:DescribeTags",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstanceTypes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*.*:network-interface/*"
            ]
        }
    ]
}
```

2. Create the IAM policy.

```
aws iam create-policy --policy-name AmazonEKS_IPV6_Policy --policy-document
file://vpc-cni-ipv6-policy.json
```

3. Attach the IAM policy to the IAM role. Replace `111122223333` with your account ID.

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::111122223333:policy/AmazonEKS_IPV6_Policy \
--role-name AmazonEKSNodeRole
```

Amazon EKS Pod execution IAM role

The Amazon EKS Pod execution role is required to run Pods on AWS Fargate infrastructure.

When your cluster creates Pods on AWS Fargate infrastructure, the components running on the Fargate infrastructure must make calls to AWS APIs on your behalf. This is so that they can do actions such as pull container images from Amazon ECR or route logs to other AWS services. The Amazon EKS Pod execution role provides the IAM permissions to do this.

When you create a Fargate profile, you must specify a Pod execution role for the Amazon EKS components that run on the Fargate infrastructure using the profile. This role is added to the cluster's Kubernetes [Role based access control](#) (RBAC) for authorization. This allows the kubelet that's running on the Fargate infrastructure to register with your Amazon EKS cluster so that it can appear in your cluster as a node.

Note

The Fargate profile must have a different IAM role than Amazon EC2 node groups.

Important

The containers running in the Fargate Pod can't assume the IAM permissions associated with a Pod execution role. To give the containers in your Fargate Pod permissions to access other AWS services, you must use [IAM roles for service accounts \(p. 464\)](#).

Before you create a Fargate profile, you must create an IAM role with the [AmazonEKSFargatePodExecutionRolePolicy](#).

Check for a correctly configured existing Pod execution role

You can use the following procedure to check and see if your account already has a correctly configured Amazon EKS Pod execution role. To avoid a confused deputy security problem, it's important that the role restricts access based on SourceArn. You can modify the execution role as needed to include support for Fargate profiles on other clusters.

To check for an Amazon EKS Pod execution role in the IAM console

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the left navigation pane, choose **Roles**.
3. On the **Roles** page, search the list of roles for **AmazonEKSFargatePodExecutionRole**. If the role doesn't exist, see [Creating the Amazon EKS Pod execution role \(p. 506\)](#) to create the role. If the role does exist, choose the role.
4. On the **AmazonEKSFargatePodExecutionRole** page, do the following:
 - a. Choose **Permissions**.
 - b. Ensure that the **AmazonEKSFargatePodExecutionRolePolicy** Amazon managed policy is attached to the role.
 - c. Choose **Trust relationships**.
 - d. Choose **Edit trust policy**.
5. On the **Edit trust policy** page, verify that the trust relationship contains the following policy and has a line for Fargate profiles on your cluster. If so, choose **Cancel**.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Condition": {  
                "ArnLike": {  
                    "aws:SourceArn": "arn:aws:eks:region-code:111122223333:fargateprofile/my-  
cluster/*"  
                }  
            },  
            "Principal": {  
                "Service": "eks-fargate-pods.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

If the policy matches but doesn't have a line specifying the Fargate profiles on your cluster, you can add the following line at the top of the ArnLike object. Replace **region-code** with the AWS Region that your cluster is in, **111122223333** with your account ID, and **my-cluster** with the name of your cluster.

```
"aws:SourceArn": "arn:aws:eks:region-code:111122223333:fargateprofile/my-cluster/*",
```

If the policy doesn't match, copy the full previous policy into the form and choose **Update policy**. Replace *region-code* with the AWS Region that your cluster is in. If you want to use the same role in all AWS Regions in your account, replace *region-code* with *. Replace *111122223333* with your account ID and *my-cluster* with the name of your cluster. If you want to use the same role for all clusters in your account, replace *my-cluster* with *.

Creating the Amazon EKS Pod execution role

If you don't already have the Amazon EKS Pod execution role for your cluster, you can use the AWS Management Console or the AWS CLI to create it.

AWS Management Console

To create an AWS FargatePod execution role with the AWS Management Console

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the left navigation pane, choose **Roles**.
3. On the **Roles** page, choose **Create role**.
4. On the **Select trusted entity** page, do the following:
 - a. In the **Trusted entity type** section, choose **AWS service**.
 - b. From the **Use cases for other AWS services** dropdown list, choose **EKS**.
 - c. Choose **EKS - Fargate Pod**.
 - d. Choose **Next**.
5. On the **Add permissions** page, choose **Next**.
6. On the **Name, review, and create** page, do the following:
 - a. For **Role name**, enter a unique name for your role, such as **AmazonEKSFargatePodExecutionRole**.
 - b. Under **Add tags (Optional)**, add metadata to the role by attaching tags as key–value pairs. For more information about using tags in IAM, see [Tagging IAM Entities](#) in the *IAM User Guide*.
 - c. Choose **Create role**.
7. On the **Roles** page, search the list of roles for **AmazonEKSFargatePodExecutionRole**. Choose the role.
8. On the **AmazonEKSFargatePodExecutionRole** page, do the following:
 - a. Choose **Trust relationships**.
 - b. Choose **Edit trust policy**.
9. On the **Edit trust policy** page, do the following:
 - a. Copy and paste the following contents into the **Edit trust policy** form. Replace *region-code* with the AWS Region that your cluster is in. If you want to use the same role in all AWS Regions in your account, replace *region-code* with *. Replace *111122223333* with your account ID and *my-cluster* with the name of your cluster. If you want to use the same role for all clusters in your account, replace *my-cluster* with *.

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

```

        "ArnLike": {
            "aws:SourceArn": "arn:aws:eks:region-  

code:111122223333:fargateprofile/my-cluster/*"
        }
    },
    "Principal": {
        "Service": "eks-fargate-pods.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
}
]
}

```

- b. Choose **Update policy**.

AWS CLI

To create an AWS FargatePod execution role with the AWS CLI

1. Copy and paste the following contents to a file named *pod-execution-role-trust-policy.json*. Replace *region-code* with the AWS Region that your cluster is in. If you want to use the same role in all AWS Regions in your account, replace *region-code* with *. Replace *111122223333* with your account ID and *my-cluster* with the name of your cluster. If you want to use the same role for all clusters in your account, replace *my-cluster* with *.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:eks:region-  

code:111122223333:fargateprofile/my-cluster/*"
                }
            },
            "Principal": {
                "Service": "eks-fargate-pods.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. Create a Pod execution IAM role.

```
aws iam create-role \
--role-name AmazonEKSFargatePodExecutionRole \
--assume-role-policy-document file:///"pod-execution-role-trust-policy.json"
```

3. Attach the required Amazon EKS managed IAM policy to the role.

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy \
--role-name AmazonEKSFargatePodExecutionRole
```

Amazon EKS connector IAM role

You can connect Kubernetes clusters to view them in your AWS Management Console. To connect to a Kubernetes cluster, create an IAM role.

Check for an existing EKS connector role

You can use the following procedure to check and see if your account already has the Amazon EKS connector role.

To check for the `AmazonEKSConnectorAgentRole` in the IAM console

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the left navigation pane, choose **Roles**.
3. Search the list of roles for `AmazonEKSConnectorAgentRole`. If a role that includes `AmazonEKSConnectorAgentRole` doesn't exist, then see [Creating the Amazon EKS connector agent role \(p. 508\)](#) to create the role. If a role that includes `AmazonEKSConnectorAgentRole` does exist, then select the role to view the attached policies.
4. Choose **Permissions**.
5. Ensure that the **AmazonEKSConnectorAgentPolicy** managed policy is attached to the role. If the policy is attached, your Amazon EKS connector role is properly configured.
6. Choose **Trust relationships**, and then choose **Edit trust policy**.
7. Verify that the trust relationship contains the following policy. If the trust relationship matches the following policy, choose **Cancel**. If the trust relationship doesn't match, copy the policy into the **Edit trust policy** window and choose **Update policy**.

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

Creating the Amazon EKS connector agent role

You can use the AWS Management Console or AWS CloudFormation to create the connector agent role.

AWS CLI

1. Create a file named `eks-connector-agent-trust-policy.json` that contains the following JSON to use for the IAM role.

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

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

2. Create a file named `eks-connector-agent-policy.json` that contains the following JSON to use for the IAM role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SsmControlChannel",
            "Effect": "Allow",
            "Action": [
                "ssmmessages:CreateControlChannel"
            ],
            "Resource": "arn:aws:eks:*:*:cluster/*"
        },
        {
            "Sid": "ssmDataplaneOperations",
            "Effect": "Allow",
            "Action": [
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenDataChannel",
                "ssmmessages:OpenControlChannel"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Create the Amazon EKS Connector agent role using the trust policy and policy you created in the previous list items.

```
aws iam create-role \
--role-name AmazonEKSConnectorAgentRole \
--assume-role-policy-document file://eks-connector-agent-trust-policy.json
```

4. Attach the policy to your Amazon EKS Connector agent role.

```
aws iam put-role-policy \
--role-name AmazonEKSConnectorAgentRole \
--policy-name AmazonEKSConnectorAgentPolicy \
--policy-document file://eks-connector-agent-policy.json
```

AWS CloudFormation

To create your Amazon EKS connector agent role with AWS CloudFormation.

1. Save the following AWS CloudFormation template to a text file on your local system.

Note

This template also creates the service-linked role that would otherwise be created when the `registerCluster` API is called. See [Using roles to connect a Kubernetes cluster to Amazon EKS \(p. 496\)](#) for details.

```
---
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Provisions necessary resources needed to register clusters in EKS'
Parameters: {}
Resources:
  EKSConnectorSLR:
    Type: AWS::IAM::ServiceLinkedRole
    Properties:
      AWSServiceName: eks-connector.amazonaws.com

  EKSConnectorAgentRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Action: [ 'sts:AssumeRole' ]
            Principal:
              Service: 'ssm.amazonaws.com'

  EKSConnectorAgentPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyName: EKSConnectorAgentPolicy
      Roles:
        - {Ref: 'EKSConnectorAgentRole'}
      PolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: 'Allow'
            Action: [ 'ssmmessages:CreateControlChannel' ]
            Resource:
              - Fn::Sub: 'arn:${AWS::Partition}:eks:/*:cluster/*'
          - Effect: 'Allow'
            Action: [ 'ssmmessages:CreateDataChannel', 'ssmmessages:OpenDataChannel',
              'ssmmessages:OpenControlChannel' ]
            Resource: "*"
Outputs:
  EKSConnectorAgentRoleArn:
    Description: The agent role that EKS connector uses to communicate with AWS services.
    Value: !GetAtt EKSConnectorAgentRole.Arn
```

2. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
3. Choose **Create stack** (either with new resources or existing resources).
4. For **Specify template**, select **Upload a template file**, and then choose **Choose file**.
5. Choose the file you created earlier, and then choose **Next**.
6. For **Stack name**, enter a name for your role, such as `eksConnectorAgentRole`, and then choose **Next**.
7. On the **Configure stack options** page, choose **Next**.
8. On the **Review** page, review your information, acknowledge that the stack might create IAM resources, and then choose **Create stack**.

AWS managed policies for Amazon Elastic Kubernetes Service

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 **ReadOnlyAccess** AWS managed policy provides read-only access to all 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*.

AWS managed policy: AmazonEKS_CNI_Policy

You can attach the AmazonEKS_CNI_Policy to your IAM entities. Before you create an Amazon EC2 node group, this policy must be attached to either the [node IAM role \(p. 501\)](#), or to an IAM role that's used specifically by the Amazon VPC CNI plugin for Kubernetes. This is so that it can perform actions on your behalf. We recommend that you attach the policy to a role that's used only by the plugin. For more information, see [the section called "Amazon VPC CNI plugin for Kubernetes" \(p. 266\)](#) and [the section called "Configure plugin for IAM account" \(p. 272\)](#).

Permissions details

This policy includes the following permissions that allow Amazon EKS to complete the following tasks:

- **ec2** – Allows the Amazon VPC CNI plugin to perform actions such as provisioning Elastic Network Interfaces and IP addresses for Pods to provide networking for applications that run in Amazon EKS.

To view the latest version of the JSON policy document, see [AmazonEKS_CNI_Policy](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: AmazonEKSClusterPolicy

You can attach AmazonEKSClusterPolicy to your IAM entities. Before creating a cluster, you must have a [cluster IAM role \(p. 499\)](#) with this policy attached. Kubernetes clusters that are managed by Amazon EKS make calls to other AWS services on your behalf. They do this to manage the resources that you use with the service.

This policy includes the following permissions that allow Amazon EKS to complete the following tasks:

- **autoscaling** – Read and update the configuration of an Auto Scaling group. These permissions aren't used by Amazon EKS but remain in the policy for backwards compatibility.
- **ec2** – Work with volumes and network resources that are associated to Amazon EC2 nodes. This is required so that the Kubernetes control plane can join instances to a cluster and dynamically provision and manage Amazon EBS volumes that are requested by Kubernetes persistent volumes.
- **elasticloadbalancing** – Work with Elastic Load Balancers and add nodes to them as targets. This is required so that the Kubernetes control plane can dynamically provision Elastic Load Balancers requested by Kubernetes services.
- **iam** – Create a service-linked role. This is required so that the Kubernetes control plane can dynamically provision Elastic Load Balancers that are requested by Kubernetes services.

- **kms** – Read a key from AWS KMS. This is required for the Kubernetes control plane to support [secrets encryption](#) of Kubernetes secrets stored in etcd.

To view the latest version of the JSON policy document, see [AmazonEKSClusterPolicy](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: [AmazonEKSFargatePodExecutionRolePolicy](#)

You can attach [AmazonEKSFargatePodExecutionRolePolicy](#) to your IAM entities. Before you can create a Fargate profile, you must create a Fargate Pod execution role and attach this policy to it. For more information, see [Create a Fargate Pod execution role \(p. 133\)](#) and [AWS Fargate profile \(p. 136\)](#).

This policy grants the role the permissions that provide access to other AWS service resources that are required to run Amazon EKS Pods on Fargate.

Permissions details

This policy includes the following permissions that allow Amazon EKS to complete the following tasks:

- **ecr** – Allows Pods that are running on Fargate to pull container images that are stored in Amazon ECR.

To view the latest version of the JSON policy document, see [AmazonEKSFargatePodExecutionRolePolicy](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: [AmazonEKSForFargateServiceRolePolicy](#)

You can't attach [AmazonEKSForFargateServiceRolePolicy](#) to your IAM entities. This policy is attached to a service-linked role that allows Amazon EKS to perform actions on your behalf. For more information, see [AWS Service Role for Amazon EKS for Fargate](#).

This policy grants necessary permissions to Amazon EKS to run Fargate tasks. The policy is only used if you have Fargate nodes.

Permissions details

This policy includes the following permissions that allow Amazon EKS to complete the following tasks.

- **ec2** – Create and delete Elastic Network Interfaces and describe Elastic Network Interfaces and resources. This is required so that the Amazon EKS Fargate service can configure the VPC networking that's required for Fargate Pods.

To view the latest version of the JSON policy document, see [AmazonEKSForFargateServiceRolePolicy](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: [AmazonEKSServicePolicy](#)

You can attach [AmazonEKSServicePolicy](#) to your IAM entities. Clusters that were created before April 16, 2020, required you to create an IAM role and attach this policy to it. Clusters that were created on or after April 16, 2020, don't require you to create a role and don't require you to assign this policy. When you create a cluster using an IAM principal that has the `iam:CreateServiceLinkedRole` permission, the [AWS Service Role for Amazon EKS \(p. 491\)](#) service-linked role is automatically created for you. The service-linked role has the [AWS managed policy: AmazonEKSServiceRolePolicy \(p. 513\)](#) attached to it.

This policy allows Amazon EKS to create and manage the necessary resources to operate Amazon EKS clusters.

Permissions details

This policy includes the following permissions that allow Amazon EKS to complete the following tasks.

- **eks** – Update the Kubernetes version of your cluster after you initiate an update. This permission isn't used by Amazon EKS but remains in the policy for backwards compatibility.
- **ec2** – Work with Elastic Network Interfaces and other network resources and tags. This is required by Amazon EKS to configure networking that facilitates communication between nodes and the Kubernetes control plane.
- **route53** – Associate a VPC with a hosted zone. This is required by Amazon EKS to enable private endpoint networking for your Kubernetes cluster API server.
- **logs** – Log events. This is required so that Amazon EKS can ship Kubernetes control plane logs to CloudWatch.
- **iam** – Create a service-linked role. This is required so that Amazon EKS can create the [AWSServiceRoleForAmazonEKS \(p. 491\)](#) service-linked role on your behalf.

To view the latest version of the JSON policy document, see [AmazonEKSServicePolicy](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: AmazonEKSServiceRolePolicy

You can't attach AmazonEKSServiceRolePolicy to your IAM entities. This policy is attached to a service-linked role that allows Amazon EKS to perform actions on your behalf. For more information, see [Service-linked role permissions for Amazon EKS \(p. 491\)](#). When you create a cluster using an IAM principal that has the `iam:CreateServiceLinkedRole` permission, the [AWSServiceRoleforAmazonEKS \(p. 491\)](#) service-linked role is automatically created for you and this policy is attached to it.

This policy allows the service-linked role to call AWS services on your behalf.

Permissions details

This policy includes the following permissions that allow Amazon EKS to complete the following tasks.

- **ec2** – Create and describe Elastic Network Interfaces and Amazon EC2 instances, the [cluster security group \(p. 263\)](#), and VPC that are required to create a cluster.
- **iam** – List all of the managed policies that attached to an IAM role. This is required so that Amazon EKS can list and validate all managed policies and permissions required to create a cluster.
- **Associate a VPC with a hosted zone** – This is required by Amazon EKS to enable private endpoint networking for your Kubernetes cluster API server.
- **Log event** – This is required so that Amazon EKS can ship Kubernetes control plane logs to CloudWatch.

To view the latest version of the JSON policy document, see [AmazonEKSServiceRolePolicy](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: AmazonEKSVPCCResourceController

You can attach the AmazonEKSVPCCResourceController policy to your IAM identities. If you're using [security groups for Pods \(p. 324\)](#), you must attach this policy to your [Amazon EKS cluster IAM role \(p. 499\)](#) to perform actions on your behalf.

This policy grants the cluster role permissions to manage Elastic Network Interfaces and IP addresses for nodes.

Permissions details

This policy includes the following permissions that allow Amazon EKS to complete the following tasks:

- **ec2** – Manage Elastic Network Interfaces and IP addresses to support Pod security groups and Windows nodes.

To view the latest version of the JSON policy document, see [AmazonEKSVPCResourceController](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: AmazonEKSWorkerNodePolicy

You can attach the AmazonEKSWorkerNodePolicy to your IAM entities. You must attach this policy to a [node IAM role \(p. 501\)](#) that you specify when you create Amazon EC2 nodes that allow Amazon EKS to perform actions on your behalf. If you create a node group using eksctl, it creates the node IAM role and attaches this policy to the role automatically.

This policy grants Amazon EKS Amazon EC2 nodes permissions to connect to Amazon EKS clusters.

Permissions details

This policy includes the following permissions that allow Amazon EKS to complete the following tasks:

- **ec2** – Read instance volume and network information. This is required so that Kubernetes nodes can describe information about Amazon EC2 resources that are required for the node to join the Amazon EKS cluster.
- **eks** – Optionally describe the cluster as part of node bootstrapping.

To view the latest version of the JSON policy document, see [AmazonEKSWorkerNodePolicy](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: AWSServiceRoleForAmazonEKSNodegroup

You can't attach AWSServiceRoleForAmazonEKSNodegroup to your IAM entities. This policy is attached to a service-linked role that allows Amazon EKS to perform actions on your behalf. For more information, see [Service-linked role permissions for Amazon EKS \(p. 492\)](#).

This policy grants the AWSServiceRoleForAmazonEKSNodegroup role permissions that allow it to create and manage Amazon EC2 node groups in your account.

Permissions details

This policy includes the following permissions that allow Amazon EKS to complete the following tasks:

- **ec2** – Work with security groups, tags, and launch templates. This is required for Amazon EKS managed node groups to enable remote access configuration. Additionally, Amazon EKS managed node groups create a launch template on your behalf. This is to configure the Amazon EC2 Auto Scaling group that backs each managed node group.
- **iam** – Create a service-linked role and pass a role. This is required by Amazon EKS managed node groups to manage instance profiles for the role being passed when creating a managed node group. This instance profile is used by Amazon EC2 instances launched as part of a managed node group. Amazon EKS needs to create service-linked roles for other services such as Amazon EC2 Auto Scaling groups. These permissions are used in the creation of a managed node group.
- **autoscaling** – Work with security Auto Scaling groups. This is required by Amazon EKS managed node groups to manage the Amazon EC2 Auto Scaling group that backs each managed node group. It's

also used to support functionality such as evicting Pods when nodes are terminated or recycled during node group updates.

To view the latest version of the JSON policy document, see [AWS Service Role for Amazon EKS Nodegroup](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: AmazonEBSCSIDriverPolicy

The AmazonEBSCSIDriverPolicy policy allows the Amazon EBS Container Storage Interface (CSI) driver to create, modify, attach, detach, and delete volumes on your behalf. It also grants the EBS CSI driver permissions to create and delete snapshots, and to list your instances, volumes, and snapshots.

To view the latest version of the JSON policy document, see [AmazonEBSCSIDriverServiceRolePolicy](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: AmazonEFSCSIDriverPolicy

The AmazonEFSCSIDriverPolicy policy allows the Amazon EFS Container Storage Interface (CSI) to create and delete access points on your behalf. It also grants the Amazon EFS CSI driver permissions to list your access points file systems, mount targets, and Amazon EC2 availability zones.

To view the latest version of the JSON policy document, see [AmazonEFSCSIDriverServiceRolePolicy](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: AmazonEKSLocalOutpostClusterPolicy

You can attach this policy to IAM entities. Before creating a local cluster, you must attach this policy to your [cluster role \(p. 499\)](#). Kubernetes clusters that are managed by Amazon EKS make calls to other AWS services on your behalf. They do this to manage the resources that you use with the service.

The AmazonEKSLocalOutpostClusterPolicy includes the following permissions:

- **ec2** – Required permissions for Amazon EC2 instances to successfully join the cluster as control plane instances.
- **ssm** – Allows Amazon EC2 Systems Manager connection to the control plane instance, which is used by Amazon EKS to communicate and manage the local cluster in your account.
- **logs** – Allows instances to push logs to Amazon CloudWatch.
- **secretsmanager** – Allows instances to get and delete bootstrap data for the control plane instances securely from AWS Secrets Manager.
- **ecr** – Allows Pods and containers that are running on the control plane instances to pull container images that are stored in Amazon Elastic Container Registry.

To view the latest version of the JSON policy document, see [AmazonEKSLocalOutpostClusterPolicy](#) in the AWS Managed Policy Reference Guide.

AWS managed policy: AmazonEKSLocalOutpostServiceRolePolicy

You can't attach this policy to your IAM entities. When you create a cluster using an IAM principal that has the `iam:CreateServiceLinkedRole` permission, Amazon EKS automatically creates the [AWS Service Role for Amazon EKS Local Outpost \(p. 497\)](#) service-linked role for you and attaches this policy to it. This policy allows the service-linked role to call AWS services on your behalf for local clusters.

The AmazonEKSLocalOutpostServiceRolePolicy includes the following permissions:

- **ec2** – Allows Amazon EKS to work with security, network, and other resources to successfully launch and manage control plane instances in your account.
- **ssm** – Allows Amazon EC2 Systems Manager connection to the control plane instances, which is used by Amazon EKS to communicate and manage the local cluster in your account.
- **iam** – Allows Amazon EKS to manage the instance profile associated with the control plane instances.
- **secretsmanager** – Allows Amazon EKS to put bootstrap data for the control plane instances into AWS Secrets Manager so it can be securely referenced during instance bootstrapping.
- **outposts** – Allows Amazon EKS to get Outpost information from your account to successfully launch a local cluster in an Outpost.

To view the latest version of the JSON policy document, see [AmazonEKSLocalOutpostServiceRolePolicy](#) in the AWS Managed Policy Reference Guide.

Amazon EKS updates to AWS managed policies

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

Change	Description	Date
Introduced AmazonEFSCSIDriverPolicy	AWS introduced the AmazonEFSCSIDriverPolicy .	July 26, 2023
Added permissions to AmazonEKSClusterPolicy	Added DescribeAvailabilityZones permission to allow Amazon EKS to get the AZ details during subnet auto-discovery while creating load balancers.	February 7, 2023
Updated policy conditions in AmazonEBSCSIDriverPolicy	Removed invalid policy conditions with wildcard characters in the StringLike key field5 . Also added a new condition <code>ec2:ResourceTag/kubernetes.io/created-for/pvc/name: "*"</code> to <code>ec2:DeleteVolume</code> , which allows the EBS CSI driver to delete volumes created by the in-tree plugin.	November 17, 2022
Added permissions to AmazonEKSLocalOutpostServiceRolePolicy	Added <code>ec2:DescribeVPCAttribute</code> , <code>ec2:DescribeConsoleOutput</code> and <code>ec2:DescribeSecret</code> to allow better prerequisite validation and managed lifecycle control. Also added <code>ec2:DescribePlacementGroups</code> and <code>"arn:aws:ec2:*:*:placement-group/*"</code> to <code>ec2:RunInstances</code> to support placement control of the control plane Amazon EC2 instances on Outposts.	October 24, 2022
Update Amazon Elastic Container	Moved action <code>ecr:GetDownloadUrlForLayer</code>	October 20, 2022

Change	Description	Date
Registry permissions in AmazonEKSLocalOutpostInstancePolicy(p* 515)	from all resource sections to a scoped section. Added resource <code>arn:aws:iam::aws:policy/eks/*</code> . Removed resource <code>arn:aws:ecr:*::repository/eks-certificates-controller-public</code> . This resource is covered by the added <code>arn:aws:ecr:*::repository/eks/*</code> resource.	
Added permissions to AmazonEKSLocalOutpostInstancePolicy(p* 515)	Added the <code>arn:aws:iam::aws:policy/eks-kubelet-config-updater</code> Amazon Elastic Container Registry repository so the cluster control plane instances can update some kubelet arguments.	August 31, 2022
Introduced AmazonEKSLocalOutpostClusterPolicy(p* 105)	AWS introduced the <code>AmazonEKSLocalOutpostClusterPolicy</code> .	August 24, 2022
Introduced AmazonEKSLocalOutpostServiceRolePolicy(p* 105)	AWS introduced the <code>AmazonEKSLocalOutpostServiceRolePolicy</code> .	August 23, 2022
Introduced AmazonEBSCSIDriverPolicy(p* 515)	AWS introduced the <code>AmazonEBSCSIDriverPolicy</code> .	April 4, 2022
Added permissions to AmazonEKSWorkerNodePolicy(p* 514)	Added <code>ec2:DescribeInstanceTypes</code> to enable Amazon EKS-optimized AMIs that can auto discover instance level properties.	March 21, 2022
Added permissions to AWSServiceRoleForAmazonEKSNetworking(p* 101)	Added <code>ec2:EnableMetricsCollection</code> permission to allow Amazon EKS to enable metrics collection.	December 13, 2021
Added permissions to AmazonEKSClusterPolicy(p* 25D)	Added <code>ec2:DescribeAccountAttributes</code> , <code>ec2:DescribeAddresses</code> , and <code>ec2:DescribeInternetGateways</code> permissions to allow Amazon EKS to create a service-linked role for a Network Load Balancer.	June 17, 2021
Amazon EKS started tracking changes.	Amazon EKS started tracking changes for its AWS managed policies.	June 17, 2021

Troubleshooting IAM

This topic covers some common errors that you may see while using Amazon EKS with IAM and how to work around them.

AccessDeniedException

If you receive an `AccessDeniedException` when calling an AWS API operation, then the [IAM principal](#) credentials that you're using don't have the required permissions to make that call.

An error occurred (AccessDeniedException) when calling the `DescribeCluster` operation:
User: arn:aws:iam::111122223333:user/`user_name` is not authorized to perform:
`eks:DescribeCluster` on resource: arn:aws:eks:`region:111122223333:cluster/my-cluster`

In the previous example message, the user does not have permissions to call the Amazon EKS `DescribeCluster` API operation. To provide Amazon EKS admin permissions to an IAM principal, see [Amazon EKS identity-based policy examples \(p. 485\)](#).

For more general information about IAM, see [Controlling access using policies](#) in the *IAM User Guide*.

Can't see Nodes on the Compute tab or anything on the Resources tab and you receive an error in the AWS Management Console

You may see a console error message that says Your current user or role does not have access to Kubernetes objects on this EKS cluster. Make sure that the [IAM principal](#) user that you're using the AWS Management Console with has the necessary permissions. For more information, see [Required permissions \(p. 529\)](#).

aws-auth ConfigMap does not grant access to the cluster

[AWS IAM Authenticator](#) does not permit a path in the role ARN used in the ConfigMap.

Therefore, before you specify `rolearn`, remove the path. For example, change

arn:aws:iam::111122223333:role/`team/developers/eks-admin` to

arn:aws:iam::111122223333:role/`eks-admin`.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Amazon EKS.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Amazon EKS. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

User: arn:aws:iam::123456789012:user/`marymajor` is not authorized to perform: `iam:PassRole`

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my Amazon EKS resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon EKS supports these features, see [How Amazon EKS works with IAM \(p. 482\)](#).
- To learn how to provide access to your resources across AWS accounts that you own, see [Providing access to an IAM user in another AWS account that you own](#) in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see [Providing access to AWS accounts owned by third parties](#) in the *IAM User Guide*.
- To learn how to provide access through identity federation, see [Providing access to externally authenticated users \(identity federation\)](#) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.

Pod containers receive the following error: An error occurred (SignatureDoesNotMatch) when calling the GetCallerIdentity operation: Credential should be scoped to a valid region

Your containers receive this error if your application is explicitly making requests to the AWS STS global endpoint (<https://sts.amazonaws>) and your Kubernetes service account is configured to use a regional endpoint. You can resolve the issue with one of the following options:

- Update your application code to remove explicit calls to the AWS STS global endpoint.
- Update your application code to make explicit calls to regional endpoints such as <https://sts.us-west-2.amazonaws.com>. Your application should have redundancy built in to pick a different AWS Region in the event of a failure of the service in the AWS Region. For more information, see [Managing AWS STS in an AWS Region](#) in the *IAM User Guide*.
- Configure your service accounts to use the global endpoint. All versions earlier than 1.22 used the global endpoint by default, but version 1.22 and later clusters use the regional endpoint by default. For more information, see [Configuring the AWS Security Token Service endpoint for a service account \(p. 474\)](#).

Compliance validation for Amazon Elastic Kubernetes Service

To learn whether an AWS service is within the scope of specific compliance programs, see [AWS services in Scope by Compliance Program](#) and choose the compliance program that you are interested in. For general information, see [AWS Compliance Programs](#).

You can download third-party audit reports using AWS Artifact. For more information, see [Downloading Reports in AWS Artifact](#).

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- [Security and Compliance Quick Start Guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

Note

Not all AWS services are HIPAA eligible. For more information, see the [HIPAA Eligible Services Reference](#).

- [AWS Compliance Resources](#) – This collection of workbooks and guides might apply to your industry and location.
- [Evaluating Resources with Rules](#) in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- [AWS Security Hub](#) – This AWS service provides a comprehensive view of your security state within AWS. Security Hub uses security controls to evaluate your AWS resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see [Security Hub controls reference](#).
- [AWS Audit Manager](#) – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Resilience in Amazon EKS

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between Availability Zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

Amazon EKS runs and scales the Kubernetes control plane across multiple AWS Availability Zones to ensure high availability. Amazon EKS automatically scales control plane instances based on load, detects and replaces unhealthy control plane instances, and automatically patches the control plane. After you initiate a version update, Amazon EKS updates your control plane for you, maintaining high availability of the control plane during the update.

This control plane consists of at least two API server instances and three etcd instances that run across three Availability Zones within an AWS Region. Amazon EKS:

- Actively monitors the load on control plane instances and automatically scales them to ensure high performance.
- Automatically detects and replaces unhealthy control plane instances, restarting them across the Availability Zones within the AWS Region as needed.
- Leverages the architecture of AWS Regions in order to maintain high availability. Because of this, Amazon EKS is able to offer an [SLA for API server endpoint availability](#).

For more information about AWS Regions and Availability Zones, see [AWS global infrastructure](#).

Infrastructure security in Amazon EKS

As a managed service, Amazon Elastic Kubernetes Service is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see [AWS Cloud Security](#). To design your AWS environment using the best practices for infrastructure security, see [Infrastructure Protection](#) in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access Amazon EKS through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the [AWS Security Token Service](#) (AWS STS) to generate temporary security credentials to sign requests.

When you create an Amazon EKS cluster, you specify the VPC subnets for your cluster to use. Amazon EKS requires subnets in at least two Availability Zones. We recommend a VPC with public and private subnets so that Kubernetes can create public load balancers in the public subnets that load balance traffic to Pods running on nodes that are in private subnets.

For more information about VPC considerations, see [Amazon EKS VPC and subnet requirements and considerations \(p. 256\)](#).

If you create your VPC and node groups with the AWS CloudFormation templates provided in the [Getting started with Amazon EKS \(p. 6\)](#) walkthrough, then your control plane and node security groups are configured with our recommended settings.

For more information about security group considerations, see [Amazon EKS security group requirements and considerations \(p. 263\)](#).

When you create a new cluster, Amazon EKS creates an endpoint for the managed Kubernetes API server that you use to communicate with your cluster (using Kubernetes management tools such as `kubectl`). By default, this API server endpoint is public to the internet, and access to the API server is secured using a combination of AWS Identity and Access Management (IAM) and native Kubernetes [Role Based Access Control](#) (RBAC).

You can enable private access to the Kubernetes API server so that all communication between your nodes and the API server stays within your VPC. You can limit the IP addresses that can access your API server from the internet, or completely disable internet access to the API server.

For more information about modifying cluster endpoint access, see [Modifying cluster endpoint access \(p. 42\)](#).

You can implement Kubernetes *network policies* with the Amazon VPC CNI or third-party tools such as [Project Calico \(p. 350\)](#). For more information about using the Amazon VPC CNI for network policies, see [Configure your cluster for Kubernetes network policies \(p. 290\)](#). Project Calico is a third party open source project. For more information, see the [Project Calico documentation](#).

Configuration and vulnerability analysis in Amazon EKS

Security is a critical consideration for configuring and maintaining Kubernetes clusters and applications. The [Center for Internet Security \(CIS\) Kubernetes Benchmark](#) provides guidance for Amazon EKS node security configurations. The benchmark:

- Is applicable to Amazon EC2 nodes (both managed and self-managed) where you are responsible for security configurations of Kubernetes components.
- Provides a standard, community-approved way to ensure that you have configured your Kubernetes cluster and nodes securely when using Amazon EKS.

- Consists of four sections; control plane logging configuration, node security configurations, policies, and managed services.
- Supports all of the Kubernetes versions currently available in Amazon EKS and can be run using [kube-bench](#), a standard open source tool for checking configuration using the CIS benchmark on Kubernetes clusters.

To learn more, see [Introducing The CIS Amazon EKS Benchmark](#).

Amazon EKS platform versions represent the capabilities of the cluster control plane, including which Kubernetes API server flags are enabled and the current Kubernetes patch version. New clusters are deployed with the latest platform version. For details, see [Amazon EKS platform versions \(p. 71\)](#).

You can [update an Amazon EKS cluster \(p. 34\)](#) to newer Kubernetes versions. As new Kubernetes versions become available in Amazon EKS, we recommend that you proactively update your clusters to use the latest available version. For more information about Kubernetes versions in EKS, see [Amazon EKS Kubernetes versions \(p. 60\)](#).

Track security or privacy events for Amazon Linux 2 at the [Amazon Linux Security Center](#) or subscribe to the associated [RSS feed](#). Security and privacy events include an overview of the issue affected, packages, and instructions for updating your instances to correct the issue.

You can use [Amazon Inspector](#) to check for unintended network accessibility of your nodes and for vulnerabilities on those Amazon EC2 instances.

Security best practices for Amazon EKS

Amazon EKS security best practices are maintained on Github: <https://aws.github.io/aws-eks-best-practices/security/docs/>

Pod security policy

The Kubernetes Pod security policy admission controller validates Pod creation and update requests against a set of rules. By default, Amazon EKS clusters ship with a fully permissive security policy with no restrictions. For more information, see [Pod Security Policies](#) in the Kubernetes documentation.

Note

The PodSecurityPolicy (PSP) was deprecated in Kubernetes version 1.21 and removed in Kubernetes 1.25. PSPs are being replaced with [Pod Security Admission \(PSA\)](#), a built-in admission controller that implements the security controls outlined in the [Pod Security Standards \(PSS\)](#). PSA and PSS have both reached beta feature states, and are enabled in Amazon EKS by default. To address PSP removal in 1.25, we recommend that you implement PSS in Amazon EKS. For more information, see [Implementing Pod Security Standards in Amazon EKS](#) on the AWS blog.

Amazon EKS default Pod security policy

Amazon EKS clusters with Kubernetes version 1.13 or higher have a default Pod security policy named `eks.privileged`. This policy has no restriction on what kind of Pod can be accepted into the system, which is equivalent to running Kubernetes with the `PodSecurityPolicy` controller disabled.

Note

This policy was created to maintain backwards compatibility with clusters that did not have the `PodSecurityPolicy` controller enabled. You can create more restrictive policies for your

cluster and for individual namespaces and service accounts and then delete the default policy to enable the more restrictive policies.

You can view the default policy with the following command.

```
kubectl get psp eks.privileged
```

An example output is as follows.

NAME	PRIV	CAPS	SELINUX	RUNASUSER	FSGROUP	SUPGROUP	READONLYROOTFS
VOLUMES							
eks.privileged	true	*	RunAsAny	RunAsAny	RunAsAny	RunAsAny	false

For more details, you can describe the policy with the following command.

```
kubectl describe psp eks.privileged
```

An example output is as follows.

```
Name: eks.privileged

Settings:
  Allow Privileged: true
  Allow Privilege Escalation: 0xc0004ce5f8
  Default Add Capabilities: <none>
  Required Drop Capabilities: <none>
  Allowed Capabilities: *
  Allowed Volume Types: *
  Allow Host Network: true
  Allow Host Ports: 0-65535
  Allow Host PID: true
  Allow Host IPC: true
  Read Only Root Filesystem: false
  SELinux Context Strategy: RunAsAny
    User: <none>
    Role: <none>
    Type: <none>
    Level: <none>
  Run As User Strategy: RunAsAny
    Ranges: <none>
  FSGroup Strategy: RunAsAny
    Ranges: <none>
  Supplemental Groups Strategy: RunAsAny
    Ranges: <none>
```

You can view the full YAML file for the eks.privileged Pod security policy, its cluster role, and cluster role binding in [Install or restore the default Pod security policy \(p. 524\)](#).

Delete the default Amazon EKS Pod security policy

If you create more restrictive policies for your Pods, then after doing so, you can delete the default Amazon EKS eks.privileged Pod security policy to enable your custom policies.

Important

If you are using version 1.7.0 or later of the CNI plugin and you assign a custom Pod security policy to the aws-node Kubernetes service account used for the aws-node Pods deployed by

the Daemonset, then the policy must have NET_ADMIN in its allowedCapabilities section along with hostNetwork: true and privileged: true in the policy's spec.

To delete the default Pod security policy

1. Create a file named *privileged-podsecuritypolicy.yaml* with the contents in the example file in [Install or restore the default Pod security policy \(p. 524\)](#).
2. Delete the YAML with the following command. This deletes the default Pod security policy, the ClusterRole, and the ClusterRoleBinding associated with it.

```
kubectl delete -f privileged-podsecuritypolicy.yaml
```

Install or restore the default Pod security policy

If you are upgrading from an earlier version of Kubernetes, or have modified or deleted the default Amazon EKS eks.privileged Pod security policy, you can restore it with the following steps.

To install or restore the default Pod security policy

1. Create a file called *privileged-podsecuritypolicy.yaml* with the following contents.

```
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: eks.privileged
  annotations:
    kubernetes.io/description: 'privileged allows full unrestricted access to
      Pod features, as if the PodSecurityPolicy controller was not enabled.'
    seccomp.security.alpha.kubernetes.io/allowedProfileNames: '*'
  labels:
    kubernetes.io/cluster-service: "true"
    eks.amazonaws.com/component: pod-security-policy
spec:
  privileged: true
  allowPrivilegeEscalation: true
  allowedCapabilities:
  - '*'
  volumes:
  - '*'
  hostNetwork: true
  hostPorts:
  - min: 0
    max: 65535
  hostIPC: true
  hostPID: true
  runAsUser:
    rule: 'RunAsAny'
  seLinux:
    rule: 'RunAsAny'
  supplementalGroups:
    rule: 'RunAsAny'
  fsGroup:
    rule: 'RunAsAny'
  readOnlyRootFilesystem: false
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: eks:podsecuritypolicy:privileged
```

```
labels:
  kubernetes.io/cluster-service: "true"
  eks.amazonaws.com/component: pod-security-policy
rules:
- apiGroups:
  - policy
  resourceNames:
  - eks.privileged
  resources:
  - podsecuritypolicies
  verbs:
  - use

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: eks:podsecuritypolicy:authenticated
  annotations:
    kubernetes.io/description: 'Allow all authenticated users to create privileged Pods.'
  labels:
    kubernetes.io/cluster-service: "true"
    eks.amazonaws.com/component: pod-security-policy
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: eks:podsecuritypolicy:privileged
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: system:authenticated
```

2. Apply the YAML with the following command.

```
kubectl apply -f privileged-podsecuritypolicy.yaml
```

Pod security policy (PSP) removal FAQ

PodSecurityPolicy was [deprecated in Kubernetes 1.21](#), and has been removed in Kubernetes 1.25. If you are using PodSecurityPolicy in your cluster, **then you must migrate to the built-in Kubernetes Pod Security Standards (PSS) or to a policy-as-code solution before upgrading your cluster to version 1.25 to avoid interruptions to your workloads**. Select any frequently asked question to learn more.

What is a PSP?

[PodSecurityPolicy](#) is a built-in admission controller that allows a cluster administrator to control security-sensitive aspects of Pod specification. If a Pod meets the requirements of its PSP, the Pod is admitted to the cluster as usual. If a Pod doesn't meet the PSP requirements, the Pod is rejected and can't run.

Is the PSP removal specific to Amazon EKS or is it being removed in upstream Kubernetes?

This is an upstream change in the Kubernetes project, and not a change made in Amazon EKS. PSP was deprecated in Kubernetes 1.21 and removed in Kubernetes 1.25. The Kubernetes community identified serious usability problems with PSP. These included accidentally granting broader permissions than intended and difficulty in inspecting which PSPs apply in a given situation. These issues couldn't be

addressed without making breaking changes. This is the primary reason why the Kubernetes community [decided to remove PSP](#).

How can I check if I'm using PSPs in my Amazon EKS clusters?

To check if you're using PSPs in your cluster, you can run the following command:

```
kubectl get psp
```

To see the Pods that the PSPs in your cluster are impacting, run the following command. This command outputs the Pod name, namespace, and PSPs:

```
kubectl get pod -A -o jsonpath='{range.items[?(@.metadata.annotations.kubernetes\\.io/psp)]} {.metadata.name}{"\t"}{.metadata.namespace}{"\t"}{.metadata.annotations.kubernetes\\.io/psp}{"\n"}'
```

If I'm using PSPs in my Amazon EKS cluster, what can I do?

Before upgrading your cluster to 1.25, you must migrate your PSPs to either one of these alternatives:

- Kubernetes PSS.
- Policy-as-code solutions from the Kubernetes environment.

In response to the PSP deprecation and the ongoing need to control Pod security from the start, the Kubernetes community created a built-in solution with [\(PSS\)](#) and [Pod Security Admission \(PSA\)](#). The PSA webhook implements the controls that are defined in the PSS.

You can review best practices for migrating PSPs to the built-in PSS in the [EKS Best Practices Guide](#). We also recommend reviewing our blog on [Implementing Pod Security Standards in Amazon EKS](#). Additional references include [Migrate from PodSecurityPolicy to the Built-In PodSecurity Admission Controller](#) and [Mapping PodSecurityPolicies to Pod Security Standards](#).

Policy-as-code solutions provide guardrails to guide cluster users and prevents unwanted behaviors through prescribed automated controls. Policy-as-code solutions typically use [Kubernetes Dynamic Admission Controllers](#) to intercept the Kubernetes API server request flow using a webhook call. Policy-as-code solutions mutate and validate request payloads based on policies written and stored as code.

There are several open source policy-as-code solutions available for Kubernetes. To review best practices for migrating PSPs to a policy-as-code solution, see the [Policy-as-code](#) section of the Pod Security page on GitHub.

I see a PSP called eks.privileged in my cluster. What is it and what can I do about it?

Amazon EKS clusters with Kubernetes version 1.13 or higher have a default PSP that's named eks.privileged. This policy is created in 1.24 and earlier clusters. It isn't used in 1.25 and later clusters. Amazon EKS automatically migrates this PSP to a PSS-based enforcement. No action is needed on your part.

Will Amazon EKS make any changes to PSPs present in my existing cluster when I update my cluster to version 1.25?

No. Besides eks.privileged, which is a PSP created by Amazon EKS, no changes are made to other PSPs in your cluster when you upgrade to 1.25.

Will Amazon EKS prevent a cluster update to version 1.25 if I haven't migrated off of PSP?

No. Amazon EKS won't prevent a cluster update to version 1.25 if you didn't migrate off of PSP yet.

What if I forget to migrate my PSPs to PSS/PSA or to a policy-as-code solution before I update my cluster to version 1.25? Can I migrate after updating my cluster?

When a cluster that contains a PSP is upgraded to Kubernetes version 1.25, the API server doesn't recognize the PSP resource in 1.25. This might result in Pods getting incorrect security scopes. For an exhaustive list of implications, see [Migrate from PodSecurityPolicy to the Built-In PodSecurity Admission Controller](#).

How does this change impact pod security for Windows workloads?

We don't expect any specific impact to Windows workloads. PodSecurityContext has a field called `windowsOptions` in the `PodSpec v1` API for Windows Pods. This uses PSS in Kubernetes 1.25. For more information and best practices about enforcing PSS for Windows workloads, see the [EKS Best Practices Guide](#) and Kubernetes [documentation](#).

Using AWS Secrets Manager secrets with Kubernetes

To show secrets from Secrets Manager and parameters from Parameter Store as files mounted in Amazon EKS Pods, you can use the AWS Secrets and Configuration Provider (ASCP) for the [Kubernetes Secrets Store CSI Driver](#).

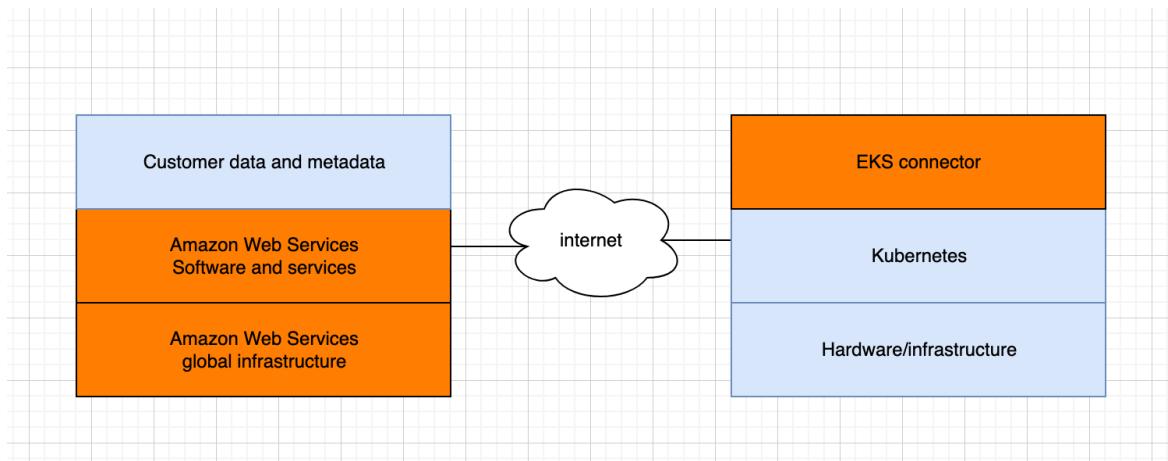
With the ASCP, you can store and manage your secrets in Secrets Manager and then retrieve them through your workloads running on Amazon EKS. You can use IAM roles and policies to limit access to your secrets to specific Kubernetes Pods in a cluster. The ASCP retrieves the Pod identity and exchanges the identity for an IAM role. ASCP assumes the IAM role of the Pod, and then it can retrieve secrets from Secrets Manager that are authorized for that role.

If you use Secrets Manager automatic rotation for your secrets, you can also use the Secrets Store CSI Driver rotation reconciler feature to ensure you are retrieving the latest secret from Secrets Manager.

For more information, see [Using Secrets Manager secrets in Amazon EKS](#) in the AWS Secrets Manager User Guide.

Amazon EKS Connector considerations

The Amazon EKS Connector is an open source component that runs on your Kubernetes cluster. This cluster can be located outside of the AWS environment. This creates additional considerations for security responsibilities. This configuration can be illustrated by the following diagram. Orange represents AWS responsibilities, and blue represents customer responsibilities:



This topic describes the differences in the responsibility model if the connected cluster is outside of AWS.

AWS responsibilities

- Maintaining, building, and delivering Amazon EKS Connector, which is an [open source component](#) that runs on a customer's Kubernetes cluster and communicates with AWS.
- Maintaining transport and application layer communication security between the connected Kubernetes cluster and AWS services.

Customer responsibilities

- Kubernetes cluster specific security, specifically along the following lines:
 - Kubernetes secrets must be properly encrypted and protected.
 - Lock down access to the `eks-connector` namespace.
- Configuring role-based access control (RBAC) permissions to manage [IAM principal](#) access from AWS. For instructions, see [the section called "Granting access to an IAM principal to view Kubernetes resources on a cluster" \(p. 579\)](#).
- Installing and upgrading Amazon EKS Connector.
- Maintaining the hardware, software, and infrastructure that supports the connected Kubernetes cluster.
- Securing their AWS accounts (for example, through safeguarding your [root user credentials](#)).

View Kubernetes resources

You can view the Kubernetes resources deployed to your cluster with the AWS Management Console. You can't view Kubernetes resources with the AWS CLI or [eksctl \(p. 13\)](#). To view Kubernetes resources using a command-line tool, use [kubectl \(p. 6\)](#).

Prerequisite

To view the **Resources** tab and **Nodes** section on the **Compute** tab in the AWS Management Console, the [IAM principal](#) that you're using must have specific IAM and Kubernetes permissions. For more information, see [Required permissions \(p. 529\)](#).

To view Kubernetes resources with the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the **Clusters** list, select the cluster that contains the Kubernetes resources that you want to view.
3. Select the **Resources** tab.
4. Select a **Resource type** group that you want to view resources for, such as **Workloads**. You see a list of resource types in that group.
5. Select a resource type, such as **Deployments**, in the **Workloads** group. You see a description of the resource type, a link to the Kubernetes documentation for more information about the resource type, and a list of resources of that type that are deployed on your cluster. If the list is empty, then there are no resources of that type deployed to your cluster.
6. Select a resource to view more information about it. Try the following examples:
 - Select the **Workloads** group, select the **Deployments** resource type, and then select the **coredns** resource. When you select a resource, you are in **Structured view**, by default. For some resource types, you see a **Pods** section in **Structured view**. This section lists the Pods managed by the workload. You can select any Pod listed to view information about the Pod. Not all resource types display information in **Structured View**. If you select **Raw view** in the top right corner of the page for the resource, you see the complete JSON response from the Kubernetes API for the resource.
 - Select the **Cluster** group and then select the **Nodes** resource type. You see a list of all nodes in your cluster. The nodes can be any [Amazon EKS node type \(p. 77\)](#). This is the same list that you see in the **Nodes** section when you select the **Compute** tab for your cluster. Select a node resource from the list. In **Structured view**, you also see a **Pods** section. This section shows you all Pods running on the node.

Required permissions

To view the **Resources** tab and **Nodes** section on the **Compute** tab in the AWS Management Console, the [IAM principal](#) that you're using must have specific minimum IAM and Kubernetes permissions. Complete the following steps to assign the required permissions to your IAM principals.

1. Make sure that the `eks : AccessKubernetesApi`, and other necessary IAM permissions to view Kubernetes resources, are assigned to the IAM principal that you're using. For more information about how to edit permissions for an IAM principal, see [Controlling access for principals](#) in the IAM User Guide. For more information about how to edit permissions for a role, see [Modifying a role permissions policy \(console\)](#) in the IAM User Guide.

The following example policy includes the necessary permissions for a principal to view Kubernetes resources for all clusters in your account. Replace `111122223333` with your AWS account ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "eks>ListFargateProfiles",
                "eks>DescribeNodegroup",
                "eks>ListNodegroups",
                "eks>ListUpdates",
                "eks>AccessKubernetesApi",
                "eks>ListAddons",
                "eks>DescribeCluster",
                "eks>DescribeAddonVersions",
                "eks>ListClusters",
                "eks>ListIdentityProviderConfigs",
                "iam>ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ssm:GetParameter",
            "Resource": "arn:aws:ssm:*:111122223333:parameter/*"
        }
    ]
}
```

To view nodes in [connected clusters \(p. 574\)](#), the [Amazon EKS connector IAM role \(p. 508\)](#) should be able to impersonate the principal in the cluster. This allows the [Amazon EKS Connector \(p. 574\)](#) to map the principal to a Kubernetes user.

2. Create a Kubernetes `rolebinding` or `clusterrolebinding` that is bound to a Kubernetes `role` or `clusterrole` that has the necessary permissions to view the Kubernetes resources. To learn more about Kubernetes roles and role bindings, see [Using RBAC Authorization](#) in the Kubernetes documentation. You can apply one of the following manifests to your cluster that create a `role` and `rolebinding` or a `clusterrole` and `clusterrolebinding` with the necessary Kubernetes permissions:

View Kubernetes resources in all namespaces

The group name in the file is `eks-console-dashboard-full-access-group`. Apply the manifest to your cluster with the following command:

```
kubectl apply -f https://s3.us-west-2.amazonaws.com/amazon-eks/docs/eks-console-full-access.yaml
```

View Kubernetes resources in a specific namespace

The namespace in this file is `default`. The group name in the file is `eks-console-dashboard-restricted-access-group`. Apply the manifest to your cluster with the following command:

```
kubectl apply -f https://s3.us-west-2.amazonaws.com/amazon-eks/docs/eks-console-restricted-access.yaml
```

If you need to change the Kubernetes group name, namespace, permissions, or any other configuration in the file, then download the file and edit it before applying it to your cluster:

1. Download the file with one of the following commands:

```
curl -o https://s3.us-west-2.amazonaws.com/amazon-eks/docs/eks-console-full-access.yaml
```

```
curl -o https://s3.us-west-2.amazonaws.com/amazon-eks/docs/eks-console-restricted-access.yaml
```

2. Edit the file as necessary.

3. Apply the manifest to your cluster with one of the following commands:

```
kubectl apply -f eks-console-full-access.yaml
```

```
kubectl apply -f eks-console-restricted-access.yaml
```

3. Map the [IAM principal](#) to the Kubernetes user or group in the aws-auth ConfigMap. You can use a tool such as eksctl to update the ConfigMap or you can update it manually by editing it.

Important

We recommend using eksctl, or another tool, to edit the ConfigMap. For information about other tools you can use, see [Use tools to make changes to the aws-authConfigMap](#) in the Amazon EKS best practices guides. An improperly formatted aws-auth ConfigMap can cause you to lose access to your cluster.

eksctl

Prerequisite

Version 0.160.0 or later of the eksctl command line tool installed on your device or AWS CloudShell. To install or update eksctl, see [Installing or updating eksctl \(p. 13\)](#).

1. View the current mappings in the ConfigMap. Replace *my-cluster* with the name of your cluster. Replace *region-code* with the AWS Region that your cluster is in.

```
eksctl get iamidentitymapping --cluster my-cluster --region=region-code
```

An example output is as follows.

ARN	USERNAME	GROUPS
ACCOUNT		
arn:aws:iam::111122223333:role/eksctl-my-cluster-my-nodegroup-NodeInstanceRole-1XLS7754U3ZPA	system:node:{{EC2PrivateDNSName}}	
	system:bootstrappers,system:nodes	

2. Add a mapping for a role. This example assume that you attached the IAM permissions in the first step to a role named *my-console-viewer-role*. Replace *111122223333* with your account ID.

```
eksctl create iamidentitymapping \
--cluster my-cluster \
--region=region-code \
--arn arn:aws:iam::111122223333:role/my-console-viewer-role \
--group eks-console-dashboard-full-access-group \
--no-duplicate-arns
```

Important

The role ARN can't include a path such as `role/my-team/developers/my-role`.
The format of the ARN must be `arn:aws:iam::111122223333:role/my-role`.
In this example, `my-team/developers/` needs to be removed.

An example output is as follows.

```
[...]
2022-05-09 14:51:20 [#] adding identity "arn:aws:iam::111122223333:role/my-console-viewer-role" to auth ConfigMap
```

3. Add a mapping for a user. [IAM best practices](#) recommend that you grant permissions to roles instead of users. This example assume that you attached the IAM permissions in the first step to a user named `my-user`. Replace `111122223333` with your account ID.

```
eksctl create iamidentitymapping \
--cluster my-cluster \
--region=region-code \
--arn arn:aws:iam::111122223333:user/my-user \
--group eks-console-dashboard-restricted-access-group \
--no-duplicate-arns
```

An example output is as follows.

```
[...]
2022-05-09 14:53:48 [#] adding identity "arn:aws:iam::111122223333:user/my-user" to auth ConfigMap
```

4. View the mappings in the ConfigMap again.

```
eksctl get iamidentitymapping --cluster my-cluster --region=region-code
```

An example output is as follows.

ARN	USERNAME ACCOUNT	GROUPS
<code>arn:aws:iam::111122223333:role/eksctl-my-cluster-my-nodegroup-NodeInstanceRole-1XLS7754U3ZPA</code>	<code>system:node:{EC2PrivateDNSName}</code>	
<code>arn:aws:iam::111122223333:role/<i>my-console-viewer-role</i></code>	<code>eks-console-dashboard-full-access-group</code>	<code>eks-console-dashboard-restricted-access-group</code>
<code>arn:aws:iam::111122223333:user/<i>my-user</i></code>		<code>eks-console-dashboard-restricted-access-group</code>

Edit ConfigMap manually

For more information about adding users or roles to the aws-auth ConfigMap, see [the section called "Add IAM principals" \(p. 421\)](#).

1. Open the aws-auth ConfigMap for editing.

```
kubectl edit -n kube-system configmap/aws-auth
```

2. Add the mappings to the aws-auth ConfigMap, but don't replace any of the existing mappings. The following example adds mappings between [IAM principals](#) with permissions added in the first step and the Kubernetes groups created in the previous step:

- The *my-console-viewer-role* role and the eks-console-dashboard-full-access-group.
- The *my-user* user and the eks-console-dashboard-restricted-access-group.

These examples assume that you attached the IAM permissions in the first step to a role named *my-console-viewer-role* and a user named *my-user*. Replace *111122223333* with your AWS account ID.

```
apiVersion: v1
data:
mapRoles: |
  - groups:
    - eks-console-dashboard-full-access-group
      rolearn: arn:aws:iam::111122223333:role/my-console-viewer-role
      username: my-console-viewer-role
mapUsers: |
  - groups:
    - eks-console-dashboard-restricted-access-group
      userarn: arn:aws:iam::111122223333:user/my-user
      username: my-user
```

Important

The role ARN can't include a path such as role/my-team/developers/*my-console-viewer-role*. The format of the ARN must be `arn:aws:iam::111122223333:role/my-console-viewer-role`. In this example, my-team/developers/ needs to be removed.

3. Save the file and exit your text editor.

Observability in Amazon EKS

You can observe your data in Amazon EKS using many available monitoring or logging tools. Your Amazon EKS log data can be streamed to AWS services or to partner tools for data analysis. There are many services available in the AWS Management Console that provide data for troubleshooting your Amazon EKS issues.

After selecting **Clusters** in the left navigation pane of the Amazon EKS console, you can view cluster health and details by selecting your cluster's name. To view details about any existing Kubernetes resources that are deployed to your cluster, see [View Kubernetes resources \(p. 529\)](#).

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon EKS and your AWS solutions. We recommend that you collect monitoring data from all of the parts of your AWS solution. That way, you can more easily debug a multi-point failure if one occurs. Before you start monitoring Amazon EKS, make sure that your monitoring plan addresses the following questions.

- What are your goals? Do you need real-time notifications if your clusters scale dramatically?
- What resources need to be observed?
- How frequently do you need to observe these resources? Does your company want to respond quickly to risks?
- What tools do you intend to use? If you already run AWS Fargate as part of your launch, then you can use the built-in [log router \(p. 145\)](#).
- Who you do intend to perform the monitoring tasks?
- Whom do you want notifications to be sent to when something goes wrong?

Logging and monitoring on Amazon EKS

Amazon EKS provides built-in tools for logging and monitoring. Control plane logging records all API calls to your clusters, audit information capturing what users performed what actions to your clusters, and role-based information. For more information, see [Logging and monitoring on Amazon EKS](#) in the [AWS Prescriptive Guidance](#).

Amazon EKS control plane logging provides audit and diagnostic logs directly from the Amazon EKS control plane to CloudWatch Logs in your account. These logs make it easy for you to secure and run your clusters. You can select the exact log types you need, and logs are sent as log streams to a group for each Amazon EKS cluster in CloudWatch. For more information, see [the section called "Configuring logging" \(p. 536\)](#).

Note

When you check the Amazon EKS authenticator logs in Amazon CloudWatch, the entries are displayed that contain text similar to the following example text.

```
level=info msg="mapping IAM role" groups="[]"
role="arn:aws:iam::111122223333:role/XXXXXXXXXXXXXXXXXX-NodeManagerRole-XXXXXXX"
username="eks:node-manager"
```

Entries that contain this text are expected. The `username` is an Amazon EKS internal service role that performs specific operations for managed node groups and Fargate. For low-level, customizable logging, then [Kubernetes logging](#) is available.

Amazon EKS is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon EKS. CloudTrail captures all API calls for Amazon EKS as events. The calls captured include calls from the Amazon EKS console and code calls to the Amazon EKS API operations. For more information, see [the section called "Logging Amazon EKS API calls with AWS CloudTrail" \(p. 543\)](#).

The Kubernetes API server exposes a number of metrics that are useful for monitoring and analysis. For more information, see [Control plane metrics with Prometheus \(p. 540\)](#).

To configure Fluent Bit for custom Amazon CloudWatch logs, see [Setting up Fluent Bit](#) in the Amazon CloudWatch User Guide.

Amazon EKS logging and monitoring tools

Amazon Web Services provides various tools that you can use to monitor Amazon EKS. You can configure some tools to set up automatic monitoring, but some require manual calls. We recommend that you automate monitoring tasks as much as your environment and existing toolset allows.

Logging Tools

Areas	Tool	Logs	Setup
Applications	Amazon CloudWatch Container Insights	It collects, aggregates, and summarizes metrics and logs from your containerized applications and microservices.	Setup procedure
Control plane	AWS CloudTrail (p. 543)	It logs API calls by a user, role, or service.	Setup procedure
Multiple areas for AWS Fargate instances	AWS Fargate log router (p. 145)	For AWS Fargate instances, it streams logs to AWS services or partner tools. Uses AWS for Fluent Bit . Logs can be streamed to other AWS services or partner tools.	Setup procedure (p. 145)

Monitoring Tools

Areas	Tool	Logs	Setup
Applications	CloudWatch Container Insights	CloudWatch Container Insights collects, aggregates, and summarizes metrics and	Setup procedure

Areas	Tool	Logs	Setup
		logs from your containerized applications and microservices.	
Applications	AWS Distro for OpenTelemetry (ADOT)	It collects and sends correlated metrics, trace data, and metadata to AWS monitoring services or partners. It can be set up through CloudWatch Container Insights.	Setup procedure (p. 549)
Applications	Amazon DevOps Guru	It detects node-level operational performance and availability.	Setup procedure
Applications	AWS X-Ray	It receives trace data about your application. This trace data includes ingoing and outgoing requests and metadata about the requests. For Amazon EKS, the implementation requires the OpenTelemetry add-on.	Setup procedure
Control plane	Prometheus (p. 540)	CloudWatch Logs ingestion, archive storage, and data scanning rates apply to enabled control plane logs.	Setup procedure

Amazon EKS control plane logging

Amazon EKS control plane logging provides audit and diagnostic logs directly from the Amazon EKS control plane to CloudWatch Logs in your account. These logs make it easy for you to secure and run your clusters. You can select the exact log types you need, and logs are sent as log streams to a group for each Amazon EKS cluster in CloudWatch. For more information, see [Amazon CloudWatch logging](#).

You can start using Amazon EKS control plane logging by choosing which log types you want to enable for each new or existing Amazon EKS cluster. You can enable or disable each log type on a per-cluster basis using the AWS Management Console, AWS CLI (version 1.16.139 or higher), or through

the Amazon EKS API. When enabled, logs are automatically sent from the Amazon EKS cluster to CloudWatch Logs in the same account.

When you use Amazon EKS control plane logging, you're charged standard Amazon EKS pricing for each cluster that you run. You are charged the standard CloudWatch Logs data ingestion and storage costs for any logs sent to CloudWatch Logs from your clusters. You are also charged for any AWS resources, such as Amazon EC2 instances or Amazon EBS volumes, that you provision as part of your cluster.

The following cluster control plane log types are available. Each log type corresponds to a component of the Kubernetes control plane. To learn more about these components, see [Kubernetes Components](#) in the Kubernetes documentation.

API server (api)

Your cluster's API server is the control plane component that exposes the Kubernetes API. If you enable API server logs when you launch the cluster, or shortly thereafter, the logs include API server flags that were used to start the API server. For more information, see [kube-apiserver](#) and the [audit policy](#) in the Kubernetes documentation.

Audit (audit)

Kubernetes audit logs provide a record of the individual users, administrators, or system components that have affected your cluster. For more information, see [Auditing](#) in the Kubernetes documentation.

Authenticator (authenticator)

Authenticator logs are unique to Amazon EKS. These logs represent the control plane component that Amazon EKS uses for Kubernetes [Role Based Access Control](#) (RBAC) authentication using IAM credentials. For more information, see [Cluster management \(p. 444\)](#).

Controller manager (controllerManager)

The controller manager manages the core control loops that are shipped with Kubernetes. For more information, see [kube-controller-manager](#) in the Kubernetes documentation.

Scheduler (scheduler)

The scheduler component manages when and where to run Pods in your cluster. For more information, see [kube-scheduler](#) in the Kubernetes documentation.

Enabling and disabling control plane logs

By default, cluster control plane logs aren't sent to CloudWatch Logs. You must enable each log type individually to send logs for your cluster. CloudWatch Logs ingestion, archive storage, and data scanning rates apply to enabled control plane logs. For more information, see [CloudWatch pricing](#).

To update the control plane logging configuration, Amazon EKS requires up to five available IP addresses in each subnet. When you enable a log type, the logs are sent with a log verbosity level of 2.

AWS Management Console

To enable or disable control plane logs with the AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose the name of the cluster to display your cluster information.
3. Choose the **Logging** tab.
4. Choose **Manage logging**.
5. For each individual log type, choose whether the log type should be **Enabled** or **Disabled**. By default, each log type is **Disabled**.

6. Choose **Save changes** to finish.

AWS CLI

To enable or disable control plane logs with the AWS CLI

1. Check your AWS CLI version with the following command.

```
aws --version
```

If your AWS CLI version is earlier than 1.16.139, you must first update to the latest version. To install or upgrade the AWS CLI, see [Installing the AWS Command Line Interface](#) in the *AWS Command Line Interface User Guide*.

2. Update your cluster's control plane log export configuration with the following AWS CLI command. Replace *my-cluster* with your cluster name and specify your desired endpoint access values.

Note

The following command sends all available log types to CloudWatch Logs.

```
aws eks update-cluster-config \
--region region-code \
--name my-cluster \
--logging '{"clusterLogging": [{"types": ["api", "audit", "authenticator", "controllerManager", "scheduler"], "enabled": true}]}'
```

An example output is as follows.

```
{
  "update": {
    "id": "883405c8-65c6-4758-8cee-2a7c1340a6d9",
    "status": "InProgress",
    "type": "LoggingUpdate",
    "params": [
      {
        "type": "ClusterLogging",
        "value": "{\"clusterLogging\": [{\"types\": [\"api\", \"audit\", \"authenticator\", \"controllerManager\", \"scheduler\"], \"enabled\": true}]}"
      }
    ],
    "createdAt": 1553271814.684,
    "errors": []
  }
}
```

3. Monitor the status of your log configuration update with the following command, using the cluster name and the update ID that were returned by the previous command. Your update is complete when the status appears as Successful.

```
aws eks describe-update \
--region region-code \
--name my-cluster \
--update-id 883405c8-65c6-4758-8cee-2a7c1340a6d9
```

An example output is as follows.

```
{
  "update": {
```

```
"id": "883405c8-65c6-4758-8cee-2a7c1340a6d9",
"status": "Successful",
"type": "LoggingUpdate",
"params": [
    {
        "type": "ClusterLogging",
        "value": "{\"clusterLogging\": [{\"types\": [\"api\", \"audit\", \"authenticator\", \"controllerManager\", \"scheduler\"], \"enabled\": true}]}"
    }
],
"createdAt": 1553271814.684,
"errors": []
}
```

Viewing cluster control plane logs

After you have enabled any of the control plane log types for your Amazon EKS cluster, you can view them on the CloudWatch console.

To learn more about viewing, analyzing, and managing logs in CloudWatch, see the [Amazon CloudWatch Logs User Guide](#).

To view your cluster control plane logs on the CloudWatch console

1. Open the [CloudWatch console](#). The link opens the console and displays your current available log groups and filters them with the /aws/eks prefix.
2. Choose the cluster that you want to view logs for. The log group name format is /aws/eks/*my-cluster*/cluster.
3. Choose the log stream to view. The following list describes the log stream name format for each log type.

Note

As log stream data grows, the log stream names are rotated. When multiple log streams exist for a particular log type, you can view the latest log stream by looking for the log stream name with the latest **Last event time**.

- **Kubernetes API server component logs (api)** – kube-apiserver-*1234567890abcdef01234567890abcde*
 - **Audit (audit)** – kube-apiserver-audit-*1234567890abcdef01234567890abcde*
 - **Authenticator (authenticator)** – authenticator-*1234567890abcdef01234567890abcde*
 - **Controller manager (controllerManager)** – kube-controller-manager-*1234567890abcdef01234567890abcde*
 - **Scheduler (scheduler)** – kube-scheduler-*1234567890abcdef01234567890abcde*
4. Look through the events of the log stream.

For example, you should see the initial API server flags for the cluster when viewing the top of kube-apiserver-*1234567890abcdef01234567890abcde*.

Note

If you don't see the API server logs at the beginning of the log stream, then it is likely that the API server log file was rotated on the server before you enabled API server logging on the server. Any log files that are rotated before API server logging is enabled can't be exported to CloudWatch.

However, you can create a new cluster with the same Kubernetes version and enable the API server logging when you create the cluster. Clusters with the same platform version have

the same flags enabled, so your flags should match the new cluster's flags. When you finish viewing the flags for the new cluster in CloudWatch, you can delete the new cluster.

Control plane metrics with Prometheus

The Kubernetes API server exposes a number of metrics that are useful for monitoring and analysis. These metrics are exposed internally through a metrics endpoint that refers to the /metrics HTTP API. Like other endpoints, this endpoint is exposed on the Amazon EKS control plane.

While this endpoint is useful if you are looking for a specific metric, you typically want to analyze these metrics over time. To do this, you can deploy [Prometheus](#) into your cluster. Prometheus is a monitoring and time series database that scrapes exposed endpoints and aggregates data, allowing you to filter, graph, and query the results. This topic explains how to deploy Prometheus and some of the ways that you can use it to view and analyze what your cluster is doing.

Viewing the raw metrics

To view the raw metrics output, use kubectl with the --raw flag. This command allows you to pass any HTTP path and returns the raw response.

```
kubectl get --raw /metrics
```

An example output is as follows.

```
[...]
# HELP rest_client_requests_total Number of HTTP requests, partitioned by status code,
method, and host.
# TYPE rest_client_requests_total counter
rest_client_requests_total{code="200",host="127.0.0.1:21362",method="POST"} 4994
rest_client_requests_total{code="200",host="127.0.0.1:443",method="DELETE"} 1
rest_client_requests_total{code="200",host="127.0.0.1:443",method="GET"} 1.326086e+06
rest_client_requests_total{code="200",host="127.0.0.1:443",method="PUT"} 862173
rest_client_requests_total{code="404",host="127.0.0.1:443",method="GET"} 2
rest_client_requests_total{code="409",host="127.0.0.1:443",method="POST"} 3
rest_client_requests_total{code="409",host="127.0.0.1:443",method="PUT"} 8
# HELP ssh_tunnel_open_count Counter of ssh tunnel total open attempts
# TYPE ssh_tunnel_open_count counter
ssh_tunnel_open_count 0
# HELP ssh_tunnel_open_fail_count Counter of ssh tunnel failed open attempts
# TYPE ssh_tunnel_open_fail_count counter
ssh_tunnel_open_fail_count 0
```

This raw output returns verbatim what the API server exposes. These metrics are represented in a [Prometheus format](#). This format allows the API server to expose different metrics broken down by line. Each line includes a metric name, tags, and a value.

```
metric_name{"tag"="value"[,...]} value
```

While this endpoint is useful if you are looking for a specific metric, you typically want to analyze these metrics over time. To do this, you can deploy Prometheus into your cluster.

Deploying Prometheus

This topic helps you deploy Prometheus into your cluster with Helm V3. If you already have Helm installed, you can check your version with the `helm version` command. Helm is a package manager

for Kubernetes clusters. For more information about Helm and how to install it, see [Using Helm with Amazon EKS \(p. 450\)](#).

After you configure Helm for your Amazon EKS cluster, you can use it to deploy Prometheus with the following steps.

To deploy Prometheus using Helm

1. Create a Prometheus namespace.

```
kubectl create namespace prometheus
```

2. Add the prometheus-community chart repository.

```
helm repo add prometheus-community https://prometheus-community.github.io/helm-charts
```

3. Deploy Prometheus.

```
helm upgrade -i prometheus prometheus-community/prometheus \
  --namespace prometheus \
  --set
  alertmanager.persistentVolume.storageClass="gp2",server.persistentVolume.storageClass="gp2"
```

Note

If you get the error `Error: failed to download "stable/prometheus"` (hint: running `helm repo update` may help) when executing this command, run `helm repo update prometheus-community`, and then try running the Step 2 command again.

If you get the error `Error: rendered manifests contain a resource that already exists`, run `helm uninstall your-release-name -n namespace`, then try running the Step 3 command again.

4. Verify that all of the Pods in the `prometheus` namespace are in the READY state.

```
kubectl get pods -n prometheus
```

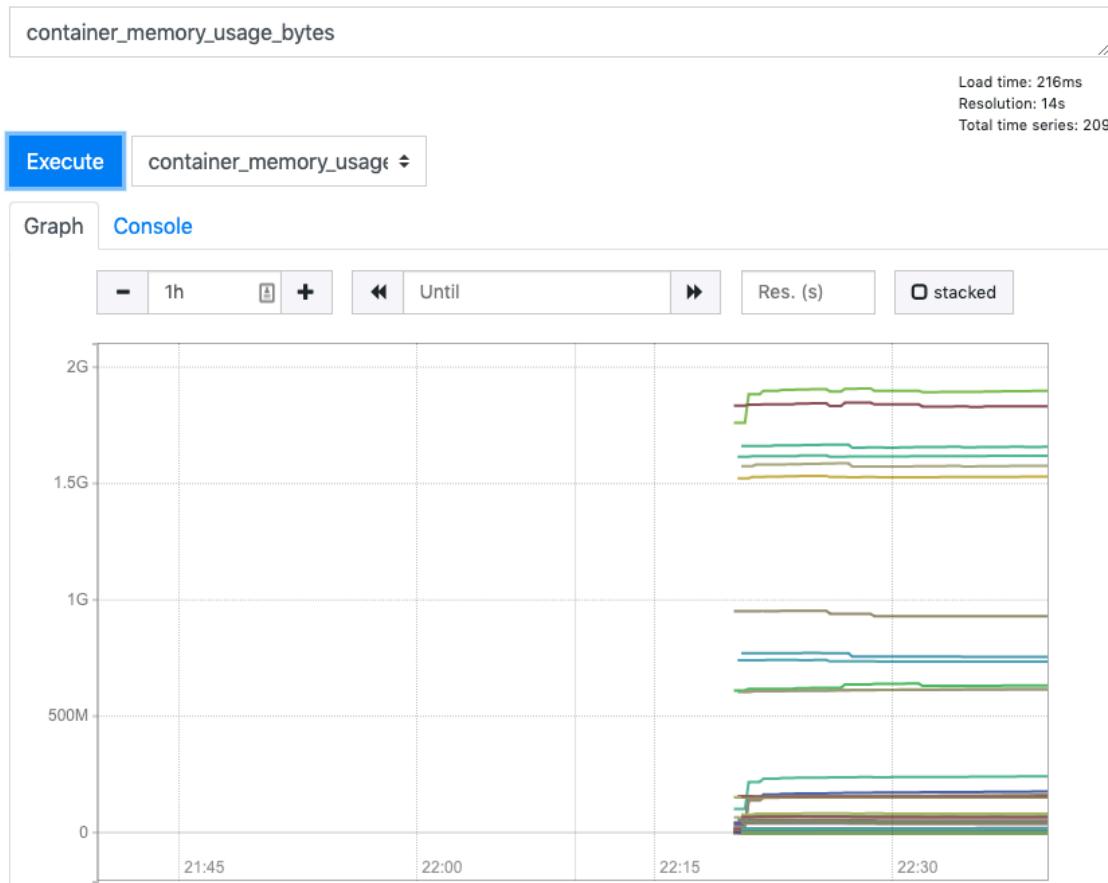
An example output is as follows.

NAME	READY	STATUS	RESTARTS	AGE
prometheus-alertmanager-59b4c8c744-r7bgp	1/2	Running	0	48s
prometheus-kube-state-metrics-7cf87cf99-jkz2f	1/1	Running	0	48s
prometheus-node-exporter-jcjzq	1/1	Running	0	48s
prometheus-node-exporter-jxv2h	1/1	Running	0	48s
prometheus-node-exporter-vbdks	1/1	Running	0	48s
prometheus-pushgateway-76c444b68c-82tnw	1/1	Running	0	48s
prometheus-server-775957f748-mmht9	1/2	Running	0	48s

5. Use `kubectl` to port forward the Prometheus console to your local machine.

```
kubectl --namespace=prometheus port-forward deploy/prometheus-server 9090
```

6. Point a web browser to `http://localhost:9090` to view the Prometheus console.
7. Choose a metric from the `- insert metric at cursor` menu, then choose **Execute**. Choose the **Graph** tab to show the metric over time. The following image shows `container_memory_usage_bytes` over time.



8. From the top navigation bar, choose **Status**, then **Targets**.

The figure shows the Prometheus interface with the top navigation bar including **Prometheus**, **Alerts**, **Graph**, **Status** (with a dropdown arrow), **Help**, and other links. A dropdown menu is open under **Status**, showing options: **Runtime & Build Information**, **Command-Line Flags**, **Configuration**, **Rules**, **Targets** (which is highlighted in blue), and **Service Discovery**. Below the dropdown, there's a section for **Element** with the message `no data`. At the bottom left is a blue **Add Graph** button.

All of the Kubernetes endpoints that are connected to Prometheus using service discovery are displayed.

Store your Prometheus metrics in Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus is a Prometheus-compatible monitoring and alerting service that makes it easy to monitor containerized applications and infrastructure at scale. It is a fully-managed service that automatically scales the ingestion, storage, querying, and alerting of your metrics. It also integrates with AWS security services to enable fast and secure access to your data. You can use the open-source PromQL query language to query your metrics and alert on them.

For more information, see [Getting started with Amazon Managed Service for Prometheus](#).

Logging Amazon EKS API calls with AWS CloudTrail

Amazon EKS is integrated with AWS CloudTrail. CloudTrail is a service that provides a record of actions by a user, role, or an AWS service in Amazon EKS. CloudTrail captures all API calls for Amazon EKS as events. This includes calls from the Amazon EKS console and from code calls to the Amazon EKS API operations.

If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket. This includes events for Amazon EKS. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information that CloudTrail collects, you can determine several details about a request. For example, you can determine when the request was made to Amazon EKS, the IP address where the request was made from, and who made the request.

To learn more about CloudTrail, see the [AWS CloudTrail User Guide](#).

Topics

- [Amazon EKS information in CloudTrail \(p. 543\)](#)
- [Understanding Amazon EKS log file entries \(p. 544\)](#)
- [Enable Auto Scaling group metrics collection \(p. 546\)](#)

Amazon EKS information in CloudTrail

When you create your AWS account, CloudTrail is also enabled on your AWS account. When any activity occurs in Amazon EKS, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see [Viewing events with CloudTrail event history](#).

For an ongoing record of events in your AWS account, including events for Amazon EKS, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all AWS Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data that's collected in CloudTrail logs. For more information, see the following resources.

- [Overview for creating a trail](#)
- [CloudTrail supported services and integrations](#)

- [Configuring Amazon SNS notifications for CloudTrail](#)
- [Receiving CloudTrail log files from multiple regions](#) and [Receiving CloudTrail log files from multiple accounts](#)

All Amazon EKS actions are logged by CloudTrail and are documented in the [Amazon EKS API Reference](#). For example, calls to the [CreateCluster](#), [ListClusters](#) and [DeleteCluster](#) sections generate entries in the CloudTrail log files.

Every event or log entry contains information about the type of IAM identity that made the request, and which credentials were used. If temporary credentials were used, the entry shows how the credentials were obtained.

For more information, see the [CloudTrail userIdentity element](#).

Understanding Amazon EKS log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action. This include information such as the date and time of the action and the request parameters that were used. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the [CreateCluster](#) action.

```
{  
    "eventVersion": "1.05",  
    "userIdentity": {  
        "type": "IAMUser",  
        "principalId": "AKIAIOSFODNN7EXAMPLE",  
        "arn": "arn:aws:iam::111122223333:user/username",  
        "accountId": "111122223333",  
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
        "userName": "username"  
    },  
    "eventTime": "2018-05-28T19:16:43Z",  
    "eventSource": "eks.amazonaws.com",  
    "eventName": "CreateCluster",  
    "awsRegion": "region-code",  
    "sourceIPAddress": "205.251.233.178",  
    "userAgent": "PostmanRuntime/6.4.0",  
    "requestParameters": {  
        "resourcesVpcConfig": {  
            "subnetIds": [  
                "subnet-a670c2df",  
                "subnet-4f8c5004"  
            ]  
        },  
        "roleArn": "arn:aws:iam::111122223333:role/AWSServiceRoleForAmazonEKS-CAC1G1VH3ZKZ",  
        "clusterName": "test"  
    },  
    "responseElements": {  
        "cluster": {  
            "clusterName": "test",  
            "status": "CREATING",  
            "createdAt": 1527535003.208,  
            "certificateAuthority": {},  
            "arn": "arn:aws:eks:region-code:111122223333:cluster/test",  
            "roleArn": "arn:aws:iam::111122223333:role/AWSServiceRoleForAmazonEKS-CAC1G1VH3ZKZ",  
            "version": "1.10",  
            "resourcesVpcConfig": {  
                "securityGroupIds": []  
            }  
        }  
    }  
}
```

```

        "vpcId": "vpc-21277358",
        "subnetIds": [
            "subnet-a670c2df",
            "subnet-4f8c5004"
        ]
    }
},
"requestID": "a7a0735d-62ab-11e8-9f79-81ce5b2b7d37",
"eventID": "eab22523-174a-499c-9dd6-91e7be3ff8e3",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}

```

Log Entries for Amazon EKS Service Linked Roles

The Amazon EKS service linked roles make API calls to AWS resources. CloudTrail log entries with `username: AWSServiceRoleForAmazonEKS` and `username: AWSServiceRoleForAmazonEKSNodegroup` appears for calls made by the Amazon EKS service linked roles. For more information about Amazon EKS and service linked roles, see [Using service-linked roles for Amazon EKS \(p. 490\)](#).

The following example shows a CloudTrail log entry that demonstrates a `DeleteInstanceProfile` action that's made by the `AWSServiceRoleForAmazonEKSNodegroup` service linked role, noted in the `sessionContext`.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA3WHGPEZ7SJ2CW55C5:EKS",
        "arn": "arn:aws:sts:111122223333:assumed-role/AWSServiceRoleForAmazonEKSNodegroup/EKS",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA3WHGPEZ7SJ2CW55C5",
                "arn": "arn:aws:iam:111122223333:role/aws-service-role/eks-nodegroup.amazonaws.com/AWSServiceRoleForAmazonEKSNodegroup",
                "accountId": "111122223333",
                "userName": "AWSServiceRoleForAmazonEKSNodegroup"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-02-26T00:56:33Z"
            }
        },
        "invokedBy": "eks-nodegroup.amazonaws.com"
    },
    "eventTime": "2020-02-26T00:56:34Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "DeleteInstanceProfile",
    "awsRegion": "region-code",
    "sourceIPAddress": "eks-nodegroup.amazonaws.com",
    "userAgent": "eks-nodegroup.amazonaws.com",
    "requestParameters": {
        "instanceProfileName": "eks-11111111-2222-3333-4444-abcdef123456"
    },
    "responseElements": null,
}
```

```

    "requestID": "11111111-2222-3333-4444-abcdef123456",
    "eventID": "11111111-2222-3333-4444-abcdef123456",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
  
```

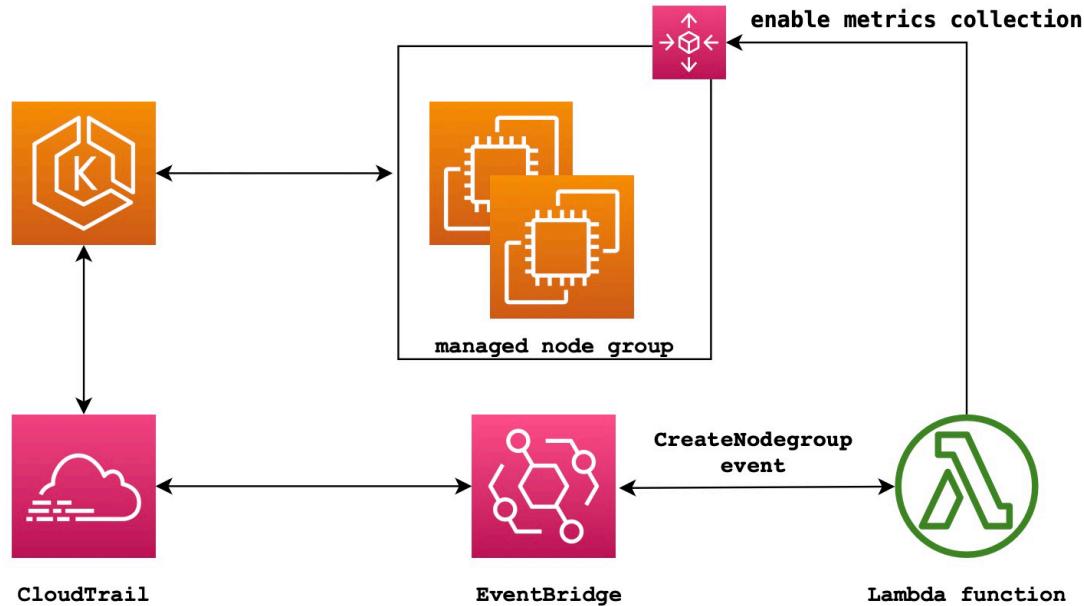
Enable Auto Scaling group metrics collection

This topic describes how you can enable Auto Scaling group metrics collection using [AWS Lambda](#) and [AWS CloudTrail](#). Amazon EKS doesn't automatically enable group metrics collection for Auto Scaling groups created for managed nodes.

You can use [Auto Scaling group metrics](#) to track changes in an Auto Scaling group and to set alarms on threshold values. Auto Scaling group metrics are available in the Auto Scaling console or the [Amazon CloudWatch](#) console. Once enabled, the Auto Scaling group sends sampled data to Amazon CloudWatch every minute. There is no charge for enabling these metrics.

By enabling Auto Scaling group metrics collection, you'll be able to monitor the scaling of managed node groups. Auto Scaling group metrics report the minimum, maximum, and desired size of an Auto Scaling group. You can create an alarm if the number of nodes in a node group falls below the minimum size, which would indicate an unhealthy node group. Tracking node group size is also useful in adjusting the maximum count so that your data plane doesn't run out of capacity.

When you create a managed node group, AWS CloudTrail sends a `CreateNodegroup` event to [Amazon EventBridge](#). By creating an Amazon EventBridge rule that matches the `CreateNodegroup` event, you trigger a Lambda function to enable group metrics collection for the Auto Scaling group associated with the managed node group.



To enable Auto Scaling group metrics collection

1. Create an IAM role for Lambda.

```

LAMBDA_ROLE=$(aws iam create-role \
--role-name lambda-asg-enable-metrics \
  
```

```
--assume-role-policy-document '{"Version": "2012-10-17", "Statement": [{"Effect": "Allow", "Principal": {"Service": "lambda.amazonaws.com"}, "Action": "sts:AssumeRole"}]}' \
--output text \
--query 'Role.Arn')
echo $LAMBDA_ROLE
```

2. Create a policy that allows describing Amazon EKS node groups and enabling Auto Scaling group metrics collection.

```
cat > /tmp/lambda-policy.json <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "eks:DescribeNodegroup",
                "autoscaling:EnableMetricsCollection"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
EOF
LAMBDA_POLICY_ARN=$(aws iam create-policy \
--policy-name lambda-asg-enable-metrics-policy \
--policy-document file:///tmp/lambda-policy.json \
--output text \
--query 'Policy.Arn')
echo $LAMBDA_POLICY_ARN
```

3. Attach the policy to the IAM role for Lambda.

```
aws iam attach-role-policy \
--policy-arn $LAMBDA_POLICY_ARN \
--role-name lambda-asg-enable-metrics
```

4. Add the AWSLambdaBasicExecutionRole managed policy, which has the permissions that the function needs to write logs to CloudWatch Logs.

```
aws iam attach-role-policy \
--role-name lambda-asg-enable-metrics \
--policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
```

5. Create the Lambda code.

```
cat > /tmp/lambda-handler.py <<EOF
import json
import boto3
import time
import logging

eks = boto3.client('eks')
autoscaling = boto3.client('autoscaling')

logger = logging.getLogger()
logger.setLevel(logging.INFO)

def lambda_handler(event, context):
    ASG_METRICS_COLLECTOR_TAG_NAME = "ASG_METRICS_COLLECTION_ENABLED"
```

```

initial_retry_delay = 10
attempts = 0

#print(event)

if not event["detail"]["eventName"] == "CreateNodegroup":
    print("invalid event.")
    return -1

clusterName = event["detail"]["requestParameters"]["name"]
nodegroupName = event["detail"]["requestParameters"]["nodegroupName"]
try:
    metricsCollectionEnabled = event["detail"]["requestParameters"]["tags"]
[ASG_METRICS_COLLECTION_TAG_NAME]
except KeyError:
    print(ASG_METRICS_COLLECTION_TAG_NAME, "tag not found.")
    return

# Check if metrics collection is enabled in tags
if metricsCollectionEnabled.lower() != "true":
    print("Metrics collection is not enabled in nodegroup tags.")
    return

# Get the name of the associated autoscaling group
print("Getting the autoscaling group name for nodegroup=", nodegroupName, ",",
cluster=", clusterName )
for i in range(0,10):
    try:
        autoScalingGroup =
eks.describe_nodegroup(clusterName=clusterName,nodegroupName=nodegroupName)
["nodegroup"]["resources"]["autoScalingGroups"][0]["name"]
    except:
        attempts += 1
        print("Failed to obtain the associated autoscaling group for nodegroup",
nodegroupName, "Retrying in", initial_retry_delay*attempts, "seconds.")
        time.sleep(initial_retry_delay*attempts)
    else:
        break

    print("Enabling metrics collection on autoscaling group ", autoScalingGroup)

    # Enable metrics collection in the autoscaling group
    try:
        enableMetricsCollection =
autoscaling.enable_metrics_collection(AutoScalingGroupName=autoScalingGroup,Granularity="1Minute")
    except:
        print("Unable to enable metrics collection on nodegroup=",nodegroup)
        print("Enabled metrics collection on nodegroup", nodegroupName)
EOF

```

6. Create a deployment package.

```

cd /tmp
zip function.zip lambda-handler.py

```

7. Create a Lambda function.

```

LAMBDA_ARN=$(aws lambda create-function --function-name asg-enable-metrics-collection \
--zip-file fileb://function.zip --handler lambda-handler.lambda_handler \
--runtime python3.9 \
--timeout 600 \
--role $LAMBDA_ROLE \
--output text \
--query 'FunctionArn')

```

```
echo $LAMBDA_ARN
```

8. Create an EventBridge rule.

```
RULE_ARN=$(aws events put-rule --name CreateNodegroupRuleToLambda \
    --event-pattern "{\"source\": [\"aws.eks\"], \"detail-type\": [\"AWS API Call via \
    CloudTrail\"], \"detail\": {\"eventName\": [\"CreateNodegroup\"], \"eventSource\": \
    [\"eks.amazonaws.com\"]}}" \
    --output text \
    --query 'RuleArn')
echo $RULE_ARN
```

9. Add the Lambda function as a target.

```
aws events put-targets --rule CreateNodegroupRuleToLambda \
    --targets "Id=\"1\",Arn=\"$LAMBDA_ARN"
```

10. Add a policy that allows EventBridge to invoke the Lambda function.

```
aws lambda add-permission \
    --function-name asg-enable-metrics-collection \
    --statement-id CreateNodegroupRuleToLambda \
    --action 'lambda:InvokeFunction' \
    --principal events.amazonaws.com \
    --source-arn $RULE_ARN
```

The Lambda function enables Auto Scaling group metrics collection for any managed node groups that you tag with ASG_METRICS_COLLECTION_ENABLED set to TRUE. To confirm that **Auto Scaling group metrics collection** is enabled, navigate to the associated Auto Scaling group in the Amazon EC2 console. In the **Monitoring** tab, you should see that the **Enable** check box is activated.

Amazon EKS add-on support for ADOT Operator

Amazon EKS supports using the AWS Management Console, AWS CLI and Amazon EKS API to install and manage the [AWS Distro for OpenTelemetry \(ADOT\)](#) Operator. This enables a simplified experience for instrumenting your applications running on Amazon EKS to send metric and trace data to multiple monitoring service options like [Amazon CloudWatch](#), [Prometheus](#), and [X-Ray](#). This topic describes how to get started using ADOT for applications running on your Amazon EKS cluster.

- [Prerequisites \(p. 550\)](#)
- [Creating an IAM role \(p. 550\)](#)
- [Installing the add-on \(p. 551\)](#)
- [Deploying the ADOT Collector \(p. 555\)](#) for your preferred monitoring option
- [Deploying the ADOT Collector using advanced configuration \(p. 555\)](#)
- [Deploying a sample application \(p. 553\)](#) to generate OTLP data

Before installing ADOT, make sure that you have read and understand the [prerequisites and considerations \(p. 550\)](#).

AWS Distro for OpenTelemetry (ADOT) prerequisites and considerations

Before installing the AWS Distro for OpenTelemetry (ADOT) add-on, you must meet the following prerequisites and considerations.

- [Connected clusters \(p. 574\)](#) can't use this add-on.
- Meet the TLS certificate requirement to ensure end-to-end encryption. The ADOT Operator uses [admission webhooks](#) to mutate and validate the Collector Custom Resource (CR) requests. In Kubernetes, the webhook requires a TLS certificate that the API server is configured to trust. There are multiple ways for you to generate the required TLS certificate. However, the default method is to install the latest version of the [cert-manager](#) manually. The cert-manager generates a self-signed certificate. For more information on installing cert-manager, see [kubectl apply](#) in the cert-manager Documentation.
- If installing an add-on version that is v0.62.1 or earlier, grant permissions to Amazon EKS add-ons to install ADOT.

```
kubectl apply -f https://amazon-eks.s3.amazonaws.com/docs/addons-otel-permissions.yaml
```

Create an IAM role

Each cluster where you [install AWS Distro for OpenTelemetry \(ADOT\) \(p. 551\)](#) must have this role to grant your AWS service account permissions. Do these steps to create and associate your IAM role to your Amazon EKS service account. For more information, see [IAM roles for service accounts \(p. 464\)](#).

1. [Creating an IAM OIDC provider for your cluster \(p. 465\)](#).
2. Create your service account and IAM role. Note the following flags included in this command:
 - For the --name flag, specify the name of the service account you want to create. In this example, it is `adot-collector`.
 - For the --namespace flag, specify the namespace your service account will reside in; for this example you will use the `default` namespace.
 - For the --cluster flag, specify the name of your cluster.
 - Use the --attach-policy-arn parameter to specify the managed IAM policy for the integration you are using to the role. For example, if you are using ADOT Collector to send metric data to CloudWatch, you specify the `CloudWatchAgentServerPolicy` managed policy.
 - The --override-existing-serviceaccounts flag is for a service account already created in the cluster without an IAM role. You can exclude this if the service account does not have an IAM role.

Enter the following command considering the previous notes:

```
eksctl create iamserviceaccount \
--name adot-collector \
--namespace default \
--cluster my-cluster \
--attach-policy-arn arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess \
--attach-policy-arn arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess \
--attach-policy-arn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy \
--approve \
--override-existing-serviceaccounts
```

In the following collector configurations, the `serviceAccount: adot-collector` field to the configuration has been added to use IAM roles for service accounts.

Manage the AWS Distro for OpenTelemetry Operator

The AWS Distro for OpenTelemetry (ADOT) Operator is available as an Amazon EKS add-on. After installing the ADOT Operator, you can configure the ADOT Collector to specify the deployment type and the service that will receive your application metric or trace data. This topic describes how to manage the ADOT add-on.

- [Install the AWS Distro for OpenTelemetry \(ADOT\) Operator \(p. 551\)](#)
- [Update the AWS Distro for OpenTelemetry \(ADOT\) Operator \(p. 552\)](#)
- [Remove the AWS Distro for OpenTelemetry \(ADOT\) Operator \(p. 553\)](#)

To install the ADOT Collector, see [Deploy the AWS Distro for OpenTelemetry Collector \(p. 555\)](#).

Alternatively, with the advanced configuration feature of Amazon EKS add-ons, you can install the ADOT Collector during add-on creation or add-on updates. For more information, see [Deploy the AWS Distro for OpenTelemetry Collector using advanced configuration \(p. 555\)](#).

Install the AWS Distro for OpenTelemetry (ADOT) Operator

Installing the ADOT add-on includes the ADOT Operator, which in turn deploys the ADOT Collector. The ADOT Operator is a custom controller which introduces a new object type called the `OpenTelemetryCollector` through [CustomResourceDefinition \(CRD\)](#). When the ADOT Operator detects the presence of the `OpenTelemetryCollector` resource, then it installs the ADOT Collector.

Prerequisites

- You have met the [ADOT prerequisites \(p. 550\)](#).
- [kubectl is installed \(p. 6\)](#).
- Update your kubeconfig if necessary using the following command.

```
aws eks update-kubeconfig --name my-cluster --region region-code
```

- [eksctl is installed \(p. 13\)](#).
- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with `aws --version | cut -d / -f2 | cut -d ' ' -f1`. Package managers such yum, apt-get, or Homebrew for macOS are often several versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.
- An existing Amazon EKS cluster.
- An existing Amazon EKS service IAM role. If you don't have the role, you can follow [Create an IAM role \(p. 550\)](#) to create one.

AWS Management Console

Install the ADOT Amazon EKS add-on to your Amazon EKS cluster using the following steps:

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. In the left pane, select **Clusters**, and then select the name of your cluster on the **Clusters** page.
3. Choose the **Add-ons** tab.

4. Choose **Get more add-ons**.
5. On the **Select add-ons** page, do the following:
 - a. In the **Amazon EKS-addons** section, select the **AWS Distro for OpenTelemetry** check box.
 - b. Choose **Next**.
6. On the **Configure selected add-ons settings** page, do the following:
 - a. The default version will be selected in the **Version** drop-down. Select the **Version** you'd like to use.
 - b. (Optional) If deploying an ADOT Collector, expand **Optional configuration settings** and provide the **Configuration values** that match your use case for Collector deployment. The **Add-on configuration schema** provides the available options for your configuration values.
 - c. If a service account is already created in the cluster without an IAM role, expand the **Optional configuration settings** and select **Override** for the **Conflict resolution method**.
 - d. Choose **Next**.
7. On the **Review and add** page, choose **Create**. After the add-on installation is complete, you see your installed add-on.

AWS CLI

1. Install the ADOT Amazon EKS add-on to your Amazon EKS cluster. Optionally, the **--configuration-values** flag can be added to deploy an ADOT Collector during add-on installation. You may also configure other available values with this flag.

```
aws eks create-addon --addon-name adot --cluster-name my-cluster --configuration-values my-configuration-values
```

The status field value will be CREATING until complete.

2. Verify that ADOT is installed and running.

```
aws eks describe-addon --addon-name adot --cluster-name my-cluster
```

You'll see "status": "ACTIVE" when creation is complete.

Update the AWS Distro for OpenTelemetry (ADOT) Operator

Amazon EKS does not automatically update ADOT on your cluster. You must initiate the update and then Amazon EKS updates the Amazon EKS add-on for you.

To update the ADOT Amazon EKS add-on using the AWS CLI

1. Check the current version of your ADOT add-on. Replace *my-cluster* with your cluster name.

```
aws eks describe-addon --cluster-name my-cluster --addon-name adot --query "addon.addonVersion" --output text
```

2. Determine the ADOT versions are available that are supported by your cluster's version.

```
aws eks describe-addon-versions --addon-name adot --kubernetes-version 1.23 \
--query "addons[].addonVersions[].[addonVersion, compatibilities[].defaultVersion]" \
--output text
```

An example output is as follows.

```
v0.58.0-eksbuild.1
True
v0.56.0-eksbuild.2
False
```

The version with `True` underneath is the default version deployed when the add-on is created. The version deployed when the add-on is created might not be the latest available version. In the previous output, the latest version is deployed when the add-on is created.

3. Update the ADOT version. Replace `my-cluster` with the name of your cluster and `v0.58.0-eksbuild.1` with the desired version. Optionally, the `--configuration-values` flag can be added to deploy an ADOT Collector during add-on installation. You may also configure other available values with this flag.

```
aws eks update-addon --cluster-name my-cluster --addon-name adot --addon-version v0.58.0-eksbuild.1 --resolve-conflicts PRESERVE --configuration-values my-configuration-values
```

The `PRESERVE` option preserves any custom settings that you've set for the add-on. For more information about other options for this setting, see [update-addon](#) in the Amazon EKS Command Line Reference. For more information about Amazon EKS add-on configuration management, see [Kubernetes field management \(p. 406\)](#).

Remove the AWS Distro for OpenTelemetry (ADOT) Operator

- You must delete the ADOT Collector resource separately from the ADOT Operator. In this command, specify the YAML file that you used to [deploy the ADOT Collector \(p. 555\)](#):

```
kubectl delete -f collector-config-(amp|cloudwatch|xray|advanced).yaml
```

- You can remove the ADOT Operator through either the AWS CLI or eksctl. If you remove the ADOT Operator, you must follow the [installation instructions \(p. 551\)](#) again to reinstall:

CLI

```
aws eks delete-addon --addon-name adot --cluster-name my-cluster
```

eksctl

```
eksctl delete addon --cluster my-cluster --name adot
```

Deploy a sample application to test the AWS Distro for OpenTelemetry Collector

The sample application will generate and send OTLP data to any of the services that you have configured through the AWS Distro for OpenTelemetry ([ADOT Collector deployment \(p. 555\)](#)). This step is optional if you already have an application running inside your cluster that can produce data. Consult your application's documentation to ensure that data is sent to the correct endpoints.

The sample application and traffic generator were largely taken from an example in the [ADOT Collector repository](#). A `docker-compose.yaml` file was translated to Kubernetes resources using the [Kompose tool](#).

To apply the traffic generator and sample application, do the following steps. Make sure that you have satisfied the prerequisites and completed the procedure in [Install the AWS Distro for OpenTelemetry \(ADOT\) Operator \(p. 551\)](#).

1. Download the `traffic-generator.yaml` file to your computer. You can also [view the file](#) on GitHub.

```
curl -0 https://raw.githubusercontent.com/aws-observability/aws-otel-community/master/sample-configs/traffic-generator.yaml
```

2. In `traffic-generator.yaml`, make sure that the second kind value reflects your mode. For more information, see [Deploy the ADOT Collector](#) on GitHub.

```
kind: Deployment
```

`traffic-generator.yaml` makes http calls to the Kubernetes service `sample-app:4567`. This allows the traffic generator to interact with the sample application on port 4567. `sample-app` resolves to the IP address of the `sample-app` Pod.

3. Apply `traffic-generator.yaml` to your cluster.

```
kubectl apply -f traffic-generator.yaml
```

4. Download the `sample-app.yaml` file to your computer. You can also [view the file](#) on GitHub.

```
curl -0 https://raw.githubusercontent.com/aws-observability/aws-otel-community/master/sample-configs/sample-app.yaml
```

5. In `sample-app.yaml`, replace the following with your own AWS Region:

```
value: "<YOUR_AWS_REGION>"
```

The following actions are defined by `sample-app.yaml`:

- The Service resource configures port: 4567 to allow HTTP requests for the traffic generator.
 - The Deployment resource configures some environment variables:
 - The `LISTEN_ADDRESS` is configured to `0.0.0.0:4567` for HTTP requests from the traffic generator.
 - The `OTEL_EXPORTER_OTLP_ENDPOINT` has a value of `http://my-collector-collector:4317`. `my-collector-collector` is the name of the Kubernetes service that allows the sample application to interact with the ADOT Collector on port 4317. In the ADOT Collector configuration, the ADOT Collector receives metrics and traces from an endpoint: `0.0.0.0:4317`.
6. In `sample-app.yaml`, update the value for `OTEL_EXPORTER_OTLP_ENDPOINT` if it doesn't match your collector service name.

For example, X-Ray requires replacing `http://my-collector-collector:4317` with `http://my-collector-xray-collector:4317`.

7. Apply `sample-app.yaml` to your cluster.

```
kubectl apply -f sample-app.yaml
```

Deploy the AWS Distro for OpenTelemetry Collector

Once the [AWS Distro for OpenTelemetry \(ADOT\) Operator is installed \(p. 551\)](#) and running, you can deploy the ADOT Collector into your Amazon EKS cluster. The ADOT Collector can be deployed in one of four modes: Deployment, DaemonSet, StatefulSet, and Sidecar and can be deployed for visibility by an individual service. For more information on these modes, see the ADOT Collector [Deploy the ADOT Collector](#) on GitHub.

You can deploy the ADOT Collector by applying a YAML file to your cluster. You should have already installed the [ADOT Operator \(p. 551\)](#). You can [Create an IAM role \(p. 550\)](#) with your Amazon EKS service account using [IRSA \(p. 464\)](#). By doing this, your service account can provide AWS permissions to the containers you run in any Pod that uses that service account.

We provide ADOT Collector examples for the following services (in deployment modes):

- [Prometheus \(p. 556\)](#)
- [Amazon CloudWatch \(p. 556\)](#)
- [X-Ray \(p. 557\)](#)

Deploy the AWS Distro for OpenTelemetry Collector using advanced configuration

Amazon EKS add-ons provides the ability to configure add-ons during installation time. With this functionality, an ADOT Collector can also be deployed during an installation, provided that add-on version v0.62.1-eksbuild.1 or higher is being used.

For an example list of configurable values Amazon EKS add-ons provides for ADOT for Collector deployment, see [EKS add-ons Advanced Configuration for ADOT: Collector Deployment](#).

An example of how to use Amazon EKS add-ons to install ADOT with a Collector deployment to Amazon Managed [Prometheus](#) can be seen in the steps that follow. Make sure that you have satisfied the prerequisites and completed the procedure in [Install the AWS Distro for OpenTelemetry \(ADOT\) Operator \(p. 551\)](#).

1. Create `configuration-values.json` with the following contents. Replace *example values* with your own.

```
{  
  "collector": {  
    "serviceAccount": {  
      "create": false,  
      "name": "your-irsa-account-name"  
    },  
    "amp": {  
      "enabled": true,  
      "remoteWriteEndpoint": "https://aps-workspaces.region-code.amazonaws.com/  
workspaces/ws-xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx/api/v1/remote_write"  
    }  
  }  
}
```

2. Run the following command. Replace *example values* with your own.

```
aws eks create-addon \  
  --cluster-name my-cluster \  
  ...
```

```
--addon-name adot \
--addon-version add-on-version \
--configuration-values file:///configuration-values.json
```

Note that the collector may take 2 to 3 minutes to create and show up in your cluster.

Deploy the AWS Distro for OpenTelemetry Collector for Amazon Managed Service for Prometheus in deployment mode

The following procedure uses an example YAML file with deployment as the mode value. This is the default mode and deploys the ADOT Collector similarly to a standalone application. This configuration receives OTLP metrics from the sample application and Amazon Managed Service for Prometheus metrics scraped from Pods on the cluster. You can change the mode to Daemonset, StatefulSet, and Sidecar depending on your deployment strategy. For a Daemonset deployment, see [Advanced Collector Configuration for Amazon Managed Prometheus](#) in the ADOT documentation or [click here](#) to download the DaemonSet example.

Make sure that you have satisfied the prerequisites and completed the procedure in [Install the AWS Distro for OpenTelemetry \(ADOT\) Operator \(p. 551\)](#).

1. Download the collector-config-amp.yaml file to your computer. You can also [view the file](#) on GitHub.

```
curl -O https://raw.githubusercontent.com/aws-observability/aws-otel-community/master/
sample-configs/operator/collector-config-amp.yaml
```

2. In collector-config-amp.yaml, replace the following with your own values:
 - mode: *deployment* (for more information, see [Deploy the ADOT Collector](#) on GitHub)
 - serviceAccount: *adot-collector*
 - endpoint: "*<YOUR_REMOTE_WRITE_ENDPOINT>*"
 - region: "*<YOUR_AWS_REGION>*"
 - name: *adot-collector*
3. Apply the YAML file to your cluster to deploy the ADOT Collector:

```
kubectl apply -f collector-config-amp.yaml
```

Deploy the AWS Distro for OpenTelemetry Collector for CloudWatch

The AWS Distro for OpenTelemetry (ADOT) Collector can be deployed to receive OTLP metrics for export to Amazon CloudWatch. This procedure downloads an example YAML file that you can apply to your cluster. Make sure that you have satisfied the prerequisites and completed the procedure in [Install the AWS Distro for OpenTelemetry \(ADOT\) Operator \(p. 551\)](#).

1. Download the collector-config-cloudwatch.yaml file to your computer. You can also [view the file](#) on GitHub.

```
curl -O https://raw.githubusercontent.com/aws-observability/aws-otel-community/master/
sample-configs/operator/collector-config-cloudwatch.yaml
```

2. In `collector-config-cloudwatch.yaml`, replace the following with your own values:
 - mode: *deployment* (for more information, see [Deploy the ADOT Collector on GitHub](#))
 - serviceAccount: *adot-collector*
 - value: *<YOUR_EKS_CLUSTER_NAME>*
 - region: "*<YOUR_AWS_REGION>*"
 - name: *adot-collector*
3. Apply the YAML file to your cluster to deploy the ADOT Collector:

```
kubectl apply -f collector-config-cloudwatch.yaml
```

4. (Optional) Verify the metrics data is being sent to Amazon CloudWatch by opening the [Amazon CloudWatch console](#) and open the **Metrics** menu on the left. Select **All metrics** and click the **AOC Docker Demo/AOC Docker Demo Service** box under **custom namespaces**. You can view any metrics data by selecting any grouping.

Deploy the AWS Distro for OpenTelemetry (ADOT) Collector for X-Ray

You can deploy the AWS Distro for OpenTelemetry (ADOT) Collector to send traces to X-Ray by applying a YAML configuration file. This procedure downloads an example YAML file that you can apply to your cluster. Make sure that you have satisfied the prerequisites and completed the procedure in [Install the AWS Distro for OpenTelemetry \(ADOT\) Operator \(p. 551\)](#).

1. Download the `collector-config-xray.yaml` file to your computer. You can also [view the file](#) on GitHub.

```
curl -O https://raw.githubusercontent.com/aws-observability/aws-otel-community/master/sample-configs/operator/collector-config-xray.yaml
```

2. In `collector-config-xray.yaml`, replace the following with your own values:
 - mode: *deployment* (for more information, see [Deploy the ADOT Collector on GitHub](#))
 - serviceAccount: *adot-collector*
 - region: "*<YOUR_AWS_REGION>*"
3. Apply the YAML file to your cluster to deploy the ADOT Collector:

```
kubectl apply -f collector-config-xray.yaml
```

4. (Optional) Verify trace data is being sent to X-Ray by opening the [X-Ray console](#) and select Traces from the left menu. Your trace data should be present.

Troubleshooting issues in ADOT Amazon EKS add-on

This topic covers some of the common errors that you might encounter while using the AWS Distro for OpenTelemetry (ADOT) Amazon EKS add-on. The topic also includes instructions on how to resolve or workaround the common errors.

```
Error: "code": "AccessDenied", "message":  
"roles.rbac.authorization.k8s.io  
\\"opentelemetry-operator-leader-election-role  
\\" is forbidden: User \\"eks:addon-manager\\"  
cannot patch resource \\"roles\\" in API group  
\\"rbac.authorization.k8s.io\\" in the namespace  
\\"opentelemetry-operator-system\\"
```

You don't have permission to install the ADOT for Amazon EKS add-on. See [Install the AWS Distro for OpenTelemetry \(ADOT\) Operator \(p. 551\)](#). If you have deleted the add-on and are now reinstalling, make sure that you have [applied the required permissions \(p. 550\)](#).

Error: "status": "CREATE_FAILED" or "status": "UPDATE_FAILED"

This can happen due to the following reasons:

- There might be a conflict. You can overwrite conflicts by adding the `--resolve-conflicts=OVERWRITE` flag and running the `create` command again.
- If you're using an add-on version earlier than v0.51.0, you may be on an unsupported architecture, such as arm64. Consult your logs to determine if this is the case. If so, updating your add-on version may resolve this issue because v0.51.0 and later are multi-arch.

Delete add-on error: "status": "DELETE_FAILED"

You can remove Amazon EKS management of the ADOT Operator add-on by adding the `--preserve` flag to your `aws eks delete-addon` command.

AWS services integrated with Amazon EKS

Amazon EKS works with other AWS services to provide additional solutions for your business challenges. This topic identifies services that either use Amazon EKS to add functionality, or services that Amazon EKS uses to perform tasks.

Topics

- [Creating Amazon EKS resources with AWS CloudFormation \(p. 559\)](#)
- [Amazon EKS and AWS Local Zones \(p. 560\)](#)
- [Deep Learning Containers \(p. 560\)](#)
- [Amazon VPC Lattice \(p. 560\)](#)
- [AWS Resilience Hub \(p. 561\)](#)
- [Amazon GuardDuty \(p. 561\)](#)
- [Amazon Detective \(p. 561\)](#)

Creating Amazon EKS resources with AWS CloudFormation

Amazon EKS is integrated with AWS CloudFormation, a service that helps you model and set up your AWS resources so that you can spend less time creating and managing your resources and infrastructure. You create a template that describes all the AWS resources that you want, for example an Amazon EKS cluster, and AWS CloudFormation takes care of provisioning and configuring those resources for you.

When you use AWS CloudFormation, you can reuse your template to set up your Amazon EKS resources consistently and repeatedly. Just describe your resources once, and then provision the same resources over and over in multiple AWS accounts and Regions.

Amazon EKS and AWS CloudFormation templates

To provision and configure resources for Amazon EKS and related services, you must understand [AWS CloudFormation templates](#). Templates are formatted text files in JSON or YAML. These templates describe the resources that you want to provision in your AWS CloudFormation stacks. If you're unfamiliar with JSON or YAML, you can use AWS CloudFormation Designer to help you get started with AWS CloudFormation templates. For more information, see [What is AWS CloudFormation Designer?](#) in the [AWS CloudFormation User Guide](#).

Amazon EKS supports creating clusters and node groups in AWS CloudFormation. For more information, including examples of JSON and YAML templates for your Amazon EKS resources, see [Amazon EKS resource type reference](#) in the [AWS CloudFormation User Guide](#).

Learn more about AWS CloudFormation

To learn more about AWS CloudFormation, see the following resources:

- [AWS CloudFormation](#)
- [AWS CloudFormation User Guide](#)
- [AWS CloudFormation Command Line Interface User Guide](#)

Amazon EKS and AWS Local Zones

An AWS Local Zone is an extension of an AWS Region in geographic proximity to your users. Local Zones have their own connections to the internet and support AWS Direct Connect. Resources created in a Local Zone can serve local users with low-latency communications. For more information, see [Local Zones](#).

Amazon EKS supports certain resources in Local Zones. This includes [self-managed Amazon EC2 nodes \(p. 108\)](#), Amazon EBS volumes, and Application Load Balancers (ALBs). We recommend that you consider the following when using Local Zones as part of your Amazon EKS cluster.

Nodes

You can't create managed node groups or Fargate nodes in Local Zones with Amazon EKS. However, you can create self-managed Amazon EC2 nodes in Local Zones using the Amazon EC2 API, AWS CloudFormation, or eksctl. For more information, see [Self-managed nodes \(p. 108\)](#).

Network architecture

- The Amazon EKS managed Kubernetes control plane always runs in the AWS Region. The Amazon EKS managed Kubernetes control plane can't run in the Local Zone. Because Local Zones appear as a subnet within your VPC, Kubernetes sees your Local Zone resources as part of that subnet.
- The Amazon EKS Kubernetes cluster communicates with the Amazon EC2 instances you run in the AWS Region or Local Zone using Amazon EKS managed [elastic network interfaces](#). To learn more about Amazon EKS networking architecture, see [Amazon EKS networking \(p. 256\)](#).
- Unlike regional subnets, Amazon EKS can't place network interfaces into your Local Zone subnets. This means that you must not specify Local Zone subnets when you create your cluster.

Deep Learning Containers

AWS Deep Learning Containers are a set of Docker images for training and serving models in TensorFlow on Amazon EKS and Amazon Elastic Container Service (Amazon ECS). Deep Learning Containers provide optimized environments with [TensorFlow](#), [NVIDIA CUDA](#) (for GPU instances), and [Intel MKL](#) (for CPU instances) libraries and are available in Amazon ECR.

To get started using AWS Deep Learning Containers on Amazon EKS, see [Amazon EKS Setup](#) in the [AWS Deep Learning Containers Developer Guide](#).

Amazon VPC Lattice

Amazon VPC Lattice is a fully managed application networking service built directly into the AWS networking infrastructure that you can use to connect, secure, and monitor your services across multiple accounts and Virtual Private Clouds (VPCs). With Amazon EKS, you can leverage Amazon VPC Lattice through the use of the AWS Gateway API Controller, an implementation of the Kubernetes [Gateway API](#). Using Amazon VPC Lattice, you can set up cross-cluster connectivity with standard Kubernetes semantics in a simple and consistent manner. To get started using Amazon VPC Lattice with Amazon EKS see the [AWS Gateway API Controller User Guide](#).

AWS Resilience Hub

AWS Resilience Hub assesses the resiliency of an Amazon EKS cluster by analyzing its infrastructure. AWS Resilience Hub uses the Kubernetes role-based access control (RBAC) configuration to assess the Kubernetes workloads deployed to your cluster. For more information, see [Enabling AWS Resilience Hub access to your Amazon EKS cluster](#) in the AWS Resilience Hub User Guide.

Amazon GuardDuty

EKS Protection in Amazon GuardDuty provides threat detection coverage to help you protect Amazon EKS clusters within your AWS environment. EKS Protection includes EKS Audit Log Monitoring and EKS Runtime Monitoring. For more information, see [EKS Protection in Amazon GuardDuty](#) in the Amazon GuardDuty User Guide. You can install the GuardDuty agent to your cluster as an Amazon EKS add-on. For more information, see [the section called "Available Amazon EKS add-ons from Amazon EKS" \(p. 386\)](#).

Amazon Detective

Amazon Detective helps you analyze, investigate, and quickly identify the root cause of security findings or suspicious activities. Detective automatically collects log data from your AWS resources. It then uses machine learning, statistical analysis, and graph theory to generate visualizations that help you to conduct faster and more efficient security investigations. The Detective prebuilt data aggregations, summaries, and context help you to quickly analyze and determine the nature and extent of possible security issues.

Amazon EKS audit logs is an optional data source package that can be added to your Detective behavior graph. You can view the available optional source packages, and their status in your account. For more information, see [Setting up Amazon Detective](#) and [Amazon EKS audit logs for Detective](#) in the Amazon Detective User Guide.

Amazon EKS troubleshooting

This chapter covers some common errors that you may see while using Amazon EKS and how to work around them. If you need to troubleshoot specific Amazon EKS areas, see the separate [the section called "Troubleshooting" \(p. 517\)](#), [the section called "Amazon EKS Connector Troubleshooting" \(p. 581\)](#), and [the section called "Troubleshooting" \(p. 557\)](#) topics.

For other troubleshooting information, see [Knowledge Center content about Amazon Elastic Kubernetes Service](#) on AWS *re:Post*.

Insufficient capacity

If you receive the following error while attempting to create an Amazon EKS cluster, then one of the Availability Zones you specified doesn't have sufficient capacity to support a cluster.

```
Cannot create cluster 'example-cluster' because region-1d, the targeted Availability Zone, does not currently have sufficient capacity to support the cluster. Retry and choose from these Availability Zones: region-1a, region-1b, region-1c
```

Retry creating your cluster with subnets in your cluster VPC that are hosted in the Availability Zones returned by this error message.

Nodes fail to join cluster

There are a few common reasons that prevent nodes from joining the cluster:

- The [aws-auth-cm.yaml \(p. 420\)](#) file doesn't have the correct IAM role ARN for your nodes. Ensure that the node IAM role ARN (not the instance profile ARN) is specified in your aws-auth-cm.yaml file. For more information, see [Launching self-managed Amazon Linux nodes \(p. 108\)](#).
- The **ClusterName** in your node AWS CloudFormation template doesn't exactly match the name of the cluster you want your nodes to join. Passing an incorrect value to this field results in an incorrect configuration of the node's /var/lib/kubelet/kubeconfig file, and the nodes will not join the cluster.
- The node is not tagged as being *owned* by the cluster. Your nodes must have the following tag applied to them, where *my-cluster* is replaced with the name of your cluster.

Key	Value
kubernetes.io/cluster/ <i>my-cluster</i>	owned

- The nodes may not be able to access the cluster using a public IP address. Ensure that nodes deployed in public subnets are assigned a public IP address. If not, you can associate an Elastic IP address to a node after it's launched. For more information, see [Associating an Elastic IP address with a running instance or network interface](#). If the public subnet is not set to automatically assign public IP addresses to instances deployed to it, then we recommend enabling that setting. For more information, see [Modifying the public IPv4 addressing attribute for your subnet](#). If the node is deployed to a private subnet, then the subnet must have a route to a NAT gateway that has a public IP address assigned to it.
- The STS endpoint for the AWS Region that you're deploying the nodes to is not enabled for your account. To enable the region, see [Activating and deactivating AWS STS in an AWS Region](#).

- The worker node doesn't have a private DNS entry, resulting in the kubelet log containing a node "" not found error. Ensure that the VPC where the worker node is created has values set for domain-name and domain-name-servers as Options in a DHCP options set. The default values are domain-name:<region>.compute.internal and domain-name-servers:AmazonProvidedDNS. For more information, see [DHCP options sets](#) in the Amazon VPC User Guide.

To identify and troubleshoot common causes that prevent worker nodes from joining a cluster, you can use the AWSSupport-TroubleshootEKSWorkerNode runbook. For more information, see [AWSSupport-TroubleshootEKSWorkerNode](#) in the *AWS Systems Manager Automation runbook* reference.

Unauthorized or access denied (kubectl)

If you receive one of the following errors while running kubectl commands, then your kubectl is not configured properly for Amazon EKS or the [IAM principal](#) credentials that you're using don't map to a Kubernetes RBAC user with sufficient permissions in your Amazon EKS cluster.

- could not get token: AccessDenied: Access denied
- error: You must be logged in to the server (Unauthorized)
- error: the server doesn't have a resource type "svc"

This could be because the cluster was created with credentials for one IAM principal and kubectl is using credentials for a different IAM principal.

When an Amazon EKS cluster is created, the IAM principal that creates the cluster is added to the Kubernetes RBAC authorization table as the administrator (with system:masters permissions). Initially, only that principal can make calls to the Kubernetes API server using kubectl . For more information, see [Enabling IAM principal access to your cluster \(p. 420\)](#). If you use the console to create the cluster, make sure that the same IAM credentials are in the AWS SDK credential chain when you are running kubectl commands on your cluster.

If you install and configure the AWS CLI, you can configure the IAM credentials you use. For more information, see [Configuring the AWS CLI](#) in the *AWS Command Line Interface User Guide*.

If you assumed a role to create the Amazon EKS cluster, you must ensure that kubectl is configured to assume the same role. Use the following command to update your kubeconfig file to use an IAM role. For more information, see [Creating or updating a kubeconfig file for an Amazon EKS cluster \(p. 431\)](#).

```
aws eks update-kubeconfig \
--region region-code \
--name my-cluster \
--role-arn arn:aws:iam::111122223333:role/role_name
```

To map an [IAM principal](#) to a Kubernetes RBAC user, see [Enabling IAM principal access to your cluster \(p. 420\)](#).

aws-iam-authenticator Not found

If you receive the error "aws-iam-authenticator": executable file not found in \$PATH, then your kubectl is not configured for Amazon EKS. For more information, see [Installing aws-iam-authenticator \(p. 436\)](#).

Note

The aws-iam-authenticator isn't required if you have the AWS CLI version 1.16.156 or higher installed.

hostname doesn't match

Your system's Python version must be 2.7.9 or later. Otherwise, you receive hostname doesn't match errors with AWS CLI calls to Amazon EKS. For more information, see [What are "hostname doesn't match" errors?](#) in the Python Requests FAQ.

getsockopt: no route to host

Docker runs in the 172.17.0.0/16 CIDR range in Amazon EKS clusters. We recommend that your cluster's VPC subnets do not overlap this range. Otherwise, you will receive the following error:

```
Error: : error upgrading connection: error dialing backend: dial tcp  
172.17.<nn>.<nn>:10250: getsockopt: no route to host
```

Instances failed to join the kubernetes cluster

If you receive the error Instances failed to join the kubernetes cluster in the AWS Management Console, ensure that either the cluster's private endpoint access is enabled, or that you have correctly configured CIDR blocks for public endpoint access. For more information, see [Amazon EKS cluster endpoint access control \(p. 41\)](#).

Managed node group error codes

If your managed node group encounters a hardware health issue, Amazon EKS returns an error code to help you to diagnose the issue. These health checks don't detect software issues because they are based on [Amazon EC2 health checks](#). The following list describes the error codes.

AccessDenied

Amazon EKS or one or more of your managed nodes is failing to authenticate or authorize with your Kubernetes cluster API server. For more information about resolving a common cause, see [Fixing a common cause of AccessDenied errors for managed node groups \(p. 566\)](#). Private Windows AMIs can also cause this error code alongside the Not authorized for images error message. For more information, see [Not authorized for images \(p. 568\)](#).

AmildNotFound

We couldn't find the AMI ID associated with your launch template. Make sure that the AMI exists and is shared with your account.

AutoScalingGroupNotFound

We couldn't find the Auto Scaling group associated with the managed node group. You may be able to recreate an Auto Scaling group with the same settings to recover.

ClusterUnreachable

Amazon EKS or one or more of your managed nodes is unable to communicate with your Kubernetes cluster API server. This can happen if there are network disruptions or if API servers are timing out processing requests.

Ec2SecurityGroupNotFound

We couldn't find the cluster security group for the cluster. You must recreate your cluster.

Ec2SecurityGroupDeletionFailure

We could not delete the remote access security group for your managed node group. Remove any dependencies from the security group.

Ec2LaunchTemplateNotFound

We couldn't find the Amazon EC2 launch template for your managed node group. You must recreate your node group to recover.

Ec2LaunchTemplateVersionMismatch

The Amazon EC2 launch template version for your managed node group doesn't match the version that Amazon EKS created. You may be able to revert to the version that Amazon EKS created to recover.

IamInstanceProfileNotFound

We couldn't find the IAM instance profile for your managed node group. You may be able to recreate an instance profile with the same settings to recover.

IamNodeRoleNotFound

We couldn't find the IAM role for your managed node group. You may be able to recreate an IAM role with the same settings to recover.

AsgInstanceLaunchFailures

Your Auto Scaling group is experiencing failures while attempting to launch instances.

NodeCreationFailure

Your launched instances are unable to register with your Amazon EKS cluster. Common causes of this failure are insufficient [node IAM role \(p. 501\)](#) permissions or lack of outbound internet access for the nodes. Your nodes must meet either of the following requirements:

- Able to access the internet using a public IP address. The security group associated to the subnet the node is in must allow the communication. For more information, see [the section called "Subnet requirements and considerations" \(p. 257\)](#) and [the section called "Security group requirements" \(p. 263\)](#).
- Your nodes and VPC must meet the requirements in [the section called "Private cluster requirements" \(p. 58\)](#).

InstanceLimitExceeded

Your AWS account is unable to launch any more instances of the specified instance type. You may be able to request an Amazon EC2 instance limit increase to recover.

InsufficientFreeAddresses

One or more of the subnets associated with your managed node group doesn't have enough available IP addresses for new nodes.

InternalFailure

These errors are usually caused by an Amazon EKS server-side issue.

Fixing a common cause of AccessDenied errors for managed node groups

The most common cause of AccessDenied errors when performing operations on managed node groups is missing the eks:node-manager ClusterRole or ClusterRoleBinding. Amazon EKS sets up these resources in your cluster as part of onboarding with managed node groups, and these are required for managing the node groups.

The ClusterRole may change over time, but it should look similar to the following example:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: eks:node-manager
rules:
- apiGroups:
  - ''
    resources:
    - pods
    verbs:
    - get
    - list
    - watch
    - delete
- apiGroups:
  - ''
    resources:
    - nodes
    verbs:
    - get
    - list
    - watch
    - patch
- apiGroups:
  - ''
    resources:
    - pods/eviction
    verbs:
    - create
```

The ClusterRoleBinding may change over time, but it should look similar to the following example:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: eks:node-manager
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: eks:node-manager
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: eks:node-manager
```

Verify that the eks:node-manager ClusterRole exists.

```
kubectl describe clusterrole eks:node-manager
```

If present, compare the output to the previous ClusterRole example.

Verify that the eks:node-manager ClusterRoleBinding exists.

```
kubectl describe clusterrolebinding eks:node-manager
```

If present, compare the output to the previous ClusterRoleBinding example.

If you've identified a missing or broken ClusterRole or ClusterRoleBinding as the cause of an AccessDenied error while requesting managed node group operations, you can restore them. Save the following contents to a file named *eks-node-manager-role.yaml*.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: eks:node-manager
rules:
- apiGroups:
  - ''
    resources:
    - pods
    verbs:
    - get
    - list
    - watch
    - delete
- apiGroups:
  - ''
    resources:
    - nodes
    verbs:
    - get
    - list
    - watch
    - patch
- apiGroups:
  - ''
    resources:
    - pods/eviction
    verbs:
    - create
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: eks:node-manager
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: eks:node-manager
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: eks:node-manager
```

Apply the file.

```
kubectl apply -f eks-node-manager-role.yaml
```

Retry the node group operation to see if that resolved your issue.

Not authorized for images

One potential cause of a Not authorized for images error message is using a private Amazon EKS Windows AMI to launch Windows managed node groups. After releasing new Windows AMIs, AWS makes Windows AMIs that are older than three months private within 10 days. If your managed node group is using a private Amazon EKS Windows AMI, consider [updating your Windows managed node group](#). For more information, see [Patches, security updates, and AMI IDs](#) in the *Amazon EC2 User Guide for Windows Instances*.

CNI log collection tool

The Amazon VPC CNI plugin for Kubernetes has its own troubleshooting script that is available on nodes at `/opt/cni/bin/aws-cni-support.sh`. You can use the script to collect diagnostic logs for support cases and general troubleshooting.

Use the following command to run the script on your node:

```
sudo bash /opt/cni/bin/aws-cni-support.sh
```

Note

If the script is not present at that location, then the CNI container failed to run. You can manually download and run the script with the following command:

```
curl -O https://raw.githubusercontent.com/awslabs/amazon-eks-ami/master/log-
collector-script/linux/eks-log-collector.sh
sudo bash eks-log-collector.sh
```

The script collects the following diagnostic information. The CNI version that you have deployed can be earlier than the script version.

```
This is version 0.6.1. New versions can be found at https://github.com/awslabs/
amazon-eks-ami

Trying to collect common operating system logs...
Trying to collect kernel logs...
Trying to collect mount points and volume information...
Trying to collect SELinux status...
Trying to collect iptables information...
Trying to collect installed packages...
Trying to collect active system services...
Trying to collect Docker daemon information...
Trying to collect kubelet information...
Trying to collect L-IPAMD information...
Trying to collect sysctls information...
Trying to collect networking information...
Trying to collect CNI configuration information...
Trying to collect running Docker containers and gather container data...
Trying to collect Docker daemon logs...
Trying to archive gathered information...

Done... your bundled logs are located in /var/log/eks_i-0717c9d54b6cf1a19_2020-03-24_0103-
UTC_0.6.1.tar.gz
```

The diagnostic information is collected and stored at:

```
/var/log/eks_i-0717c9d54b6cf1a19_2020-03-24_0103-UTC_0.6.1.tar.gz
```

Container runtime network not ready

You may receive a `Container runtime network not ready` error and authorization errors similar to the following:

```
4191 kubelet.go:2130] Container runtime network not ready: NetworkReady=false
  reason:NetworkPluginNotReady message:docker: network plugin is not ready: cni config
  uninitialized
4191 reflector.go:205] k8s.io/kubernetes/pkg/kubelet/kubelet.go:452: Failed to list
  *v1.Service: Unauthorized
4191 kubelet_node_status.go:106] Unable to register node "ip-10-40-175-122.ec2.internal"
  with API server: Unauthorized
4191 reflector.go:205] k8s.io/kubernetes/pkg/kubelet/kubelet.go:452: Failed to list
  *v1.Service: Unauthorized
```

The errors are most likely because the AWS IAM Authenticator (`aws-auth`) configuration map isn't applied to the cluster. The configuration map provides the `system:bootstrappers` and `system:nodes` Kubernetes RBAC permissions for nodes to register to the cluster. To apply the configuration map to your cluster, see [Apply the `aws-authConfigMap` to your cluster \(p. 426\)](#).

The authenticator doesn't recognize a **Role ARN** if it includes a path other than `/`, such as the following example:

```
arn:aws:iam::111122223333:role/development/apps/prod-iam-role-NodeInstanceRole-621LVEXAMPLE
```

When specifying a **Role ARN** in the configuration map that includes a path other than `/`, you must drop the path. The previous ARN should be specified as the following:

```
arn:aws:iam::111122223333:role/prod-iam-role-NodeInstanceRole-621LVEXAMPLE
```

TLS handshake timeout

When a node is unable to establish a connection to the public API server endpoint, you may see an error similar to the following error.

```
server.go:233] failed to run Kubelet: could not init cloud provider "aws": error finding
instance i-1111f222f333e44c: "error listing AWS instances: \"RequestError: send request
failed\\ncaused by: Post net/http: TLS handshake timeout\""
```

The `kubelet` process will continually respawn and test the API server endpoint. The error can also occur temporarily during any procedure that performs a rolling update of the cluster in the control plane, such as a configuration change or version update.

To resolve the issue, check the route table and security groups to ensure that traffic from the nodes can reach the public endpoint.

InvalidClientTokenId

If you're using IAM roles for service accounts for a Pod or DaemonSet deployed to a cluster in a China AWS Region, and haven't set the `AWS_DEFAULT_REGION` environment variable in the spec, the Pod or DaemonSet may receive the following error:

An error occurred (InvalidClientTokenId) when calling the GetCallerIdentity operation: The security token included in the request is invalid

To resolve the issue, you need to add the AWS_DEFAULT_REGION environment variable to your Pod or DaemonSet spec, as shown in the following example Pod spec.

```
apiVersion: v1
kind: Pod
metadata:
  name: envar-demo
  labels:
    purpose: demonstrate-envvars
spec:
  containers:
    - name: envar-demo-container
      image: gcr.io/google-samples/node-hello:1.0
      env:
        - name: AWS_DEFAULT_REGION
          value: "region-code"
```

VPC admission webhook certificate expiration

If the certificate used to sign the VPC admission webhook expires, the status for new Windows Pod deployments stays at ContainerCreating.

To resolve the issue if you have legacy Windows support on your data plane, see [the section called "Renew VPC admission webhook certificate" \(p. 56\)](#). If your cluster and platform version are later than a version listed in the [Windows support prerequisites \(p. 50\)](#), then we recommend that you remove legacy Windows support on your data plane and enable it for your control plane. Once you do, you don't need to manage the webhook certificate. For more information, see [Enabling Windows support for your Amazon EKS cluster \(p. 49\)](#).

Node groups must match Kubernetes version before updating control plane

Before you update a control plane to a new Kubernetes version, the minor version of the managed and Fargate nodes in your cluster must be the same as the version of your control plane's current version. The EKS update-cluster-version API rejects requests until you update all EKS managed nodes to the current cluster version. EKS provides APIs to update managed nodes. For information on updating managed node group Kubernetes versions, see [Updating a managed node group \(p. 91\)](#). To update the version of a Fargate node, delete the Pod that's represented by the node and redeploy the Pod after you update your control plane. For more information, see [Updating an Amazon EKS cluster Kubernetes version \(p. 34\)](#).

When launching many nodes, there are Too Many Requests errors

If you launch many nodes simultaneously, you may see an error message in the [Amazon EC2 user data](#) execution logs that says Too Many Requests. This can occur because the control plane is being

overloaded with `describeCluster` calls. The overloading results in throttling, nodes failing to run the bootstrap script, and nodes failing to join the cluster altogether.

Make sure that `--apiserver-endpoint`, `--b64-cluster-ca`, and `--dns-cluster-ip` arguments are being passed to the worker node bootstrap script. When including these arguments, there's no need for the bootstrap script to make a `describeCluster` call, which helps prevent the control plane from being overloaded. For more information, see [Provide user data to pass arguments to the bootstrap.sh file included with an Amazon EKS optimized Linux/Bottlerocket AMI \(p. 102\)](#).

HTTP 401 unauthorized error response on Kubernetes API server requests

You see these errors if a Pod's service account token has expired on a cluster.

Your Amazon EKS cluster's Kubernetes API server rejects requests with tokens older than 90 days. In previous Kubernetes versions, tokens did not have an expiration. This means that clients that rely on these tokens must refresh them within an hour. To prevent the Kubernetes API server from rejecting your request due to an invalid token, the [Kubernetes client SDK](#) version used by your workload must be the same, or later than the following versions:

- Go version `0.15.7` and later
- Python version `12.0.0` and later
- Java version `9.0.0` and later
- JavaScript version `0.10.3` and later
- Ruby master branch
- Haskell version `0.3.0.0`
- C# version `7.0.5` and later

You can identify all existing Pods in your cluster that are using stale tokens. For more information, see [Kubernetes service accounts \(p. 463\)](#).

Amazon EKS platform version is more than two versions behind the current platform version

This can happen when Amazon EKS isn't able to automatically update your cluster's [platform version \(p. 71\)](#). Though there are many causes for this, some of the common causes follow. If any of these problems apply to your cluster, it may still function, its platform version just won't be updated by Amazon EKS.

Problem

The [cluster IAM role \(p. 499\)](#) was deleted – This role was specified when the cluster was created. You can see which role was specified with the following command. Replace `my-cluster` with the name of your cluster.

```
aws eks describe-cluster --name my-cluster --query cluster.roleArn --output text | cut -d / -f 2
```

An example output is as follows.

```
eksClusterRole
```

Solution

Create a new [cluster IAM role \(p. 499\)](#) with the same name.

Problem

A subnet specified during cluster creation was deleted – The subnets to use with the cluster were specified during cluster creation. You can see which subnets were specified with the following command. Replace *my-cluster* with the name of your cluster.

```
aws eks describe-cluster --name my-cluster --query cluster.resourcesVpcConfig.subnetIds
```

An example output is as follows.

```
[  
"subnet-EXAMPLE1",  
"subnet-EXAMPLE2"  
]
```

Solution

Confirm whether the subnet IDs exist in your account.

```
vpc_id=$(aws eks describe-cluster --name my-cluster --query  
cluster.resourcesVpcConfig.vpcId --output text)  
aws ec2 describe-subnets --filters "Name=vpc-id,Values=$vpc_id" --query  
"Subnets[*].SubnetId"
```

An example output is as follows.

```
[  
"subnet-EXAMPLE3",  
"subnet-EXAMPLE4"  
]
```

If the subnet IDs returned in the output don't match the subnet IDs that were specified when the cluster was created, then if you want Amazon EKS to update the cluster, you might need to create a new cluster. This is because if you specified more than two subnets when you created your cluster, Amazon EKS randomly selects subnets that you specified to create new elastic network interfaces in. These network interfaces enable the control plane to communicate with your nodes. Amazon EKS won't update the cluster if the subnet it selects doesn't exist. You have no control over which of the subnets that you specified at cluster creation that Amazon EKS chooses to create a new network interface in. You can't create new subnets for your cluster to use after cluster creation.

When you initiate a Kubernetes version update for your cluster, the update can fail for the same reason.

Problem

A security group specified during cluster creation was deleted – If you specified security groups during cluster creation, you can see their IDs with the following command. Replace *my-cluster* with the name of your cluster.

```
aws eks describe-cluster --name my-cluster --query  
cluster.resourcesVpcConfig.securityGroupIds
```

An example output is as follows.

```
[  
    "sg-EXAMPLE1"  
]
```

If [] is returned, then no security groups were specified when the cluster was created and a missing security group isn't the problem. If security groups are returned, then confirm that the security groups exist in your account.

Solution

Confirm whether these security groups exist in your account.

```
vpc_id=$(aws eks describe-cluster --name my-cluster --query  
    cluster.resourcesVpcConfig.vpcId --output text)  
aws ec2 describe-security-groups --filters "Name=vpc-id,Values=$vpc_id" --query  
    "SecurityGroups[*].GroupId"
```

An example output is as follows.

```
[  
    "sg-EXAMPLE2"  
]
```

If the security group IDs returned in the output don't match the security group IDs that were specified when the cluster was created, then if you want Amazon EKS to update the cluster, you need to create a new cluster. Amazon EKS won't update a cluster if the security group IDs specified at cluster creation don't exist. You can't specify different security groups after cluster creation.

When you initiate a Kubernetes version update for your cluster, the update can fail for the same reason.

Other reasons that Amazon EKS doesn't update the platform version of your cluster

- You don't have at least six (though we recommend 16) available IP addresses in each of the subnets that you specified when you created your cluster. If you don't have enough available IP addresses in the subnet, you either need to free up IP addresses in the subnet or you need to create a new cluster that uses subnets with enough available IP addresses.
- You enabled [secrets encryption \(p. 46\)](#) when you created your cluster and the AWS KMS key that you specified has been deleted. If you want Amazon EKS to update the cluster, you need to create a new cluster

Amazon EKS Connector

You can use Amazon EKS Connector to register and connect any conformant Kubernetes cluster to AWS and visualize it in the Amazon EKS console. After a cluster is connected, you can see the status, configuration, and workloads for that cluster in the Amazon EKS console. You can use this feature to view connected clusters in Amazon EKS console, but you can't manage them. The Amazon EKS Connector requires an agent that is an [open source project on Github](#). For additional technical content, including frequently asked questions and troubleshooting, see [Troubleshooting issues in Amazon EKS Connector \(p. 581\)](#).

The Amazon EKS Connector can connect the following types of Kubernetes clusters to Amazon EKS.

- On-premises Kubernetes clusters
- Self-managed clusters that are running on Amazon EC2
- Managed clusters from other cloud providers

Amazon EKS Connector considerations

Before you use Amazon EKS Connector, understand the following:

- You must have administrative privileges to the Kubernetes cluster to connect the cluster to Amazon EKS.
- The Kubernetes cluster must have Linux 64-bit (x86) worker nodes present before connecting. ARM worker nodes aren't supported.
- You must have worker nodes in your Kubernetes cluster that have outbound access to the `ssm.` and `ssmmessages.` Systems Manager endpoints. For more information, see [Systems Manager endpoints](#) in the *AWS General Reference*.
- By default, you can connect up to 10 clusters in a Region. You can request an increase through the [service quota console](#). See [Requesting a quota increase](#) for more information.
- Only the Amazon EKS `RegisterCluster`, `ListClusters`, `DescribeCluster`, and `DeregisterCluster` APIs are supported for external Kubernetes clusters.
- You must have the following permissions to register a cluster:
 - `eks:RegisterCluster`
 - `ssm>CreateActivation`
 - `ssm>DeleteActivation`
 - `iam:PassRole`
- You must have the following permissions to deregister a cluster:
 - `eks:DeregisterCluster`
 - `ssm>DeleteActivation`
 - `ssm:DeregisterManagedInstance`

Required IAM roles for Amazon EKS Connector

Using the Amazon EKS Connector requires the following two IAM roles:

- The [Amazon EKS Connector \(p. 496\)](#) service-linked role is created when you register a cluster for the first time.
- You must create the Amazon EKS Connector agent IAM role. See [Amazon EKS connector IAM role \(p. 508\)](#) for details.

To enable cluster and workload view permission for [IAM principals](#), apply the `eks-connector` and Amazon EKS Connector cluster roles to your cluster. Follow the steps in [Granting access to an IAM principal to view Kubernetes resources on a cluster \(p. 579\)](#).

Connecting an external cluster

You can connect an external Kubernetes cluster to Amazon EKS by using multiple methods in the following process. This process involves two steps: Registering the cluster with Amazon EKS and installing the `eks-connector` agent in the cluster.

Important

You must complete the second step within 3 days of completing the first step, before the registration expires.

Connector methods

Not all of the methods to install the agent can be used after each of the methods to register the cluster. The following table lists each of the registration method and which methods for installing the agent can be used.

Step	Methods		
Register the cluster	AWS Management Console	AWS Command Line Interface	<code>eksctl</code>
Install the agent	Helm, YAML manifests	Helm, YAML manifests	YAML manifests

Prerequisites

- Ensure the Amazon EKS Connector agent role was created. Follow the steps in [Creating the Amazon EKS connector agent role \(p. 508\)](#).
- You must have the following permissions to register a cluster:
 - `eks:RegisterCluster`
 - `ssm>CreateActivation`
 - `ssm>DeleteActivation`
 - `iam:PassRole`

Step 1: Registering the cluster

AWS CLI

Prerequisites

- AWS CLI must be installed. To install or upgrade it, see [Installing the AWS CLI](#).

To register your cluster with the AWS CLI

- For the Connector configuration, specify your Amazon EKS Connector agent IAM role. For more information, see [Required IAM roles for Amazon EKS Connector \(p. 574\)](#).

```
aws eks register-cluster \
    --name my-first-registered-cluster \
    --connector-config roleArn=arn:aws:iam::111122223333:role/AmazonEKSConnectorAgentRole,provider="OTHER" \
    --region aws-region
```

An example output is as follows.

```
{  
  "cluster": {  
    "name": "my-first-registered-cluster",  
    "arn": "arn:aws:eks:region:111122223333:cluster/my-first-registered-cluster",  
    "createdAt": 1627669203.531,  
    "ConnectorConfig": {  
      "activationId": "xxxxxxxxACTIVATION_IDxxxxxxxx",  
      "activationCode": "xxxxxxxxACTIVATION_CODExxxxxxxx",  
      "activationExpiry": 1627672543.0,  
      "provider": "OTHER",  
      "roleArn": "arn:aws:iam::111122223333:role/AmazonEKSConnectorAgentRole"  
    },  
    "status": "CREATING"  
  }  
}
```

You use the `aws-region`, `activationId`, and `activationCode` values in the next step.

AWS Management Console

To register your Kubernetes cluster with the console.

- Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
- Choose **Add cluster** and select **Register** to bring up the configuration page.
- On the **Configure cluster** section, fill in the following fields:
 - Name** – A unique name for your cluster.
 - Provider** – Choose to display the dropdown list of Kubernetes cluster providers. If you don't know the specific provider, select **Other**.
 - EKS Connector role** – Select the role to use for connecting the cluster.
- Select **Register cluster**.
- The Cluster overview page displays. If you want to use the Helm chart, copy the `helm install` command and continue to the next step. If you want to use the YAML manifest, choose **Download YAML file** to download the manifest file to your local drive.

Important

- This is your only opportunity to copy the `helm install` command or download this file. Don't navigate away from this page, as the link will not be accessible and you must deregister the cluster and start the steps from the beginning.
- The command or manifest file can be used only once for the registered cluster. If you delete resources from the Kubernetes cluster, you must re-register the cluster and obtain a new manifest file.

Continue to the next step to apply the manifest file to your Kubernetes cluster.

eksctl

Prerequisites

- eksctl version 0.68 or later must be installed. To install or upgrade it, see [Getting started with Amazon EKS – eksctl \(p. 13\)](#).

To register your cluster with eksctl

- Register the cluster by providing a name, provider, and region.

```
eksctl register cluster --name my-cluster --provider my-provider --region region-code
```

Example output:

```
2021-08-19 13:47:26 [#] creating IAM role "eksctl-20210819194112186040"
2021-08-19 13:47:26 [#] registered cluster "<name>" successfully
2021-08-19 13:47:26 [#] wrote file eks-connector.yaml to <current directory>
2021-08-19 13:47:26 [#] wrote file eks-connector-clusterrole.yaml to <current directory>
2021-08-19 13:47:26 [#] wrote file eks-connector-console-dashboard-full-access-group.yaml to <current directory>
2021-08-19 13:47:26 [!] note: "eks-connector-clusterrole.yaml" and "eks-connector-console-dashboard-full-access-group.yaml" give full EKS Console access to IAM identity "<aws-arn>", edit if required; read https://eksctl.io/usage/eks-connector for more info
2021-08-19 13:47:26 [#] run `kubectl apply -f eks-connector.yaml,eks-connector-clusterrole.yaml,eks-connector-console-dashboard-full-access-group.yaml` before expiry> to connect the cluster
```

This creates files on your local computer. These files must be applied to the external cluster within 3 days, or the registration expires.

- In a terminal that can access the cluster, apply the eks-connector-binding.yaml file:

```
kubectl apply -f eks-connector-binding.yaml
```

Step 2: Installing the eks-connector agent

Helm chart

- If you used the AWS CLI in the previous step, replace the ACTIVATION_CODE and ACTIVATION_ID in the following command with the activationId, and activationCode values respectively. Replace the aws-region with the AWS Region that you used in the previous step. Then run the command to install the eks-connector agent on the registering cluster:

```
$ helm install eks-connector \
--namespace eks-connector \
```

```
oci://public.ecr.aws/eks-connector/eks-connector-chart \
--set eks.activationCode=ACTIVATION_CODE \
--set eks.activationId=ACTIVATION_ID \
--set eks.agentRegion=aws-region
```

If you used the AWS Management Console in the previous step, use the command that you copied from the previous step that has these values filled in.

2. Check the healthiness of the installed eks-connector deployment and wait for the status of the registered cluster in Amazon EKS to be ACTIVE.

YAML manifest

Complete the connection by applying the Amazon EKS Connector manifest file to your Kubernetes cluster. To do this, you must use the methods described previously. If the manifest isn't applied within three days, the Amazon EKS Connector registration expires. If the cluster connection expires, the cluster must be deregistered before connecting the cluster again.

1. Download the Amazon EKS Connector YAML file.

```
curl -O https://amazon-eks.s3.us-west-2.amazonaws.com/eks-connector/manifests/eks-
connector/latest/eks-connector.yaml
```

2. Edit the Amazon EKS Connector YAML file to replace all references of %AWS_REGION%, %EKS_ACTIVATION_ID%, %EKS_ACTIVATION_CODE% with the aws-region, activationId, and activationCode from the output of the previous step.

The following example command can replace these values.

```
sed -i "s~%AWS_REGION%~$aws-region~g; s~%EKS_ACTIVATION_ID%~$EKS_ACTIVATION_ID~g;
s~%EKS_ACTIVATION_CODE%~$(echo -n $EKS_ACTIVATION_CODE | base64)~g" eks-
connector.yaml
```

Important

Ensure that your activation code is in the base64 format.

3. In a terminal that can access the cluster, you can apply the updated manifest file by running the following command:

```
kubectl apply -f eks-connector.yaml
```

4. After the Amazon EKS Connector manifest and role binding YAML files are applied to your Kubernetes cluster, confirm that the cluster is now connected.

```
aws eks describe-cluster \
--name "my-first-registered-cluster" \
--region AWS_REGION
```

The output should include status=ACTIVE.

5. (Optional) Add tags to your cluster. For more information, see [Tagging your Amazon EKS resources \(p. 451\)](#).

Next steps

If you have any issues with these steps, see [Troubleshooting issues in Amazon EKS Connector \(p. 581\)](#).

To grant additional [IAM principals](#) access to the Amazon EKS console to view Kubernetes resources in a connected cluster, see [Granting access to an IAM principal to view Kubernetes resources on a cluster \(p. 579\)](#).

Granting access to an IAM principal to view Kubernetes resources on a cluster

Grant [IAM principals](#) access to the Amazon EKS console to view information about Kubernetes resources running on your connected cluster.

Prerequisites

The [IAM principal](#) that you use to access the AWS Management Console must meet the following requirements:

- It must have the `eks:AccessKubernetesApi` IAM permission.
- The Amazon EKS Connector service account can impersonate the IAM principal in the cluster. This allows the Amazon EKS Connector to map the IAM principal to a Kubernetes user.

To create and apply the Amazon EKS Connector cluster role

1. Download the `eks-connector` cluster role template.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/eks-connector/manifests/eks-  
connector-console-roles/eks-connector-clusterrole.yaml
```

2. Edit the cluster role template YAML file. Replace references of `%IAM_ARN%` with the Amazon Resource Name (ARN) of your IAM principal.
3. Apply the Amazon EKS Connector cluster role YAML to your Kubernetes cluster.

```
kubectl apply -f eks-connector-clusterrole.yaml
```

For an IAM principal to view Kubernetes resources in Amazon EKS console, the principal must be associated with a Kubernetes `role` or `clusterrole` with necessary permissions to read the resources. For more information, see [Using RBAC Authorization](#) in the Kubernetes documentation.

To configure an IAM principal to access the connected cluster

1. You can download either of these example manifest files to create a `clusterrole` and `clusterrolebinding` or a `role` and `rolebinding`, respectively:

View Kubernetes resources in all namespaces

The `eks-connector-console-dashboard-full-access-clusterrole` cluster role gives access to all namespaces and resources that can be visualized in the console. You can change the name of the `role`, `clusterrole` and their corresponding binding before applying it to your cluster. Use the following command to download a sample file.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/eks-connector/manifests/eks-  
connector-console-roles/eks-connector-console-dashboard-full-access-group.yaml
```

View Kubernetes resources in a specific namespace

The namespace in this file is default, so if you want to specify a different namespace, edit the file before applying it to your cluster. Use the following command to download a sample file.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/eks-connector/manifests/  
eks-connector-console-roles/eks-connector-console-dashboard-restricted-access-  
group.yaml
```

2. Edit the full access or restricted access YAML file to replace references of %IAM_ARN% with the Amazon Resource Name (ARN) of your IAM principal.
3. Apply the full access or restricted access YAML files to your Kubernetes cluster. Replace the YAML file value with your own.

```
kubectl apply -f eks-connector-console-dashboard-full-access-group.yaml
```

To view Kubernetes resources in your connected cluster, see [View Kubernetes resources \(p. 529\)](#). Data for some resource types on the **Resources** tab isn't available for connected clusters.

Deregistering a cluster

If you are finished using a connected cluster, you can deregister it. After it's deregistered, the cluster is no longer visible in the Amazon EKS console.

You must have the following permissions to call the `deregisterCluster` API:

- `eks:DeregisterCluster`
- `ssm>DeleteActivation`
- `ssm:DeregisterManagedInstance`

This process involves two steps: Deregistering the cluster with Amazon EKS and uninstalling the `eks-connector` agent in the cluster.

To deregister the Kubernetes cluster

AWS CLI

Prerequisites

- AWS CLI must be installed. To install or upgrade it, see [Installing the AWS CLI](#).
- Ensure the Amazon EKS Connector agent role was created. .

Deregister the connected cluster.

```
aws eks deregister-cluster \  
  --name my-cluster \  
  --region region-code
```

AWS Management Console

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose **Clusters**.

3. On the **Clusters** page, select the connected cluster and select **Deregister**.
4. Confirm that you want to deregister the cluster.

eksctl

Prerequisites

- eksctl version 0.68 or later must be installed. To install or upgrade it, see [Getting started with Amazon EKS – eksctl \(p. 13\)](#).
- Ensure the Amazon EKS Connector agent role was created. .

To deregister your cluster with eksctl

- For the Connector configuration, specify your Amazon EKS Connector agent IAM role. For more information, see [Required IAM roles for Amazon EKS Connector \(p. 574\)](#).

```
eksctl deregister cluster --name my-cluster
```

To clean up the resources in your Kubernetes cluster

Helm

- Run the following command to uninstall the agent.

```
helm -n eks-connector uninstall eks-connector
```

YAML manifest

1. Delete the Amazon EKS Connector YAML file from your Kubernetes cluster.

```
kubectl delete -f eks-connector.yaml
```

2. If you created clusterrole or clusterrolebindings for additional [IAM principals](#) to access the cluster, delete them from your Kubernetes cluster.

Troubleshooting issues in Amazon EKS Connector

This topic covers some of the common errors that you might encounter while using the Amazon EKS Connector, including instructions on how to resolve them and workarounds.

Basic troubleshooting

This section describes steps to diagnose the issue if it's unclear.

Check Amazon EKS Connector status

Check the Amazon EKS Connector status.

```
kubectl get pods -n eks-connector
```

Inspect Amazon EKS Connector logs

The Amazon EKS Connector Pod consists of three containers. To retrieve full logs for all of these containers so that you can inspect them, run the following commands:

- connector-init

```
kubectl logs eks-connector-0 --container connector-init -n eks-connector
kubectl logs eks-connector-1 --container connector-init -n eks-connector
```

- connector-proxy

```
kubectl logs eks-connector-0 --container connector-proxy -n eks-connector
kubectl logs eks-connector-1 --container connector-proxy -n eks-connector
```

- connector-agent

```
kubectl exec eks-connector-0 --container connector-agent -n eks-connector -- cat /var/
log/amazon/ssm/amazon-ssm-agent.log
kubectl exec eks-connector-1 --container connector-agent -n eks-connector -- cat /var/
log/amazon/ssm/amazon-ssm-agent.log
```

Get the effective cluster name

Amazon EKS clusters are uniquely identified by `clusterName` within a single AWS account and AWS Region. If you have multiple connected clusters in Amazon EKS, you can confirm which Amazon EKS cluster that the current Kubernetes cluster is registered to. To do this, enter the following to find out the `clusterName` of the current cluster.

```
kubectl exec eks-connector-0 --container connector-agent -n eks-connector \
-- cat /var/log/amazon/ssm/amazon-ssm-agent.log | grep -m1 -oE "eks_c:[a-zA-Z0-9_-]+" |
sed -E "s/^.*eks_c:([a-zA-Z0-9_-]+)_([a-zA-Z0-9]+).*$/\1/"
kubectl exec eks-connector-1 --container connector-agent -n eks-connector \
-- cat /var/log/amazon/ssm/amazon-ssm-agent.log | grep -m1 -oE "eks_c:[a-zA-Z0-9_-]+" |
sed -E "s/^.*eks_c:([a-zA-Z0-9_-]+)_([a-zA-Z0-9]+).*$/\1/"
```

Miscellaneous commands

The following commands are useful to retrieve information that you need to troubleshoot issues.

- Use the following command to gather images that's used by Pods in Amazon EKS Connector.

```
kubectl get pods -n eks-connector -o jsonpath=".items[*].spec.containers[*].image" | tr
-s '[[[:space:]]]' '\n'
```

- Use the following command to determine the node names that Amazon EKS Connector is running on.

```
kubectl get pods -n eks-connector -o jsonpath=".items[*].spec.nodeName" | tr -s
'[[[:space:]]]' '\n'
```

- Run the following command to get your Kubernetes client and server versions.

```
kubectl version
```

- Run the following command to get information about your nodes.

```
kubectl get nodes -o wide --show-labels
```

Helm issue: 403 Forbidden

If you received the following error when running helm install commands:

```
Error: INSTALLATION FAILED: unexpected status from HEAD request to https://public.ecr.aws/v2/eks-connector/eks-connector-chart/manifests/0.0.6: 403 Forbidden
```

You can run the following line to fix it:

```
docker logout public.ecr.aws
```

Console error: the cluster is stuck in the Pending state

If the cluster gets stuck in the Pending state on the Amazon EKS console after you're registered it, it might be because the Amazon EKS Connector didn't successfully connect the cluster to AWS yet. For a registered cluster, the Pending state means that the connection isn't successfully established. To resolve this issue, make sure that you have applied the manifest to the target Kubernetes cluster. If you applied it to the cluster, but the cluster is still in the Pending state, then the eks-connector statefulset might be unhealthy. To troubleshoot this issue, see [Amazon EKS connector Pods are crash looping \(p. 584\)](#) in this topic.

Console error: User "system:serviceaccount:eks-connector:eks-connector" can't impersonate resource "users" in API group "" at cluster scope

The Amazon EKS Connector uses Kubernetes [user impersonation](#) to act on behalf of [IAM principals](#) from the AWS Management Console. Each principal that accesses the Kubernetes API from the AWS eks-connector service account must be granted permission to impersonate the corresponding Kubernetes user with an IAM ARN as its Kubernetes user name. In the following examples, the IAM ARN is mapped to a Kubernetes user.

- IAM user *john* from AWS account *111122223333* is mapped to a Kubernetes user. [IAM best practices](#) recommend that you grant permissions to roles instead of users.

```
arn:aws:iam::111122223333:user/john
```

- IAM role *admin* from AWS account *111122223333* is mapped to a Kubernetes user:

```
arn:aws:iam::111122223333:role/admin
```

The result is an IAM role ARN, instead of the AWS STS session ARN.

For instructions on how to configure the `ClusterRole` and `ClusterRoleBinding` to grant the eks-connector service account privilege to impersonate the mapped user, see [Granting access to an IAM principal to view Kubernetes resources on a cluster \(p. 579\)](#). Make sure that in the template, `%IAM_ARN%` is replaced with the IAM ARN of the AWS Management Console IAM principal.

Console error: [...] is forbidden: User [...] cannot list resource “[...] in API group” at the cluster scope

Consider the following problem. The Amazon EKS Connector has successfully impersonated the requesting AWS Management Console IAM principal in the target Kubernetes cluster. However, the impersonated principal doesn't have RBAC permission for Kubernetes API operations.

To resolve this issue, there are two methods to give permissions to additional users. If you previously installed eks-connector via helm chart, you can easily grant users access by running the following command. Replace the `userARN1` and `userARN2` with a list of the ARNs of the IAM roles to give access to view the Kubernetes resources:

```
helm upgrade eks-connector oci://public.ecr.aws/eks-connector/eks-connector-chart \
--reuse-values \
--set 'authentication.allowedUserARNs={userARN1,userARN2}'
```

Or, as the cluster administrator, grant the appropriate level of RBAC privileges to individual Kubernetes users. For more information and examples, see [Granting access to an IAM principal to view Kubernetes resources on a cluster \(p. 579\)](#).

Console error: Amazon EKS can't communicate with your Kubernetes cluster API server. The cluster must be in an ACTIVE state for successful connection. Try again in few minutes.

If the Amazon EKS service can't communicate with the Amazon EKS connector in the target cluster, it might be because of one of the following reasons:

- The Amazon EKS Connector in the target cluster is unhealthy.
- Poor connectivity or an interrupted connection between the target cluster and the AWS Region.

To resolve this problem, check the [Amazon EKS Connector logs \(p. 582\)](#). If you don't see an error for the Amazon EKS Connector, retry the connection after a few minutes. If you regularly experience high latency or intermittent connectivity for the target cluster, consider re-registering the cluster to an AWS Region that's located closer to you.

Amazon EKS connector Pods are crash looping

There are many reasons that can cause an Amazon EKS connector Pod to enter the `CrashLoopBackOff` status. This issue likely involves the `connector-init` container. Check the status of the Amazon EKS connector Pod.

```
kubectl get pods -n eks-connector
```

An example output is as follows.

NAME	READY	STATUS	RESTARTS	AGE
eks-connector-0	0/2	Init:CrashLoopBackOff	1	7s

If your output is similar to the previous output, see [Inspect Amazon EKS Connector logs \(p. 582\)](#) to troubleshoot the issue.

Failed to initiate eks-connector: InvalidActivation

When you start the Amazon EKS Connector for the first time, it registers an activationId and activationCode with Amazon Web Services. The registration might fail, which can cause the connector-init container to crash with an error similar to the following error.

```
F1116 20:30:47.261469      1 init.go:43] failed to initiate eks-connector:  
InvalidActivation:
```

To troubleshoot this issue, consider the following causes and recommended fixes:

- Registration might have failed because the activationId and activationCode aren't in your manifest file. If this is the case, make sure that they are the correct values that were returned from the RegisterCluster API operation, and that the activationCode is in the manifest file. The activationCode is added to Kubernetes secrets, so it must be base64 encoded. For more information, see [Step 1: Registering the cluster \(p. 575\)](#).
- Registration might have failed because your activation expired. This is because, for security reasons, you must activate the Amazon EKS Connector within three days after registering the cluster. To resolve this issue, make sure that the Amazon EKS Connector manifest is applied to the target Kubernetes cluster before the expiry date and time. To confirm your activation expiry date, call the DescribeCluster API operation.

```
aws eks describe-cluster --name my-cluster
```

In the following example response, the expiry date and time is recorded as 2021-11-12T22:28:51.101000-08:00.

```
{  
  "cluster": {  
    "name": "my-cluster",  
    "arn": "arn:aws:eks:region:111122223333:cluster/my-cluster",  
    "createdAt": "2021-11-09T22:28:51.449000-08:00",  
    "status": "FAILED",  
    "tags": {},  
    "connectorConfig": {  
      "activationId": "00000000-0000-0000-0000-000000000000",  
      "activationExpiry": "2021-11-12T22:28:51.101000-08:00",  
      "provider": "OTHER",  
      "roleArn": "arn:aws:iam::111122223333:role/my-connector-role"  
    }  
  }  
}
```

If the activationExpiry passed, deregister the cluster and register it again. Do this generates a new activation.

Cluster node is missing outbound connectivity

To work properly, the Amazon EKS Connector requires outbound connectivity to several AWS endpoints. You can't connect a private cluster without outbound connectivity to a target AWS Region. To resolve this issue, you must add the necessary outbound connectivity. For information about connector requirements, see [Amazon EKS Connector considerations \(p. 574\)](#).

Amazon EKS connector Pods are in ImagePullBackOff state

If you run the `get pods` command and Pods are in the `ImagePullBackOff` state, they can't work properly. If the Amazon EKS Connector Pods are in the `ImagePullBackOff` state, they can't work properly. Check the status of your Amazon EKS Connector Pods.

```
kubectl get pods -n eks-connector
```

An example output is as follows.

NAME	READY	STATUS	RESTARTS	AGE
eks-connector-0	0/2	Init:ImagePullBackOff	0	4s

The default Amazon EKS Connector manifest file references images from the [Amazon ECR Public Gallery](#). It's possible that the target Kubernetes cluster can't pull images from the Amazon ECR Public Gallery. Either resolve the Amazon ECR Public Gallery image pull issue, or consider mirroring the images in the private container registry of your choice.

Frequently asked questions

Q: How does the underlying technology behind the Amazon EKS Connector work?

A: The Amazon EKS Connector is based on the AWS Systems Manager (Systems Manager) agent. The Amazon EKS Connector runs as a StatefulSet on your Kubernetes cluster. It establishes a connection and proxies the communication between the API server of your cluster and Amazon Web Services. It does this to display cluster data in the Amazon EKS console until you disconnect the cluster from AWS. The Systems Manager agent is an open source project. For more information about this project, see the [GitHub project page](#).

Q: I have an on-premises Kubernetes cluster that I want to connect. Do I need to open firewall ports to connect it?

A: No, you don't need to open any firewall ports. The Kubernetes cluster only requires outbound connection to AWS Regions. AWS services never access resources in your on-premises network. The Amazon EKS Connector runs on your cluster and initiates the connection to AWS. When the cluster registration completes, AWS only issues commands to the Amazon EKS Connector after you start an action from the Amazon EKS console that requires information from the Kubernetes API server on your cluster.

Q: What data is sent from my cluster to AWS by the Amazon EKS Connector?

A: The Amazon EKS Connector sends technical information that's necessary for your cluster to be registered on AWS. It also sends cluster and workload metadata for the Amazon EKS console features that customers request. The Amazon EKS Connector only gathers or sends this data if you start an action from the Amazon EKS console or the Amazon EKS API that necessitates the data to be sent to AWS.

Other than the Kubernetes version number, AWS doesn't store any data by default. It stores data only if you authorize it to.

Q: Can I connect a cluster outside of an AWS Region?

A: Yes, you can connect a cluster from any location to Amazon EKS. Moreover, your Amazon EKS service can be located in any AWS public commercial AWS Region. This works with a valid network connection from your cluster to the target AWS Region. We recommend that you pick an AWS Region that is closest to your cluster location for UI performance optimization. For example, if you have a cluster running in Tokyo, connect your cluster to the AWS Region in Tokyo (that is, the ap-northeast-1 AWS Region) for low latency. You can connect a cluster from any location to Amazon EKS in any of the public commercial AWS Regions, except the China or GovCloud AWS Regions.

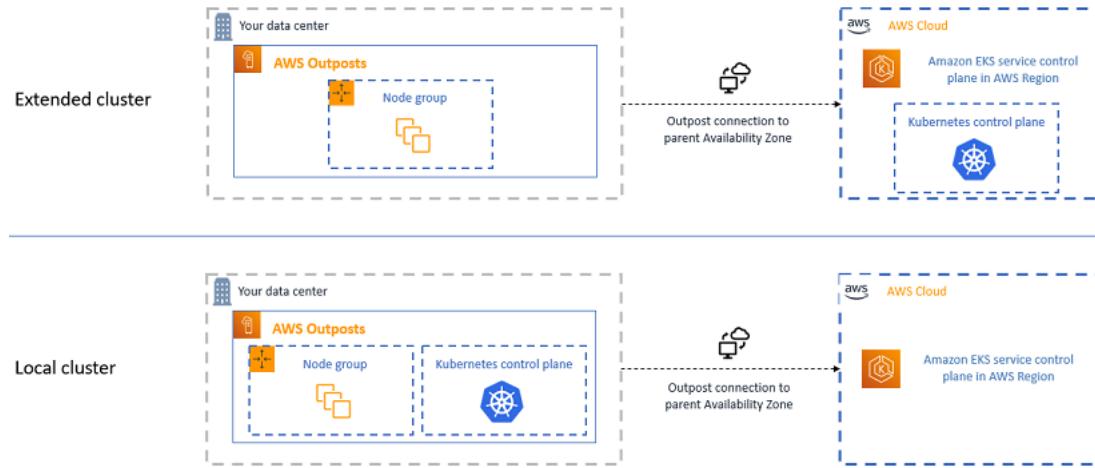
Amazon EKS on AWS Outposts

You can use Amazon EKS to run on-premises Kubernetes applications on AWS Outposts. You can deploy Amazon EKS on Outposts in the following ways:

- **Extended clusters** – Run the Kubernetes control plane in an AWS Region and nodes on your Outpost.
- **Local clusters** – Run the Kubernetes control plane and nodes on your Outpost.

For both deployment options, the Kubernetes control plane is fully managed by AWS. You can use the same Amazon EKS APIs, tools, and console that you use in the cloud to create and run Amazon EKS on Outposts.

The following diagram shows these deployment options.



When to use each deployment option

Both local and extended clusters are general-purpose deployment options and can be used for a range of applications.

With local clusters, you can run the entire Amazon EKS cluster locally on Outposts. This option can mitigate the risk of application downtime that might result from temporary network disconnects to the cloud. These network disconnects can be caused by fiber cuts or weather events. Because the entire Amazon EKS cluster runs locally on Outposts, applications remain available. You can perform cluster operations during network disconnects to the cloud. For more information, see [the section called "Network disconnects" \(p. 604\)](#). If you're concerned about the quality of the network connection from your Outposts to the parent AWS Region and require high availability through network disconnects, use the local cluster deployment option.

With extended clusters, you can conserve capacity on your Outpost because the Kubernetes control plane runs in the parent AWS Region. This option is suitable if you can invest in reliable, redundant network connectivity from your Outpost to the AWS Region. The quality of the network connection is

critical for this option. The way that Kubernetes handles network disconnects between the Kubernetes control plane and nodes might lead to application downtime. For more information on the behavior of Kubernetes, see [Scheduling, Preemption, and Eviction](#) in the Kubernetes documentation.

Comparing the deployment options

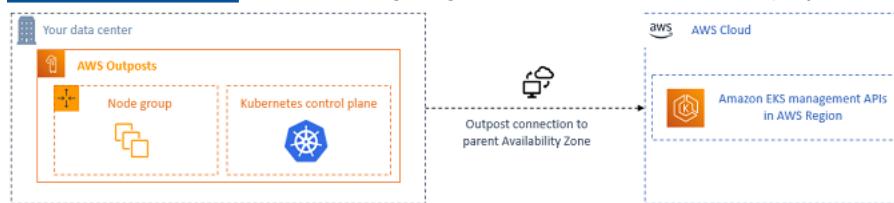
The following table compares the differences between the two options.

Feature	Extended cluster	Local cluster
Kubernetes control plane location	AWS Region	Outpost
Kubernetes control plane account	AWS account	Your account
Regional availability	See Service endpoints	US East (N. Virginia), US East (Ohio), US West (N. California), US West (Oregon), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Canada (Central), Europe (Frankfurt), Europe (London), Middle East (Bahrain), and South America (São Paulo)
Kubernetes minor versions	Supported Amazon EKS versions (p. 60)	Supported Amazon EKS versions (p. 60)
Platform versions	See the section called “Platform versions” (p. 71)	See the section called “Platform versions” (p. 597)
Outpost form factors	Outpost racks	Outpost racks
User interfaces	AWS Management Console, AWS CLI, Amazon EKS API, eksctl, AWS CloudFormation, and Terraform	AWS Management Console, AWS CLI, Amazon EKS API, eksctl, AWS CloudFormation, and Terraform
Managed policies	AmazonEKSClusterPolicy (p. 511) and AmazonEKSServiceRolePolicy (p. 513)	AmazonEKSLocalOutpostClusterPolicy (p. 515) and AmazonEKSLocalOutpostServiceRolePolicy (p. 517)
Cluster VPC and subnets	See the section called “VPC and subnet requirements” (p. 256)	See the section called “VPC and subnet requirements” (p. 601)
Cluster endpoint access	Public or private or both	Private only
Kubernetes API server authentication	AWS Identity and Access Management (IAM) and OIDC	IAM and x.509 certificates
Node types	Self-managed only	Self-managed only
Node compute types	Amazon EC2 on-demand	Amazon EC2 on-demand
Node storage types	Amazon EBS gp2 and local NVMe SSD	Amazon EBS gp2 and local NVMe SSD

Feature	Extended cluster	Local cluster
Amazon EKS optimized AMIs	Amazon Linux, Windows, and Bottlerocket	Amazon Linux only
IP versions	IPv4 only	IPv4 only
Add-ons	Amazon EKS add-ons or self-managed add-ons	Self-managed add-ons only
Default Container Network Interface	Amazon VPC CNI plugin for Kubernetes	Amazon VPC CNI plugin for Kubernetes
Kubernetes control plane logs	Amazon CloudWatch Logs	Amazon CloudWatch Logs
Load balancing	Use the AWS Load Balancer Controller (p. 333) to provision Application Load Balancers only (no Network Load Balancers)	Use the AWS Load Balancer Controller (p. 333) to provision Application Load Balancers only (no Network Load Balancers)
Secrets envelope encryption	See the section called "Enabling secret encryption" (p. 46)	Not supported
IAM roles for service accounts	See the section called "IAM roles for service accounts" (p. 464)	Not supported
Troubleshooting	See Troubleshooting (p. 562)	See the section called "Troubleshooting" (p. 608)

Local clusters for Amazon EKS on AWS Outposts

You can use local clusters to run your entire Amazon EKS cluster locally on AWS Outposts. This helps mitigate the risk of application downtime that might result from temporary network disconnects to the cloud. These disconnects can be caused by fiber cuts or weather events. Because the entire Kubernetes cluster runs locally on Outposts, applications remain available. You can perform cluster operations during network disconnects to the cloud. For more information, see [the section called "Network disconnects" \(p. 604\)](#). The following diagram shows a local cluster deployment.



Local clusters are generally available for use with Outposts racks.

Supported AWS Regions

You can create local clusters in the following AWS Regions: US East (N. Virginia), US East (Ohio), US West (N. California), US West (Oregon), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Canada (Central), Europe (Frankfurt), Europe (London), Middle East (Bahrain), and South America (São Paulo). For detailed information about supported features, see [the section called "Comparing the deployment options" \(p. 589\)](#).

Topics

- [Creating a local cluster on an Outpost \(p. 591\)](#)

- [Amazon EKS local cluster platform versions \(p. 597\)](#)
- [Amazon EKS local cluster VPC and subnet requirements and considerations \(p. 601\)](#)
- [Preparing for network disconnects \(p. 604\)](#)
- [Capacity considerations \(p. 607\)](#)
- [Troubleshooting local clusters for Amazon EKS on AWS Outposts \(p. 608\)](#)

Creating a local cluster on an Outpost

This topic provides an overview of what to consider when running a local cluster on an Outpost. The topic also provides instructions for how to deploy a local cluster on an Outpost.

Considerations

Important

- These considerations aren't replicated in related Amazon EKS documentation. If other Amazon EKS documentation topics conflict with the considerations here, follow the considerations here.
 - These considerations are subject to change and might change frequently. So, we recommend that you regularly review this topic.
 - Many of the considerations are different than the considerations for creating a cluster on the AWS Cloud.
-
- Local clusters support Outpost racks only. A single local cluster can run across multiple physical Outpost racks that comprise a single logical Outpost. A single local cluster can't run across multiple logical Outposts. Each logical Outpost has a single Outpost ARN.
 - Local clusters run and manage the Kubernetes control plane in your account on the Outpost. You can't run workloads on the Kubernetes control plane instances or modify the Kubernetes control plane components. These nodes are managed by the Amazon EKS service. Changes to the Kubernetes control plane don't persist through automatic Amazon EKS management actions, such as patching.
 - Local clusters support self-managed add-ons and self-managed Amazon Linux 2 node groups. The [Amazon VPC CNI plugin for Kubernetes \(p. 266\)](#), [kube-proxy \(p. 347\)](#), and [CoreDNS \(p. 341\)](#) add-ons are automatically installed on local clusters.
 - Local clusters require the use of Amazon EBS on Outposts. Your Outpost must have Amazon EBS available for the Kubernetes control plane storage.
 - Local clusters use Amazon EBS on Outposts. Your Outpost must have Amazon EBS available for the Kubernetes control plane storage. Outposts support Amazon EBS gp2 volumes only.
 - Amazon EBS backed Kubernetes PersistentVolumes are supported using the Amazon EBS CSI driver.

Prerequisites

- Familiarity with the [Outposts deployment options \(p. 589\)](#), the section called "Capacity considerations" (p. 607), and the section called "VPC and subnet requirements" (p. 601).
- An existing Outpost. For more information, see [What is AWS Outposts](#).
- The kubectl command line tool is installed on your computer or AWS CloudShell. The version can be the same as or up to one minor version earlier or later than the Kubernetes version of your cluster. For example, if your cluster version is 1.27, you can use kubectl version 1.26, 1.27, or 1.28 with it. To install or upgrade kubectl, see [the section called "Installing kubectl" \(p. 6\)](#).
- Version 2.12.3 or later or 1.27.160 or later of the AWS CLI installed and configured on your device or AWS CloudShell. You can check your current version with aws --version | cut -d / -f2 | cut -d ' ' -f1. Package managers such yum, apt-get, or Homebrew for macOS are often several

versions behind the latest version of the AWS CLI. To install the latest version, see [Installing, updating, and uninstalling the AWS CLI](#) and [Quick configuration with aws configure](#) in the AWS Command Line Interface User Guide. The AWS CLI version installed in the AWS CloudShell may also be several versions behind the latest version. To update it, see [Installing AWS CLI to your home directory](#) in the AWS CloudShell User Guide.

- An [IAM principal](#) with permissions to create and describe an Amazon EKS cluster. For more information, see [the section called “Create a local Kubernetes cluster on an Outpost” \(p. 489\)](#) and [the section called “List or describe all clusters” \(p. 490\)](#).

When a local Amazon EKS cluster is created, the [IAM principal](#) that creates the cluster is permanently added. The principal is specifically added to the Kubernetes RBAC authorization table as the administrator. This entity has `system:masters` permissions. The identity of this entity isn't visible in your cluster configuration. So, it's important to note the entity that created the cluster and make sure that you never delete it. Initially, only the principal that created the server can make calls to the Kubernetes API server using `kubectl`. If you use the console to create the cluster, make sure that the same IAM credentials are in the AWS SDK credential chain when you run `kubectl` commands on your cluster. After your cluster is created, you can grant other IAM principals access to your cluster.

To create a local Amazon EKS local cluster

You can create a local cluster with `eksctl`, the AWS Management Console, the [AWS CLI](#), the [Amazon EKS API](#), the [AWS SDKs](#), [AWS CloudFormation](#) or [Terraform](#).

1. Create a local cluster.

`eksctl`

Prerequisite

Version `0.160.0` or later of the `eksctl` command line tool installed on your device or AWS CloudShell. To install or update `eksctl`, see [Installing or updating eksctl \(p. 13\)](#).

To create your cluster with `eksctl`

1. Copy the contents that follow to your device. Replace the following values and then run the modified command to create the `outpost-control-plane.yaml` file:
 - Replace `region-code` with the [supported AWS Region \(p. 590\)](#) that you want to create your cluster in.
 - Replace `my-cluster` with a name for your cluster. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters. The name must be unique within the AWS Region and AWS account that you're creating the cluster in.
 - Replace `vpc-ExampleID1` and `subnet-ExampleID1` with the IDs of your existing VPC and subnet. The VPC and subnet must meet the requirements in [the section called “VPC and subnet requirements” \(p. 601\)](#).
 - Replace `uniqueid` with the ID of your Outpost.
 - Replace `m5.large` with an instance type available on your Outpost. Before choosing an instance type, see [the section called “Capacity considerations” \(p. 607\)](#). Three control plane instances are deployed. You can't change this number.

```
cat >outpost-control-plane.yaml <<EOF
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-cluster
EOF
```

```

region: region-code
version: "1.24"

vpc:
  clusterEndpoints:
    privateAccess: true
    id: "vpc-vpc-ExampleID1"
  subnets:
    private:
      outpost-subnet-1:
        id: "subnet-subnet-ExampleID1"

outpost:
  controlPlaneOutpostARN: arn:aws:outposts:region-code:111122223333:outpost/op-uniqueid
  controlPlaneInstanceType: m5.large
EOF

```

For a complete list of all available options and defaults, see [AWS Outposts Support](#) and [Config file schema](#) in the `eksctl` documentation.

2. Create the cluster using the configuration file that you created in the previous step. `eksctl` creates a VPC and one subnet on your Outpost to deploy the cluster in.

```
eksctl create cluster -f outpost-control-plane.yaml
```

Cluster provisioning takes several minutes. While the cluster is being created, several lines of output appear. The last line of output is similar to the following example line.

```
[#] EKS cluster "my-cluster" in "region-code" region is ready
```

Tip

To see the most options that you can specify when creating a cluster with `eksctl`, use the `eksctl create cluster --help` command. To see all the available options, you can use a config file. For more information, see [Using config files](#) and the [config file schema](#) in the `eksctl` documentation. You can find [config file examples](#) on GitHub.

AWS Management Console

Prerequisite

An existing VPC and subnet that meet Amazon EKS requirements. For more information, see [the section called "VPC and subnet requirements" \(p. 601\)](#).

To create your cluster with the AWS Management Console

1. If you already have a local cluster IAM role, or you're going to create your cluster with `eksctl`, then you can skip this step. By default, `eksctl` creates a role for you.
 - a. Run the following command to create an IAM trust policy JSON file.

```

cat >eks-local-cluster-role-trust-policy.json <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },

```

```
        "Action": "sts:AssumeRole"
    }
}
EOF
```

- b. Create the Amazon EKS cluster IAM role. To create an IAM role, the [IAM principal](#) that is creating the role must be assigned the `iam:CreateRole` action (permission).

```
aws iam create-role --role-name myAmazonEKSLocalClusterRole --assume-role-policy-document file:///"eks-local-cluster-role-trust-policy.json"
```

- c. Attach the Amazon EKS managed policy named [AmazonEKSLocalOutpostClusterPolicy](#) to the role. To attach an IAM policy to an [IAM principal](#), the principal that is attaching the policy must be assigned one of the following IAM actions (permissions): `iam:AttachUserPolicy` or `iam:AttachRolePolicy`.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/  
AmazonEKSLocalOutpostClusterPolicy --role-name myAmazonEKSLocalClusterRole
```

2. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
3. At the top of the console screen, make sure that you have selected a [supported AWS Region \(p. 590\)](#).
4. Choose **Add cluster** and then choose **Create**.
5. On the **Configure cluster** page, enter or select values for the following fields:
 - **Kubernetes control plane location** – Choose AWS Outposts.
 - **Outpost ID** – Choose the ID of the Outpost that you want to create your control plane on.
 - **Instance type** – Select an instance type. Only the instance types available in your Outpost are displayed. In the dropdown list, each instance type describes how many nodes the instance type is recommended for. Before choosing an instance type, see [the section called "Capacity considerations" \(p. 607\)](#). All replicas are deployed using the same instance type. You can't change the instance type after your cluster is created. Three control plane instances are deployed. You can't change this number.
 - **Name** – A name for your cluster. It must be unique in your AWS account. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters. The name must be unique within the AWS Region and AWS account that you're creating the cluster in.
 - **Kubernetes version** – Choose the Kubernetes version that you want to use for your cluster. We recommend selecting the latest version, unless you need to use an earlier version.
 - **Cluster service role** – Choose the Amazon EKS cluster IAM role that you created in a previous step to allow the Kubernetes control plane to manage AWS resources.
 - **Tags** – (Optional) Add any tags to your cluster. For more information, see [Tagging your Amazon EKS resources \(p. 451\)](#).
6. Select **Next**.
7. On the **Specify networking** page, select values for the following fields:
 - **VPC** – Choose an existing VPC. The VPC must have a sufficient number of IP addresses available for the cluster, any nodes, and other Kubernetes resources that you want to create. Your VPC must meet the requirements in [the section called "VPC requirements and considerations" \(p. 602\)](#).
 - **Subnets** – By default, all available subnets in the VPC specified in the previous field are preselected. The subnets that you choose must meet the requirements in [the section called "Subnet requirements and considerations" \(p. 602\)](#). You can't change which subnets you want to use after cluster creation.

Security groups – (Optional) Specify one or more security groups that you want Amazon EKS to associate to the network interfaces that it creates. Amazon EKS automatically creates a security group that enables communication between your cluster and your VPC. Amazon EKS associates this security group, and any that you choose, to the network interfaces that it creates. For more information about the cluster security group that Amazon EKS creates, see [the section called “Security group requirements” \(p. 263\)](#). You can modify the rules in the cluster security group that Amazon EKS creates. If you choose to add your own security groups, you can’t change the ones that you choose after cluster creation. For on-premises hosts to communicate with the cluster endpoint, you must allow inbound traffic from the cluster security group. For clusters that don’t have an ingress and egress internet connection (also known as private clusters), you must do one of the following:

- Add the security group associated with required VPC endpoints. For more information about the required endpoints, see [Interface VPC endpoints \(p. 603\)](#) in [the section called “Subnet access to AWS services” \(p. 602\)](#).
- Modify the security group that Amazon EKS created to allow traffic from the security group associated with the VPC endpoints.

8. Select **Next**.

9. On the **Configure logging** page, you can optionally choose which log types that you want to enable. By default, each log type is **Disabled**. Before selecting a different option, familiarize yourself with the information in [Amazon EKS control plane logging \(p. 536\)](#). After you create the cluster, you can change this option.

10. Select **Next**.

11. On the **Review and create** page, review the information that you entered or selected on the previous pages. If you need to make changes, choose **Edit**. When you’re satisfied, choose **Create**. The **Status** field shows **CREATING** while the cluster is provisioned.

Cluster provisioning takes several minutes.

2. After your cluster is created, you can view the Amazon EC2 control plane instances that were created.

```
aws ec2 describe-instances --query 'Reservations[*].Instances[*].[Name:Tags[?Key==`Name`][0].Value]' | grep my-cluster-control-plane
```

An example output is as follows.

```
"Name": "my-cluster-control-plane-id1"  
"Name": "my-cluster-control-plane-id2"  
"Name": "my-cluster-control-plane-id3"
```

Each instance is tainted with `node-role.eks-local.amazonaws.com/control-plane` so that no workloads are ever scheduled on the control plane instances. For more information about taints, see [Taints and Tolerations](#) in the Kubernetes documentation. Amazon EKS continuously monitors the state of local clusters. We perform automatic management actions, such as security patches and repairing unhealthy instances. When local clusters are disconnected from the cloud, we complete actions to ensure that the cluster is repaired to a healthy state upon reconnect.

3. If you created your cluster using `eksctl`, then you can skip this step. `eksctl` completes this step for you. Enable `kubectl` to communicate with your cluster by adding a new context to the `kubectl config` file. For instructions on how to create and update the file, see [the section called “Creating kubeconfig file” \(p. 431\)](#).

```
aws eks update-kubeconfig --region region-code --name my-cluster
```

An example output is as follows.

```
Added new context arn:aws:eks:region-code:111122223333:cluster/my-cluster to /home/username/.kube/config
```

4. To connect to your local cluster's Kubernetes API server, have access to the local gateway for the subnet, or connect from within the VPC. For more information about connecting an Outpost rack to your on-premises network, see [How local gateways for racks work](#) in the AWS Outposts User Guide. If you use Direct VPC Routing and the Outpost subnet has a route to your local gateway, the private IP addresses of the Kubernetes control plane instances are automatically broadcasted over your local network. The local cluster's Kubernetes API server endpoint is hosted in Amazon Route 53 (Route 53). The API service endpoint can be resolved by public DNS servers to the Kubernetes API servers' private IP addresses.

Local clusters' Kubernetes control plane instances are configured with static elastic network interfaces with fixed private IP addresses that don't change throughout the cluster lifecycle. Machines that interact with the Kubernetes API server might not have connectivity to Route 53 during network disconnects. If this is the case, we recommend configuring /etc/hosts with the static private IP addresses for continued operations. We also recommend setting up local DNS servers and connecting them to your Outpost. For more information, see the [AWS Outposts documentation](#). Run the following command to confirm that communication's established with your cluster.

```
kubectl get svc
```

An example output is as follows.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
kubernetes	ClusterIP	10.100.0.1	<none>	443/TCP	28h

5. (Optional) Test authentication to your local cluster when it's in a disconnected state from the AWS Cloud. For instructions, see [the section called "Network disconnects" \(p. 604\)](#).

Internal resources

Amazon EKS creates the following resources on your cluster. The resources are for Amazon EKS internal use. For proper functioning of your cluster, don't edit or modify these resources.

- The following [mirror Pods](#):
 - aws-iam-authenticator-*node-hostname*
 - eks-certificates-controller-*node-hostname*
 - etcd-*node-hostname*
 - kube-apiserver-*node-hostname*
 - kube-controller-manager-*node-hostname*
 - kube-scheduler-*node-hostname*
- The following self-managed add-ons:
 - kube-system/coredns
 - kube-system/kube-proxy (not created until you add your first node)
 - kube-system/aws-node (not created until you add your first node). Local clusters use the Amazon VPC CNI plugin for Kubernetes plugin for cluster networking. Do not change the configuration for control plane instances (Pods named aws-node-controlplane-*). There are configuration

variables that you can use to change the default value for when the plugin creates new network interfaces. For more information, see the [documentation](#) on GitHub.

- The following services:
 - default/kubernetes
 - kube-system/kube-dns
- A PodSecurityPolicy named eks.system
- A ClusterRole named eks:system:podsecuritypolicy
- A ClusterRoleBinding named eks:system
- A default [PodSecurityPolicy \(p. 522\)](#)
- In addition to the [cluster security group \(p. 263\)](#), Amazon EKS creates a security group in your AWS account that's named eks-local-internal-do-not-use-or-edit-*cluster-name-uniqueid*. This security group allows traffic to flow freely between Kubernetes components running on the control plane instances.

Recommended next steps:

- [Grant the IAM principal that created the cluster the required permissions to view Kubernetes resources in the AWS Management Console \(p. 529\)](#)
- [Grant IAM entities access to your cluster \(p. 420\)](#). If you want the entities to view Kubernetes resources in the Amazon EKS console, grant the [the section called "Required permissions" \(p. 529\)](#) to the entities.
- [Configure logging for your cluster \(p. 536\)](#)
- Familiarize yourself with what happens during [network disconnects \(p. 604\)](#).
- [Add nodes to your cluster \(p. 614\)](#)
- Consider setting up a backup plan for your etcd. Amazon EKS doesn't support automated backup and restore of etcd for local clusters. For more information, see [Backing up an etcd cluster](#) in the Kubernetes documentation. The two main options are using etcdctl to automate taking snapshots or using Amazon EBS storage volume backup.

Amazon EKS local cluster platform versions

Local cluster platform versions represent the capabilities of the Amazon EKS cluster on AWS Outposts. The versions include the components that run on the Kubernetes control plane, which Kubernetes API server flags are enabled. They also include the current Kubernetes patch version. Each Kubernetes minor version has one or more associated platform versions. The platform versions for different Kubernetes minor versions are independent. The platform versions for local clusters and Amazon EKS clusters in the cloud are independent.

When a new Kubernetes minor version is available for local clusters, such as 1.28, the initial platform version for that Kubernetes minor version starts at eks-local-outposts.1. However, Amazon EKS releases new platform versions periodically to enable new Kubernetes control plane settings and to provide security fixes.

When new local cluster platform versions become available for a minor version:

- The platform version number is incremented (eks-local-outposts.n+1).
- Amazon EKS automatically updates all existing local clusters to the latest platform version for their corresponding Kubernetes minor version. Automatic updates of existing platform versions are rolled out incrementally. The roll-out process might take some time. If you need the latest platform version features immediately, we recommend that you create a new local cluster.
- Amazon EKS might publish a new node AMI with a corresponding patch version. All patch versions are compatible between the Kubernetes control plane and node AMIs for a single Kubernetes minor version.

New platform versions don't introduce breaking changes or cause service interruptions.

Local clusters are always created with the latest available platform version (`eks-local-outposts.n`) for the specified Kubernetes version.

The current and recent platform versions are described in the following tables.

Kubernetes version 1.28

The following admission controllers are enabled for all 1.28 platform versions:
`CertificateApproval`, `CertificateSigning`, `CertificateSubjectRestriction`,
`DefaultIngressClass`, `DefaultStorageClass`, `DefaultTolerationSeconds`,
`ExtendedResourceToleration`, `LimitRanger`, `MutatingAdmissionWebhook`,
`NamespaceLifecycle`, `NodeRestriction`, `PersistentVolumeClaimResize`,
`Priority`, `PodSecurity`, `ResourceQuota`, `RuntimeClass`, `ServiceAccount`,
`StorageObjectInUseProtection`, `TaintNodesByCondition`, `ValidatingAdmissionPolicy`,
and `ValidatingAdmissionWebhook`.

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.28.1	<code>eks-local-outposts.1</code>	Initial release of Kubernetes version 1.28 for local Amazon EKS clusters on Outposts.	October 4, 2023

Kubernetes version 1.27

The following admission controllers are enabled for all 1.27 platform versions:
`CertificateApproval`, `CertificateSigning`, `CertificateSubjectRestriction`,
`DefaultIngressClass`, `DefaultStorageClass`, `DefaultTolerationSeconds`,
`ExtendedResourceToleration`, `LimitRanger`, `MutatingAdmissionWebhook`,
`NamespaceLifecycle`, `NodeRestriction`, `PersistentVolumeClaimResize`,
`Priority`, `PodSecurity`, `ResourceQuota`, `RuntimeClass`, `ServiceAccount`,
`StorageObjectInUseProtection`, `TaintNodesByCondition`, `ValidatingAdmissionPolicy`,
and `ValidatingAdmissionWebhook`.

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.27.3	<code>eks-local-outposts.3</code>	New platform version with security fixes and enhancements. <code>kube-proxy</code> updated to v1.27.3. Amazon VPC CNI plugin for Kubernetes updated to v1.13.2.	July 14, 2023
1.27.1	<code>eks-local-outposts.2</code>	Updated CoreDNS image to v1.10.1	June 22, 2023
1.27.1	<code>eks-local-outposts.1</code>	Initial release of Kubernetes version 1.27 for local Amazon EKS clusters on Outposts.	May 30, 2023

Kubernetes version 1.26

The following admission controllers are enabled for all 1.26 platform versions: CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, DefaultStorageClass, DefaultTolerationSeconds, ExtendedResourceToleration, LimitRanger, MutatingAdmissionWebhook, NamespaceLifecycle, NodeRestriction, PersistentVolumeClaimResize, Priority, PodSecurity, ResourceQuota, RuntimeClass, ServiceAccount, StorageObjectInUseProtection, TaintNodesByCondition, ValidatingAdmissionPolicy, and ValidatingAdmissionWebhook.

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.26.6	eks-local-outposts.4	New platform version with security fixes and enhancements. kube-proxy updated to v1.26.6. Amazon VPC CNI plugin for Kubernetes updated to v1.13.2.	July 14, 2023
1.26.4	eks-local-outposts.3	New platform version with security fixes and enhancements.	July 13, 2023
1.26.2	eks-local-outposts.2	Updated Bottlerocket version to 1.13.2	May 2, 2023
1.26.2	eks-local-outposts.1	Initial release of Kubernetes version 1.26 for local Amazon EKS clusters on Outposts.	April 11, 2023

Kubernetes version 1.25

The following admission controllers are enabled for all 1.25 platform versions: CertificateApproval, CertificateSigning, CertificateSubjectRestriction, DefaultIngressClass, DefaultStorageClass, DefaultTolerationSeconds, ExtendedResourceToleration, LimitRanger, MutatingAdmissionWebhook, NamespaceLifecycle, NodeRestriction, PersistentVolumeClaimResize, Priority, PodSecurity, ResourceQuota, RuntimeClass, ServiceAccount, StorageObjectInUseProtection, TaintNodesByCondition, and ValidatingAdmissionWebhook.

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.25.11	eks-local-outposts.6	New platform version with security fixes and enhancements. kube-proxy updated to v1.25.11. Amazon VPC CNI plugin for Kubernetes updated to v1.13.2.	July 14, 2023
1.25.9	eks-local-outposts.5	New platform version with security fixes and enhancements.	July 13, 2023

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.25.6	eks-local-outposts.4	Updated Bottlerocket version to 1.13.2	May 2, 2023
1.25.6	eks-local-outposts.3	Amazon EKS control plane instance operating system updated to Bottlerocket version v1.13.1 and Amazon VPC CNI plugin for Kubernetes updated to version v1.12.6.	April 14, 2023
1.25.6	eks-local-outposts.2	Improved diagnostics collection for Kubernetes control plane instances.	March 8, 2023
1.25.6	eks-local-outposts.1	Initial release of Kubernetes version 1.25 for local Amazon EKS clusters on Outposts.	March 1, 2023

Kubernetes version 1.24

The following admission controllers are enabled for all 1.24 platform versions: DefaultStorageClass, DefaultTolerationSeconds, LimitRanger, MutatingAdmissionWebhook, NamespaceLifecycle, NodeRestriction, ResourceQuota, ServiceAccount, ValidatingAdmissionWebhook, PodSecurityPolicy, TaintNodesByCondition, StorageObjectInUseProtection, PersistentVolumeClaimResize, ExtendedResourceToleration, CertificateApproval, PodPriority, CertificateSigning, CertificateSubjectRestriction, RuntimeClass, and DefaultIngressClass.

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.24.15	eks-local-outposts.6	New platform version with security fixes and enhancements. kube-proxy updated to v1.24.15. Amazon VPC CNI plugin for Kubernetes updated to v1.13.2.	July 14, 2023
1.24.13	eks-local-outposts.5	New platform version with security fixes and enhancements.	July 13, 2023
1.24.9	eks-local-outposts.4	Updated Bottlerocket version to 1.13.2	May 2, 2023
1.24.9	eks-local-outposts.3	Amazon EKS control plane instance operating system updated to Bottlerocket version v1.13.1 and Amazon VPC CNI plugin for Kubernetes updated to version v1.12.6.	April 14, 2023

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.24.9	eks-local-outposts.2	Improved diagnostics collection for Kubernetes control plane instances.	March 8, 2023
1.24.9	eks-local-outposts.1	Initial release of Kubernetes version 1.24 for local Amazon EKS clusters on Outposts.	January 17, 2023

Kubernetes version 1.23

The following admission controllers are enabled for all 1.23 platform versions: DefaultStorageClass, DefaultTolerationSeconds, LimitRanger, MutatingAdmissionWebhook, NamespaceLifecycle, NodeRestriction, ResourceQuota, ServiceAccount, ValidatingAdmissionWebhook, PodSecurityPolicy, TaintNodesByCondition, StorageObjectInUseProtection, PersistentVolumeClaimResize, ExtendedResourceToleration, CertificateApproval, PodPriority, CertificateSigning, CertificateSubjectRestriction, RuntimeClass, and DefaultIngressClass.

Kubernetes version	Amazon EKS platform version	Release notes	Release date
1.23.17	eks-local-outposts.5	New platform version with security fixes and enhancements.	July 13, 2023
1.23.15	eks-local-outposts.4	Updated Bottlerocket version to 1.13.2	May 2, 2023
1.23.15	eks-local-outposts.3	Amazon EKS control plane instance operating system updated to Bottlerocket version v1.13.1 and Amazon VPC CNI plugin for Kubernetes updated to version v1.12.6.	April 14, 2023
1.23.15	eks-local-outposts.2	Improved diagnostics collection for Kubernetes control plane instances.	March 8, 2023
1.23.15	eks-local-outposts.1	Initial release of Kubernetes version 1.23 for local Amazon EKS clusters on Outposts.	January 17, 2023

Amazon EKS local cluster VPC and subnet requirements and considerations

When you create a local cluster, you specify a VPC and at least one private subnet that runs on Outposts. This topic provides an overview of the VPC and subnets requirements and considerations for your local cluster.

VPC requirements and considerations

When you create a local cluster, the VPC that you specify must meet the following requirements and considerations:

- Make sure that the VPC has enough IP addresses for the local cluster, any nodes, and other Kubernetes resources that you want to create. If the VPC that you want to use doesn't have enough IP addresses, increase the number of available IP addresses. You can do this by [associating additional Classless Inter-Domain Routing \(CIDR\) blocks](#) with your VPC. You can associate private (RFC 1918) and public (non-RFC 1918) CIDR blocks to your VPC either before or after you create your cluster. It can take a cluster up to 5 hours for a CIDR block that you associated with a VPC to be recognized.
- The VPC can't have assigned IP prefixes or IPv6 CIDR blocks. Because of these constraints, the information that's covered in [the section called "Increase available IP addresses" \(p. 318\)](#) and [the section called "IPv6" \(p. 278\)](#) isn't applicable to your VPC.
- The VPC has a DNS hostname and DNS resolution enabled. Without these features, the local cluster fails to create, and you need to enable the features and recreate your cluster. For more information, see [DNS attributes for your VPC](#) in the Amazon VPC User Guide.
- To access your local cluster over your local network, the VPC must be associated with your Outpost's local gateway route table. For more information, see [VPC associations](#) in the AWS Outposts User Guide.

Subnet requirements and considerations

When you create the cluster, specify at least one private subnet. If you specify more than one subnet, the Kubernetes control plane instances are evenly distributed across the subnets. If more than one subnet is specified, the subnets must exist on the same Outpost. Moreover, the subnets must also have proper routes and security group permissions to communicate with each other. When you create a local cluster, the subnets that you specify must meet the following requirements:

- The subnets are all on the same logical Outpost.
- The subnets together have at least three available IP addresses for the Kubernetes control plane instances. If three subnets are specified, each subnet must have at least one available IP address. If two subnets are specified, each subnet must have at least two available IP addresses. If one subnet is specified, the subnet must have at least three available IP addresses.
- The subnets have a route to the Outpost rack's [local gateway](#) to access the Kubernetes API server over your local network. If the subnets don't have a route to the Outpost rack's local gateway, you must communicate with your Kubernetes API server from within the VPC.
- The subnets must use IP address-based naming. Amazon EC2 [resource-based naming](#) isn't supported by Amazon EKS.

Subnet access to AWS services

The local cluster's private subnets on Outposts must be able to communicate with Regional AWS services. You can achieve this by using a [NAT gateway](#) for outbound internet access or, if you want to keep all traffic private within your VPC, using [interface VPC endpoints](#).

Using a NAT gateway

The local cluster's private subnets on Outposts must have an associated route table that has a route to a NAT gateway in a public subnet that is in the Outpost's parent Availability Zone. The public subnet must have a route to an [internet gateway](#). The NAT gateway enables outbound internet access and prevents unsolicited inbound connections from the internet to instances on the Outpost.

Using interface VPC endpoints

If the local cluster's private subnets on Outposts don't have an outbound internet connection, or if you want to keep all traffic private within your VPC, then you must create the following interface VPC endpoints and [gateway endpoint](#) in a Regional subnet before creating your cluster.

Endpoint	Endpoint type
com.amazonaws. <i>region-code</i> .ssm	Interface
com.amazonaws. <i>region-code</i> .ssmmessages	Interface
com.amazonaws. <i>region-code</i> .ec2messages	Interface
com.amazonaws. <i>region-code</i> .ec2	Interface
com.amazonaws. <i>region-code</i> .secretsmanager	Interface
com.amazonaws. <i>region-code</i> .logs	Interface
com.amazonaws. <i>region-code</i> .sts	Interface
com.amazonaws. <i>region-code</i> .ecr.api	Interface
com.amazonaws. <i>region-code</i> .ecr.dkr	Interface
com.amazonaws. <i>region-code</i> .s3	Gateway

The endpoints must meet the following requirements:

- Created in a private subnet located in your Outpost's parent Availability Zone
- Have private DNS names enabled
- Have an attached security group that permits inbound HTTPS traffic from the CIDR range of the private outpost subnet.

Creating endpoints incurs charges. For more information, see [AWS PrivateLink pricing](#). If your Pods need access to other AWS services, then you need to create additional endpoints. For a comprehensive list of endpoints, see [AWS services that integrate with AWS PrivateLink](#).

Create a VPC

You can create a VPC that meets the previous requirements using one of the following AWS CloudFormation templates:

- [Template 1](#) – This template creates a VPC with one private subnet on the Outpost and one public subnet in the AWS Region. The private subnet has a route to an internet through a NAT Gateway that resides in the public subnet in the AWS Region. This template can be used to create a local cluster in a subnet with egress internet access.
- [Template 2](#) – This template creates a VPC with one private subnet on the Outpost and the minimum set of VPC Endpoints required to create a local cluster in a subnet that doesn't have ingress or egress internet access (also referred to as a private subnet).

Preparing for network disconnects

If your local network has lost connectivity with the AWS Cloud, you can continue to use your local Amazon EKS cluster on an Outpost. This topic covers how you can prepare your local cluster for network disconnects and related considerations.

Considerations when preparing your local cluster for a network disconnect:

- Local clusters enable stability and continued operations during temporary, unplanned network disconnects. AWS Outposts remains a fully connected offering that acts as an extension of the AWS Cloud in your data center. In the event of network disconnects between your Outpost and AWS Cloud, we recommend attempting to restore your connection. For instruction, see [AWS Outposts rack network troubleshooting checklist](#) in the *AWS Outposts User Guide*. For more information about how to troubleshoot issues with local clusters, see [the section called "Troubleshooting" \(p. 608\)](#).
- Outposts emit a `ConnectedStatus` metric that you can use to monitor the connectivity state of your Outpost. For more information, see [Outposts Metrics](#) in the *AWS Outposts User Guide*.
- Local clusters use IAM as the default authentication mechanism using the [AWS Identity and Access Management authenticator for Kubernetes](#). IAM isn't available during network disconnects. So, local clusters support an alternative authentication mechanism using x.509 certificates that you can use to connect to your cluster during network disconnects. For information about how to obtain and use an x.509 certificate for your cluster, see [the section called "Authenticating to your cluster" \(p. 605\)](#).
- If you can't access Route 53 during network disconnects, consider using local DNS servers in your on-premises environment. The Kubernetes control plane instances use static IP addresses. You can configure the hosts that you use to connect to your cluster with the endpoint hostname and IP addresses as an alternative to using local DNS servers. For more information, see [DNS](#) in the *AWS Outposts User Guide*.
- If you expect increases in application traffic during network disconnects, you can provision spare compute capacity in your cluster when connected to the cloud. Amazon EC2 instances are included in the price of AWS Outposts. So, running spare instances doesn't impact your AWS usage cost.
- During network disconnects to enable create, update, and scale operations for workloads, your application's container images must be accessible over the local network and your cluster must have enough capacity. Local clusters don't host a container registry for you. If the Pods have previously run on those nodes, container images are cached on the nodes. If you typically pull your application's container images from Amazon ECR in the cloud, consider running a local cache or registry. A local cache or registry is helpful if you require create, update, and scale operations for workload resources during network disconnects.
- Local clusters use Amazon EBS as the default storage class for persistent volumes and the Amazon EBS CSI driver to manage the lifecycle of Amazon EBS persistent volumes. During network disconnects, Pods that are backed by Amazon EBS can't be created, updated, or scaled. This is because these operations require calls to the Amazon EBS API in the cloud. If you're deploying stateful workloads on local clusters and require create, update, or scale operations during network disconnects, consider using an alternative storage mechanism.
- Amazon EBS snapshots can't be created or deleted if AWS Outposts can't access the relevant AWS in-region APIs (such as the APIs for Amazon EBS or Amazon S3).
- When integrating ALB (Ingress) with AWS Certificate Manager (ACM), certificates are pushed and stored in memory of the AWS Outposts ALB Compute instance. Current TLS termination will continue to operate in the event of a disconnect from the AWS Region. Mutating operations in this context will fail (such as new ingress definitions, new ACM based certificates API operations, ALB compute scale, or certificate rotation). For more information, see [Troubleshooting managed certificate renewal](#) in the *AWS Certificate Manager User Guide*.
- The Amazon EKS control plane logs are cached locally on the Kubernetes control plane instances during network disconnects. Upon reconnect, the logs are sent to CloudWatch Logs in the parent AWS Region. You can use [Prometheus](#), [Grafana](#), or Amazon EKS partner solutions to monitor the cluster locally using the Kubernetes API server's metrics endpoint or using Fluent Bit for logs.

- If you're using the AWS Load Balancer Controller on Outposts for application traffic, existing Pods fronted by the AWS Load Balancer Controller continue to receive traffic during network disconnects. New Pods created during network disconnects don't receive traffic until the Outpost is reconnected to the AWS Cloud. Consider setting the replica count for your applications while connected to the AWS Cloud to accommodate your scaling needs during network disconnects.
- The Amazon VPC CNI plugin for Kubernetes defaults to [secondary IP mode](#). It's configured with WARM_ENI_TARGET=1, which allows the plugin to keep "a full elastic network interface" of available IP addresses available. Consider changing WARM_ENI_TARGET, WARM_IP_TARGET, and MINIMUM_IP_TARGET values according to your scaling needs during a disconnected state. For more information, see the [readme](#) file for the plugin on GitHub. For a list of the maximum number of Pods that's supported by each instance type, see the [eni-max-pods.txt](#) file on GitHub.

Authenticating to your local cluster during a network disconnect

AWS Identity and Access Management (IAM) isn't available during network disconnects. You can't authenticate to your local cluster using IAM credentials while disconnected. However, you can connect to your cluster over your local network using x509 certificates when disconnected. You need to download and store a client X509 certificate to use during disconnects. In this topic, you learn how to create and use the certificate to authenticate to your cluster when it's in a disconnected state.

1. Create a certificate signing request.

- a. Generate a certificate signing request.

```
openssl req -new -newkey rsa:4096 -nodes -days 365 \
-keyout admin.key -out admin.csr -subj "/CN=admin"
```

- b. Create a certificate signing request in Kubernetes.

```
BASE64_CSR=$(cat admin.csr | base64 -w 0)
cat << EOF > admin-csr.yaml
apiVersion: certificates.k8s.io/v1
kind: CertificateSigningRequest
metadata:
  name: admin-csr
spec:
  signerName: kubernetes.io/kube-apiserver-client
  request: ${BASE64_CSR}
  usages:
  - client auth
EOF
```

2. Create a certificate signing request using kubectl.

```
kubectl create -f admin-csr.yaml
```

3. Check the status of the certificate signing request.

```
kubectl get csr admin-csr
```

An example output is as follows.

NAME	AGE	REQUESTOR	CONDITION
admin-csr	11m	kubernetes-admin	Pending

Kubernetes created the certificate signing request.

4. Approve the certificate signing request.

```
kubectl certificate approve admin-csr
```

5. Recheck the certificate signing request status for approval.

```
kubectl get csr admin-csr
```

An example output is as follows.

NAME	AGE	REQUESTOR	CONDITION
admin-csr	11m	kubernetes-admin	Approved

6. Retrieve and verify the certificate.

- a. Retrieve the certificate.

```
kubectl get csr admin-csr -o jsonpath='{.status.certificate}' | base64 --decode > admin.crt
```

- b. Verify the certificate.

```
cat admin.crt
```

7. Create a cluster role binding for an admin user.

```
kubectl create clusterrolebinding admin --clusterrole=cluster-admin \
--user=admin --group=system:masters
```

8. Generate a user-scoped kubeconfig for a disconnected state.

You can generate a kubeconfig file using the downloaded admin certificates. Replace *my-cluster* and *apiserver-endpoint* in the following commands.

```
aws eks describe-cluster --name my-cluster \
--query "cluster.certificateAuthority" \
--output text | base64 --decode > ca.crt
```

```
kubectl config --kubeconfig admin.kubeconfig set-cluster my-cluster \
--certificate-authority=ca.crt --server apiserver-endpoint --embed-certs
```

```
kubectl config --kubeconfig admin.kubeconfig set-credentials admin \
--client-certificate=admin.crt --client-key=admin.key --embed-certs
```

```
kubectl config --kubeconfig admin.kubeconfig set-context admin@my-cluster \
--cluster my-cluster --user admin
```

```
kubectl config --kubeconfig admin.kubeconfig use-context admin@my-cluster
```

9. View your kubeconfig file.

```
kubectl get nodes --kubeconfig admin.kubeconfig
```

10. If you have services already in production on your Outpost, skip this step. If Amazon EKS is the only service running on your Outpost and the Outpost isn't currently in production, you can simulate a network disconnect. Before you go into production with your local cluster, simulate a disconnect to make sure that you can access your cluster when it's in a disconnected state.
 - a. Apply firewall rules on the networking devices that connect your Outpost to the AWS Region. This disconnects the service link of the Outpost. You can't create any new instances. Currently running instances lose connectivity to the AWS Region and the internet.
 - b. You can test the connection to your local cluster while disconnected using the x509 certificate. Make sure to change your kubeconfig to the admin.kubeconfig that you created in a previous step. Replace *my-cluster* with the name of your local cluster.

```
kubectl config use-context admin@my-cluster --kubeconfig admin.kubeconfig
```

If you notice any issues with your local clusters while they're in a disconnected state, we recommend opening a support ticket.

Capacity considerations

This topic provides guidance for selecting the Kubernetes control plane instance type and (optionally) using placement groups to meet high-availability requirements for your local Amazon EKS cluster on an Outpost.

Before you select an instance type (such as m5, c5, or r5) to use for your local cluster's Kubernetes control plane on Outposts, confirm the instance types that are available on your Outpost configuration. After you identify the available instance types, select the instance size (such as large, xlarge, or 2xlarge) based on the number of nodes that your workloads require. The following table provides recommendations for choosing an instance size.

Note

The instance sizes must be slotted on your Outposts. Make sure that you have enough capacity for three instances of the size available on your Outposts for the lifetime of your local cluster. For a list of the available Amazon EC2 instance types, see the Compute and storage sections in [AWS Outposts rack features](#).

Number of nodes	Kubernetes control plane instance size
1–20	large
21–100	xlarge
101–250	2xlarge
251–500	4xlarge

The storage for the Kubernetes control plane requires 246 GB of Amazon EBS storage for each local cluster to meet etcd's required IOPS. When the local cluster is created, the Amazon EBS volumes are provisioned automatically for you.

Control plane placement

When you don't specify a placement group with the `OutpostConfig.ControlPlanePlacement.GroupName` property, the Amazon EC2 instances

provisioned for your Kubernetes control plane don't receive any specific hardware placement enforcement across the underlying capacity available on your Outpost.

You can use placement groups to meet the high-availability requirements for your local Amazon EKS cluster on an Outpost. By specifying a placement group during cluster creation, you influence the placement of the Kubernetes control plane instances. The instances are spread across independent underlying hardware (racks or hosts), minimizing correlated instance impact on the event of hardware failures.

Requirements

The type of spread that you can configure depends on the number of Outpost racks you have in your deployment.

- **Deployments with one or two physical racks in a single logical Outpost** – You must have at least three hosts that are configured with the instance type that you choose for your Kubernetes control plane instances. A *spread* placement group using *host-level spread* ensures that all Kubernetes control plane instances run on distinct hosts within the underlying racks available in your Outpost deployment.
- **Deployments with three or more physical racks in a single logical Outpost** – You must have at least three hosts configured with the instance type you choose for your Kubernetes control plane instances. A *spread* placement group using *rack-level spread* ensures that all Kubernetes control plane instances run on distinct racks in your Outpost deployment. You can alternatively use the *host-level spread* placement group as described in the previous option.

You are responsible for creating the desired placement group. You specify the placement group when calling the `CreateCluster` API. For more information about placement groups and how to create them, see [Placement Groups](#) in the Amazon EC2 User Guide for Linux Instances.

Considerations

- When a placement group is specified, there must be available slotted capacity on your Outpost to successfully create a local Amazon EKS cluster. The capacity varies based on whether you use the host or rack spread type. If there isn't enough capacity, the cluster remains in the `Creating` state. You are able to check the `Insufficient Capacity Error` on the `health` field of the [DescribeCluster](#) API response. You must free capacity for the creation process to progress.
- During Amazon EKS local cluster platform and version updates, the Kubernetes control plane instances from your cluster are replaced by new instances using a rolling update strategy. During this replacement process, each control plane instance is terminated, freeing up its respective slot. A new updated instance is provisioned in its place. The updated instance might be placed in the slot that was released. If the slot is consumed by another unrelated instance and there is no more capacity left that respects the required spread topology requirement, then the cluster remains in the `Updating` state. You are able to see the respective `Insufficient Capacity Error` on the `health` field of the [DescribeCluster](#) API response. You must free capacity so the update process can progress and reestablish prior high availability levels.
- You can create a maximum of 500 placement groups per account in each AWS Region. For more information, see [General rules and limitations](#) in the Amazon EC2 User Guide for Linux Instances.

Troubleshooting local clusters for Amazon EKS on AWS Outposts

This topic covers some common errors that you might see while using local clusters and how to troubleshoot them. Local clusters are similar to Amazon EKS clusters in the cloud, but there are some differences in how they're managed by Amazon EKS.

API behavior

Local clusters are created through the Amazon EKS API, but are run in an asynchronous manner. This means that requests to the Amazon EKS API return immediately for local clusters. However, these requests might succeed, fail fast because of input validation errors, or fail and have descriptive validation errors. This behavior is similar to the Kubernetes API.

Local clusters don't transition to a FAILED status. Amazon EKS attempts to reconcile the cluster state with the user-requested desired state in a continuous manner. As a result, a local cluster might remain in the CREATING state for an extended period of time until the underlying issue is resolved.

Describe cluster health field

Local cluster issues can be discovered using the [describe-cluster](#) Amazon EKS AWS CLI command. Local cluster issues are surfaced by the `cluster.health` field of the `describe-cluster` command's response. The message contained in this field includes an error code, descriptive message, and related resource IDs. This information is available through the Amazon EKS API and AWS CLI only. In the following example, replace `my-cluster` with the name of your local cluster.

```
aws eks describe-cluster --name my-cluster --query 'cluster.health'
```

An example output is as follows.

```
{
  "issues": [
    {
      "code": "ConfigurationConflict",
      "message": "The instance type 'm5.large' is not supported in Outpost 'my-
outpost-arn'.",
      "resourceIds": [
        "my-cluster-arn"
      ]
    }
  ]
}
```

If the problem is beyond repair, you might need to delete the local cluster and create a new one. For example, trying to provision a cluster with an instance type that's not available on your Outpost. The following table includes common health related errors.

Error scenario	Code	Message	ResourceIds
Provided subnets couldn't be found.	ResourceNotFound	The subnet ID <code>subnet-id</code> does not exist	All provided subnet IDs
Provided subnets don't belong to the same VPC.	ConfigurationConflict	Subnets specified must belong to the same VPC	All provided subnet IDs
Some provided subnets don't belong to the specified Outpost.	ConfigurationConflict	Subnet <code>subnet-id</code> expected to be in <code>outpost-arn</code> , but is in <code>other-outpost-arn</code>	Problematic subnet ID

Error scenario	Code	Message	Resource IDs
Some provided subnets don't belong to any Outpost.	ConfigurationConflict	Subnet <i>subnet-id</i> is not part of any Outpost	Problematic subnet ID
Some provided subnets don't have enough free addresses to create elastic network interfaces for control plane instances.	ResourceLimitExceeded	The specified subnet does not have enough free addresses to satisfy the request.	Problematic subnet ID
The specified control plane instance type isn't supported on your Outpost.	ConfigurationConflict	The instance type <i>type</i> is not supported in Outpost <i>outpost-arn</i>	Cluster ARN
You terminated a control plane Amazon EC2 instance or <code>run-instance</code> succeeded, but the state observed changes to Terminated. This can happen for a period of time after your Outpost reconnects and Amazon EBS internal errors cause an Amazon EC2 internal work flow to fail.	InternalFailure	EC2 instance state "Terminated" is unexpected	Cluster ARN
You have insufficient capacity on your Outpost. This can also happen when a cluster is being created if an Outpost is disconnected from the AWS Region.	ResourceLimitExceeded	There is not enough capacity on the Outpost to launch or start the instance.	Cluster ARN
Your account exceeded your security group quota.	ResourceLimitExceeded	Error message returned by Amazon EC2 API	Target VPC ID
Your account exceeded your elastic network interface quota.	ResourceLimitExceeded	Error message returned by Amazon EC2 API	Target subnet ID

Error scenario	Code	Message	Resource IDs
Control plane instances weren't reachable through AWS Systems Manager. For resolution, see the section called "Control plane instances aren't reachable through AWS Systems Manager" (p. 614) .	ClusterUnreachable	Amazon EKS control plane instances are not reachable through SSM. Please verify your SSM and network configuration, and reference the EKS on Outposts troubleshooting documentation.	Amazon EC2 instance IDs
An error occurred while getting details for a managed security group or elastic network interface.	Based on Amazon EC2 client error code.	Error message returned by Amazon EC2 API	All managed security group IDs
An error occurred while authorizing or revoking security group ingress rules. This applies to both the cluster and control plane security groups.	Based on Amazon EC2 client error code.	Error message returned by Amazon EC2 API	Problematic security group ID
An error occurred while deleting an elastic network interface for a control plane instance.	Based on Amazon EC2 client error code.	Error message returned by Amazon EC2 API	Problematic elastic network interface ID

The following table lists errors from other AWS services that are presented in the health field of the `describe-cluster` response.

Amazon EC2 error code	Cluster health issue code	Description
AuthFailure	AccessDenied	This error can occur for a variety of reasons. The most common reason is that you accidentally removed a tag that the service uses to scope down the service linked role policy from the control plane. If this occurs, Amazon EKS can no longer manage and monitor these AWS resources.
UnauthorizedOperation	AccessDenied	This error can occur for a variety of reasons. The most common reason is that you accidentally removed a tag that the service uses to scope down the service linked role policy from the control plane. If this occurs, Amazon EKS can no longer

Amazon EC2 error code	Cluster health issue code	Description
		manage and monitor these AWS resources.
InvalidSubnetID.NotFound	ResourceNotFound	This error occurs when subnet ID for the ingress rules of a security group can't be found.
InvalidPermission.NotFound	ResourceNotFound	This error occurs when the permissions for the ingress rules of a security group aren't correct.
InvalidGroup.NotFound	ResourceNotFound	This error occurs when the group of the ingress rules of a security group can't be found.
InvalidNetworkInterfaceID.NotFound	ResourceNotFound	This error occurs when the network interface ID for the ingress rules of a security group can't be found.
InsufficientFreeAddressesInSubnet	ResourceLimitExceeded	This error occurs when the subnet resource quota is exceeded.
InsufficientCapacityOnOutputPort	ResourceLimitExceeded	This error occurs when the outpost capacity quota is exceeded.
NetworkInterfaceLimitExceeded	ResourceLimitExceeded	This error occurs when the elastic network interface quota is exceeded.
SecurityGroupLimitExceeded	ResourceLimitExceeded	This error occurs when the security group quota is exceeded.
VcpuLimitExceeded	ResourceLimitExceeded	This is observed when creating an Amazon EC2 instance in a new account. The error might be similar to the following: "You have requested more vCPU capacity than your current vCPU limit of 32 allows for the instance bucket that the specified instance type belongs to. Please visit http://aws.amazon.com/contact-us/ec2-request to request an adjustment to this limit."
InvalidParameterValue	ConfigurationConflict	Amazon EC2 returns this error code if the specified instance type isn't supported on the Outpost.

Amazon EC2 error code	Cluster health issue code	Description
All other failures	InternalFailure	None

Unable to create or modify clusters

Local clusters require different permissions and policies than Amazon EKS clusters that are hosted in the cloud. When a cluster fails to create and produces an `InvalidPermissions` error, double check that the cluster role that you're using has the [AmazonEKSLocalOutpostClusterPolicy \(p. 515\)](#) managed policy attached to it. All other API calls require the same set of permissions as Amazon EKS clusters in the cloud.

Cluster is stuck in CREATING state

The amount of time it takes to create a local cluster varies depending on several factors. These factors include your network configuration, Outpost configuration, and the cluster's configuration. In general, a local cluster is created and changes to the ACTIVE status within 15–20 minutes. If a local cluster remains in the CREATING state, you can call `describe-cluster` for information about the cause in the `cluster.health` output field.

The most common issues are the following:

AWS Systems Manager (Systems Manager) encounters the following issues:

- Your cluster can't connect to the control plane instance from the AWS Region that Systems Manager is in. You can verify this by calling `aws ssm start-session --target instance-id` from an in-Region bastion host. If that command doesn't work, check if Systems Manager is running on the control plane instance. Or, another work around is to delete the cluster and then recreate it.
- Systems Manager control plane instances might not have internet access. Check if the subnet that you provided when you created the cluster has a NAT gateway and a VPC with an internet gateway. Use VPC reachability analyzer to verify that the control plane instance can reach the internet gateway. For more information, see [Getting started with VPC Reachability Analyzer](#).
- The role ARN that you provided is missing policies. Check if the [the section called "AmazonEKSLocalOutpostClusterPolicy" \(p. 515\)](#) was removed from the role. This can also occur if an AWS CloudFormation stack is misconfigured.

Multiple subnets are misconfigured and specified when a cluster is created:

- All the provided subnets must be associated with the same Outpost and must reach each other. When multiple subnets are specified when a cluster is created, Amazon EKS attempts to spread the control plane instances across multiple subnets.
- The Amazon EKS managed security groups are applied at the elastic network interface. However, other configuration elements such as NACL firewall rules might conflict with the rules for the elastic network interface.

VPC and subnet DNS configuration is misconfigured or missing

Review [the section called "VPC and subnet requirements" \(p. 601\)](#).

Can't join nodes to a cluster

Common causes:

- AMI issues:

- You're using an unsupported AMI. You must use [v20220620](#) or later for the [the section called "Amazon Linux" \(p. 156\)](#) Amazon EKS optimized Amazon Linux.
- If you used an AWS CloudFormation template to create your nodes, make sure it wasn't using an unsupported AMI.
- Missing the AWS IAM Authenticator ConfigMap – If it's missing, you must create it. For more information, see [the section called "Apply the aws-authConfigMap to your cluster" \(p. 426\)](#).
- The wrong security group is used – Make sure to use eks-cluster-sg-*cluster-name-uniqueid* for your worker nodes' security group. The selected security group is changed by AWS CloudFormation to allow a new security group each time the stack is used.
- Following unexpected private link VPC steps – Wrong CA data (--b64-cluster-ca) or API Endpoint (--apiserver-endpoint) are passed.
- Misconfigured Pod security policy:
 - The CoreDNS and Amazon VPC CNI plugin for Kubernetes Daemonsets must run on nodes for nodes to join and communicate with the cluster.
 - The Amazon VPC CNI plugin for Kubernetes requires some privileged networking features to work properly. You can view the privileged networking features with the following command: kubectl describe psp eks.privileged.

We don't recommend modifying the default pod security policy. For more information, see [the section called "Pod security policy" \(p. 522\)](#).

Collecting logs

When an Outpost gets disconnected from the AWS Region that it's associated with, the Kubernetes cluster likely will continue working normally. However, if the cluster doesn't work properly, follow the troubleshooting steps in [the section called "Network disconnects" \(p. 604\)](#). If you encounter other issues, contact AWS Support. AWS Support can guide you on downloading and running a log collection tool. That way, you can collect logs from your Kubernetes cluster control plane instances and send them to AWS Support support for further investigation.

Control plane instances aren't reachable through AWS Systems Manager

When the Amazon EKS control plane instances aren't reachable through AWS Systems Manager (Systems Manager), Amazon EKS displays the following error for your cluster.

Amazon EKS control plane instances are not reachable through SSM. Please verify your SSM and network configuration, and reference the EKS on Outposts troubleshooting documentation.

To resolve this issue, make sure that your VPC and subnets meet the requirements in [the section called "VPC and subnet requirements" \(p. 601\)](#) and that you completed the steps in [Setting up Session Manager](#) in the AWS Systems Manager User Guide.

Launching self-managed Amazon Linux nodes on an Outpost

This topic describes how you can launch Auto Scaling groups of Amazon Linux nodes on an Outpost that register with your Amazon EKS cluster. The cluster can be on the AWS Cloud or on an Outpost.

Prerequisites

- An existing Outpost. For more information, see [What is AWS Outposts](#).

- An existing Amazon EKS cluster. To deploy a cluster on the AWS Cloud, see [the section called “Creating a cluster” \(p. 25\)](#). To deploy a cluster on an Outpost, see [the section called “Local clusters” \(p. 590\)](#).
- Suppose that you’re creating your nodes in a cluster on the AWS Cloud and you have subnets in the AWS Region where you have AWS Outposts, AWS Wavelength, or AWS Local Zones enabled. Then, those subnets must not have been passed in when you created your cluster. If you’re creating your nodes in a cluster on an Outpost, you must have passed in an Outpost subnet when creating your cluster.
- (Recommended for clusters on the AWS Cloud) The Amazon VPC CNI plugin for Kubernetes add-on configured with its own IAM role that has the necessary IAM policy attached to it. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#). Local clusters do not support IAM roles for service accounts.

You can create a self-managed Amazon Linux node group with `eksctl` or the AWS Management Console (with an AWS CloudFormation template). You can also use [Terraform](#).

`eksctl`

Prerequisite

Version `0.160.0` or later of the `eksctl` command line tool installed on your device or AWS CloudShell. To install or update `eksctl`, see [Installing or updating eksctl \(p. 13\)](#).

To launch self-managed Linux nodes using `eksctl`

1. If your cluster is on the AWS Cloud and the `AmazonEKS_CNI_Policy` managed IAM policy is attached to your [the section called “Node IAM role” \(p. 501\)](#), we recommend assigning it to an IAM role that you associate to the Kubernetes `aws-node` service account instead. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#). If your cluster is on your Outpost, the policy must be attached to your node role.
2. The following command creates a node group in an existing cluster. The cluster must have been created using `eksctl`. Replace `al-nodes` with a name for your node group. The node group name can’t be longer than 63 characters. It must start with letter or digit, but can also include hyphens and underscores for the remaining characters. Replace `my-cluster` with the name of your cluster. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can’t be longer than 100 characters. If your cluster exists on an Outpost, replace `id` with the ID of an Outpost subnet. If your cluster exists on the AWS Cloud, replace `id` with the ID of a subnet that you didn’t specify when you created your cluster. Replace `instance-type` with an instance type supported by your Outpost. Replace the remaining `example values` with your own values. The nodes are created with the same Kubernetes version as the control plane, by default.

Replace `instance-type` with an instance type available on your Outpost.

Replace `my-key` with the name of your Amazon EC2 key pair or public key. This key is used to SSH into your nodes after they launch. If you don’t already have an Amazon EC2 key pair, you can create one in the AWS Management Console. For more information, see [Amazon EC2 key pairs](#) in the [Amazon EC2 User Guide for Linux Instances](#).

Create your node group with the following command.

```
eksctl create nodegroup --cluster my-cluster --name al-nodes --node-type instance-type \
    --nodes 3 --nodes-min 1 --nodes-max 4 --managed=false --node-volume-type gp2 --
    subnet-ids subnet-id
```

If your cluster is deployed on the AWS Cloud:

- The node group that you deploy can assign IPv4 addresses to Pods from a different CIDR block than that of the instance. For more information, see [Custom networking for pods \(p. 306\)](#).
- The node group that you deploy doesn't require outbound internet access. For more information, see [Private cluster requirements \(p. 58\)](#).

For a complete list of all available options and defaults, see [AWS Outposts Support](#) in the eksctl documentation.

If nodes fail to join the cluster, then see [Nodes fail to join cluster \(p. 562\)](#) in [Troubleshooting \(p. 562\)](#) and [the section called "Can't join nodes to a cluster" \(p. 613\)](#) in [the section called "Troubleshooting" \(p. 608\)](#).

An example output is as follows. Several lines are output while the nodes are created. One of the last lines of output is the following example line.

```
[#]  created 1 nodegroup(s) in cluster "my-cluster"
```

3. (Optional) Deploy a [sample application \(p. 356\)](#) to test your cluster and Linux nodes.

AWS Management Console

Step 1: To launch self-managed Amazon Linux nodes using the AWS Management Console

1. Download the latest version of the AWS CloudFormation template.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2022-12-23/amazon-eks-nodegroup.yaml
```

2. Open the AWS CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
3. Choose **Create stack** and then select **With new resources (standard)**.
4. For **Specify template**, select **Upload a template file** and then select **Choose file**. Select the amazon-eks-nodegroup.yaml file that you downloaded in a previous step and then select **Next**.
5. On the **Specify stack details** page, enter the following parameters accordingly, and then choose **Next**:
 - **Stack name**: Choose a stack name for your AWS CloudFormation stack. For example, you can call it **al-nodes**. The name can contain only alphanumeric characters (case-sensitive) and hyphens. It must start with an alphabetic character and can't be longer than 100 characters.
 - **ClusterName**: Enter the name of your cluster. If this name doesn't match your cluster name, your nodes can't join the cluster.
 - **ClusterControlPlaneSecurityGroup**: Choose the **SecurityGroups** value from the AWS CloudFormation output that you generated when you created your [VPC \(p. 259\)](#).

The following steps show one operation to retrieve the applicable group.

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose the name of the cluster.
3. Choose the **Networking** tab.
4. Use the **Additional security groups** value as a reference when selecting from the **ClusterControlPlaneSecurityGroup** dropdown list.

- **NodeGroupName:** Enter a name for your node group. This name can be used later to identify the Auto Scaling node group that's created for your nodes.
- **NodeAutoScalingGroupMinSize:** Enter the minimum number of nodes that your node Auto Scaling group can scale in to.
- **NodeAutoScalingGroupDesiredCapacity:** Enter the desired number of nodes to scale to when your stack is created.
- **NodeAutoScalingGroupMaxSize:** Enter the maximum number of nodes that your node Auto Scaling group can scale out to.
- **NodeInstanceType:** Choose an instance type for your nodes. If your cluster is running on the AWS Cloud, then for more information, see [Choosing an Amazon EC2 instance type \(p. 152\)](#). If your cluster is running on an Outpost, then you can only select an instance type that is available on your Outpost.
- **NodeImageIdSSMParam:** Pre-populated with the Amazon EC2 Systems Manager parameter of a recent Amazon EKS optimized AMI for a variable Kubernetes version. To use a different Kubernetes minor version supported with Amazon EKS, replace **1.XX** with a different [supported version \(p. 60\)](#). We recommend specifying the same Kubernetes version as your cluster.

To use the Amazon EKS optimized accelerated AMI, replace **amazon-linux-2** with **amazon-linux-2-gpu**. To use the Amazon EKS optimized Arm AMI, replace **amazon-linux-2** with **amazon-linux-2-arm64**.

Note

The Amazon EKS node AMI is based on Amazon Linux 2. You can track security or privacy events for Amazon Linux 2 at the [Amazon Linux Security Center](#) or subscribe to the associated [RSS feed](#). Security and privacy events include an overview of the issue, what packages are affected, and how to update your instances to correct the issue.

- **NodeImageId:** (Optional) If you're using your own custom AMI (instead of the Amazon EKS optimized AMI), enter a node AMI ID for your AWS Region. If you specify a value here, it overrides any values in the **NodeImageIdSSMParam** field.
- **NodeVolumeSize:** Specify a root volume size for your nodes, in GiB.
- **NodeVolumeType:** Specify a root volume type for your nodes.
- **KeyName:** Enter the name of an Amazon EC2 SSH key pair that you can use to connect using SSH into your nodes with after they launch. If you don't already have an Amazon EC2 key pair, you can create one in the AWS Management Console. For more information, see [Amazon EC2 key pairs](#) in the [Amazon EC2 User Guide for Linux Instances](#).

Note

If you don't provide a key pair here, the AWS CloudFormation stack creation fails.

- **BootstrapArguments:** There are several optional arguments that you can pass to your nodes. For more information, view the [bootstrap script usage information](#) on GitHub. If you're adding nodes to a cluster that doesn't have an ingress and egress internet connection (also known as private clusters), then you must provide the following bootstrap arguments (as a single line).

```
--b64-cluster-ca ${CLUSTER_CA} --apiserver-endpoint https://${APISERVER_ENDPOINT}  
--enable-local-outpost true --container-runtime containerd --cluster-id  
${CLUSTER_ID}
```

- **DisableIMDSv1:** By default, each node supports the Instance Metadata Service Version 1 (IMDSv1) and IMDSv2. You can disable IMDSv1. To prevent future nodes and Pods in the node group from using IMDSv1, set **DisableIMDSv1** to **true**. For more information about IMDS, see [Configuring the instance metadata service](#). For more information about restricting access to it on your nodes, see [Restrict access to the instance profile assigned to the worker node](#).

- **VpcId:** Enter the ID for the [VPC \(p. 259\)](#) that you created. Before choosing a VPC, review [the section called "VPC requirements and considerations" \(p. 602\)](#).
 - **Subnets:** If your cluster is on an Outpost, then choose at least one private subnet in your VPC. Before choosing subnets, review [Subnet requirements and considerations \(p. 602\)](#). You can see which subnets are private by opening each subnet link from the **Networking** tab of your cluster.
6. Select your desired choices on the **Configure stack options** page, and then choose **Next**.
 7. Select the check box to the left of **I acknowledge that AWS CloudFormation might create IAM resources.**, and then choose **Create stack**.
 8. When your stack has finished creating, select it in the console and choose **Outputs**.
 9. Record the **NodeInstanceRole** for the node group that was created. You need this when you configure your Amazon EKS nodes.

Step 2: To enable nodes to join your cluster

1. Check to see if you already have an aws-auth ConfigMap.

```
kubectl describe configmap -n kube-system aws-auth
```

2. If you are shown an aws-auth ConfigMap, then update it as needed.

- a. Open the ConfigMap for editing.

```
kubectl edit -n kube-system configmap/aws-auth
```

- b. Add a new mapRoles entry as needed. Set the rolearn value to the **NodeInstanceRole** value that you recorded in the previous procedure.

```
[...]
data:
  mapRoles: |
    - rolearn: <ARN of instance role (not instance profile)>
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
[...]
```

- c. Save the file and exit your text editor.
3. If you received an error stating "Error from server (NotFound): configmaps "aws-auth" not found, then apply the stock ConfigMap.

- a. Download the configuration map.

```
curl -O https://s3.us-west-2.amazonaws.com/amazon-eks/cloudformation/2020-10-29/aws-auth-cm.yaml
```

- b. In the aws-auth-cm.yaml file, set the rolearn to the **NodeInstanceRole** value that you recorded in the previous procedure. You can do this with a text editor, or by replacing **my-node-instance-role** and running the following command:

```
sed -i.bak -e 's|<ARN of instance role (not instance profile)>|my-node-instance-role|' aws-auth-cm.yaml
```

- c. Apply the configuration. This command may take a few minutes to finish.

```
kubectl apply -f aws-auth-cm.yaml
```

4. Watch the status of your nodes and wait for them to reach the Ready status.

```
kubectl get nodes --watch
```

Enter Ctrl+C to return to a shell prompt.

Note

If you receive any authorization or resource type errors, see [Unauthorized or access denied \(kubectl\) \(p. 563\)](#) in the troubleshooting topic.

If nodes fail to join the cluster, then see [Nodes fail to join cluster \(p. 562\)](#) in [Troubleshooting \(p. 562\)](#) and the section called "Can't join nodes to a cluster" (p. 613) in the section called "Troubleshooting" (p. 608).

5. Install the Amazon EBS CSI driver. For more information, see [Installation](#) on GitHub. In the **Set up driver permission** section, make sure to follow the instruction for the **Using IAM instance profile** option. You must use the gp2 storage class. The gp3 storage class isn't supported.

To create a gp2 storage class on your cluster, complete the following steps.

1. Run the following command to create the gp2-storage-class.yaml file.

```
cat >gp2-storage-class.yaml <<EOF
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
  name: ebs-sc
provisioner: ebs.csi.aws.com
volumeBindingMode: WaitForFirstConsumer
parameters:
  type: gp2
  encrypted: "true"
allowVolumeExpansion: true
EOF
```

2. Apply the manifest to your cluster.

```
kubectl apply -f gp2-storage-class.yaml
```

6. (GPU nodes only) If you chose a GPU instance type and the Amazon EKS optimized accelerated AMI, you must apply the [NVIDIA device plugin for Kubernetes](#) as a DaemonSet on your cluster. Replace vX.X.X with your desired [NVIDIA/k8s-device-plugin](#) version before running the following command.

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/vX.X.X/nvidia-device-plugin.yaml
```

Step 3: Additional actions

1. (Optional) Deploy a [sample application \(p. 356\)](#) to test your cluster and Linux nodes.
2. If your cluster is deployed on an Outpost, then skip this step. If your cluster is deployed on the AWS Cloud, the following information is optional. If the **AmazonEKS_CNI_Policy** managed IAM policy is attached to your [the section called "Node IAM role" \(p. 501\)](#), we recommend assigning

it to an IAM role that you associate to the Kubernetes aws-node service account instead. For more information, see [Configuring the Amazon VPC CNI plugin for Kubernetes to use IAM roles for service accounts \(p. 272\)](#).

Related projects

These open-source projects extend the functionality of Kubernetes clusters running on or outside of AWS, including clusters managed by Amazon EKS.

Management tools

Related management tools for Amazon EKS and Kubernetes clusters.

eksctl

eksctl is a simple CLI tool for creating clusters on Amazon EKS.

- [Project URL](#)
- [Project documentation](#)
- AWS open source blog: [eksctl: Amazon EKS cluster with one command](#)

AWS controllers for Kubernetes

With AWS Controllers for Kubernetes, you can create and manage AWS resources directly from your Kubernetes cluster.

- [Project URL](#)
- AWS open source blog: [AWS service operator for Kubernetes now available](#)

Flux CD

Flux is a tool that you can use to manage your cluster configuration using Git. It uses an operator in the cluster to trigger deployments inside of Kubernetes. For more information about operators, see [OperatorHub.io](#) on GitHub.

- [Project URL](#)
- [Project documentation](#)

CDK for Kubernetes

With the CDK for Kubernetes (cdk8s), you can define Kubernetes apps and components using familiar programming languages. cdk8s apps synthesize into standard Kubernetes manifests, which can be applied to any Kubernetes cluster.

- [Project URL](#)
- [Project documentation](#)
- AWS containers blog: [Introducing cdk8s+: Intent-driven APIs for Kubernetes objects](#)

Networking

Related networking projects for Amazon EKS and Kubernetes clusters.

Amazon VPC CNI plugin for Kubernetes

Amazon EKS supports native VPC networking through the Amazon VPC CNI plugin for Kubernetes. The plugin assigns an IP address from your VPC to each Pod.

- [Project URL](#)
- [Project documentation](#)

AWS Load Balancer Controller for Kubernetes

The AWS Load Balancer Controller helps manage AWS Elastic Load Balancers for a Kubernetes cluster. It satisfies Kubernetes Ingress resources by provisioning AWS Application Load Balancers. It satisfies Kubernetes service resources by provisioning AWS Network Load Balancers.

- [Project URL](#)
- [Project documentation](#)

ExternalDNS

ExternalDNS synchronizes exposed Kubernetes services and ingresses with DNS providers including Amazon Route 53 and AWS Service Discovery.

- [Project URL](#)
- [Project documentation](#)

Security

Related security projects for Amazon EKS and Kubernetes clusters.

AWS IAM authenticator

A tool to use AWS IAM credentials to authenticate to a Kubernetes cluster if you're not using the AWS CLI version 1.16.156 or higher. For more information, see [Installing aws-iam-authenticator \(p. 436\)](#).

- [Project URL](#)
- [Project documentation](#)
- AWS open source blog: [Deploying the AWS IAM authenticator to kops](#)

Machine learning

Related machine learning projects for Amazon EKS and Kubernetes clusters.

Kubeflow

A machine learning toolkit for Kubernetes.

- [Project URL](#)
- [Project documentation](#)
- AWS open source blog: [Kubeflow on Amazon EKS](#)

Auto Scaling

Related auto scaling projects for Amazon EKS and Kubernetes clusters.

Cluster autoscaler

Cluster Autoscaler is a tool that automatically adjusts the size of the Kubernetes cluster based on CPU and memory pressure.

- [Project URL](#)
- [Project documentation](#)
- Amazon EKS workshop: <https://www.eksworkshop.com/>

Escalator

Escalator is a batch or job optimized horizontal autoscaler for Kubernetes.

- [Project URL](#)
- [Project documentation](#)

Monitoring

Related monitoring projects for Amazon EKS and Kubernetes clusters.

Prometheus

Prometheus is an open-source systems monitoring and alerting toolkit.

- [Project URL](#)
- [Project documentation](#)
- Amazon EKS workshop: https://eksworkshop.com/intermediate/240_monitoring/

Continuous integration / continuous deployment

Related CI/CD projects for Amazon EKS and Kubernetes clusters.

Jenkins X

CI/CD solution for modern cloud applications on Amazon EKS and Kubernetes clusters.

- [Project URL](#)
- [Project documentation](#)

Amazon EKS new features and roadmap

You can learn about new Amazon EKS features by scrolling to the What's New feed on the [What's New with AWS](#) page. You can also review the [roadmap](#) on GitHub, which lets you know about upcoming features and priorities so that you can plan how you want to use Amazon EKS in the future. You can provide direct feedback to us about the roadmap priorities.

Document history for Amazon EKS

The following table describes the major updates and new features for the Amazon EKS User Guide. We also update the documentation frequently to address the feedback that you send us.

Change	Description	Date
Preview release: Amazon EKS Extended Support for Kubernetes versions	Extended Kubernetes version support allows you to stay at a specific Kubernetes version for longer than 14 months.	October 4, 2023
Remove references to AWS App Mesh integration (p. 626)	Amazon EKS integrations with AWS App Mesh remain for existing customers of App Mesh only.	September 29, 2023
Kubernetes version 1.28	Added Kubernetes version 1.28 support for new clusters and version upgrades.	September 26, 2023
Existing clusters support Kubernetes network policy enforcement in the Amazon VPC CNI plugin for Kubernetes	You can use Kubernetes <i>network policy</i> in existing clusters with the Amazon VPC CNI plugin for Kubernetes, instead of requiring a third party solution.	September 15, 2023
CoreDNS Amazon EKS add-on supports modifying PDB	You can modify the PodDisruptionBudget of the EKS add-on for CoreDNS in versions v1.9.3-eksbuild.7 and later and v1.10.1-eksbuild.4 and later.	September 15, 2023
Amazon EKS support for shared subnets	New Shared subnet requirements and considerations for making Amazon EKS clusters in shared subnets.	September 7, 2023
Updates to What is Amazon EKS?	Added new Common use cases and Architecture topics. Refreshed other topics.	September 6, 2023
Kubernetes network policy enforcement in the Amazon VPC CNI plugin for Kubernetes	You can use Kubernetes <i>network policy</i> with the Amazon VPC CNI plugin for Kubernetes, instead of requiring a third party solution.	August 29, 2023
Amazon EKS AWS Region expansion (p. 626)	Amazon EKS is now available in the Israel (Tel Aviv) (il-central-1) AWS Region.	August 1, 2023
Configurable ephemeral storage for Fargate	You can increase the total amount of ephemeral storage for each Pod running on Amazon EKS Fargate.	July 31, 2023

<u>Add-on support for Amazon EFS CSI driver</u>	You can now use the AWS Management Console, AWS CLI, and API to manage the Amazon EFS CSI driver.	July 26, 2023
<u>AWS managed policy updates - New policy</u>	Amazon EKS added a new AWS managed policy.	July 26, 2023
<u>Kubernetes version updates for 1.27, 1.26, 1.25, and 1.24 are now available for local clusters on AWS Outposts</u>	Kubernetes version updates to 1.27.3, 1.26.6, 1.25.11, and 1.24.15 are now available for local clusters on AWS Outposts	July 20, 2023
<u>IP prefixes support for Windows nodes</u>	Assigning IP prefixes to your nodes can enable you to host a significantly higher number of Pods on your nodes than you can when assigning individual secondary IP addresses to your nodes.	July 6, 2023
<u>Amazon FSx for OpenZFS CSI driver</u>	You can now install the Amazon FSx for OpenZFS CSI driver on Amazon EKS clusters.	June 30, 2023
<u>Pods on Linux nodes in IPv4 clusters can now communicate with IPv6 endpoints.</u>	After assigning an IPv6 address to your node, your Pods' IPv4 address is network address translated to the IPv6 address of the node that it's running on.	June 19, 2023
<u>Windows managed node groups in AWS GovCloud (US-East) and AWS GovCloud (US-West)</u>	In the AWS GovCloud (US-East) and AWS GovCloud (US-West) AWS Regions, Amazon EKS managed node groups can now run Windows containers.	May 30, 2023
<u>Kubernetes version 1.27</u>	Added Kubernetes version 1.27 support for new clusters and version upgrades.	May 24, 2023
<u>Kubernetes version 1.26</u>	Added Kubernetes version 1.26 support for new clusters and version upgrades.	April 11, 2023
<u>Domainless gMSA</u>	You can now use domainless gMSA with Windows Pods.	March 27, 2023
<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the Asia Pacific (Melbourne) (ap-southeast-4) AWS Region.	March 10, 2023
<u>Amazon File Cache CSI driver</u>	You can now install the Amazon File Cache CSI driver on Amazon EKS clusters.	March 3, 2023

<u>Kubernetes version 1.25 is now available for local clusters on AWS Outposts</u>	You can now create an Amazon EKS local cluster on an Outpost using Kubernetes versions 1.22 – 1.25.	March 1, 2023
<u>Kubernetes version 1.25</u>	Added Kubernetes version 1.25 support for new clusters and version upgrades.	February 22, 2023
<u>AWS managed policy updates - Update to an existing policy</u>	Amazon EKS updated an existing AWS managed policy.	February 7, 2023
<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the Asia Pacific (Hyderabad) (ap-south-2), Europe (Zurich) (eu-central-2), and Europe (Spain) (eu-south-2) AWS Regions.	February 6, 2023
<u>Kubernetes versions 1.21 – 1.24 are now available for local clusters on AWS Outposts.</u>	You can now create an Amazon EKS local cluster on an Outpost using Kubernetes versions 1.21 – 1.24. Previously, only version 1.21 was available.	January 17, 2023
<u>Amazon EKS now supports AWS PrivateLink</u>	You can use an AWS PrivateLink to create a private connection between your VPC and Amazon EKS.	December 16, 2022
<u>Managed node group Windows support</u>	You can now use Windows for Amazon EKS managed node groups.	December 15, 2022
<u>Amazon EKS add-ons from independent software vendors are now available in the AWS Marketplace</u>	You can now browse and subscribe to Amazon EKS add-ons from independent software vendors through the AWS Marketplace.	November 28, 2022
<u>AWS managed policy updates - Update to an existing policy</u>	Amazon EKS updated an existing AWS managed policy.	November 17, 2022
<u>Kubernetes version 1.24</u>	Added Kubernetes version 1.24 support for new clusters and version upgrades.	November 15, 2022
<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the Middle East (UAE) (me-central-1) AWS Region.	November 3, 2022
<u>AWS managed policy updates - Update to an existing policy</u>	Amazon EKS updated an existing AWS managed policy.	October 24, 2022
<u>AWS managed policy updates - Update to an existing policy</u>	Amazon EKS updated an existing AWS managed policy.	October 20, 2022
<u>Local clusters on AWS Outposts are now available</u>	You can now create an Amazon EKS local cluster on an Outpost.	September 19, 2022

<u>Fargate vCPU based quotas</u>	Fargate is transitioning from Pod based quotas to vCPU based quotas.	September 8, 2022
<u>AWS managed policy updates - Update to an existing policy</u>	Amazon EKS updated an existing AWS managed policy.	August 31, 2022
<u>Cost monitoring</u>	Amazon EKS now supports Kubecost, which enables you to monitor costs broken down by Kubernetes resources including Pods, nodes, namespaces, and labels.	August 24, 2022
<u>AWS managed policy updates - New policy</u>	Amazon EKS added a new AWS managed policy.	August 24, 2022
<u>AWS managed policy updates - New policy</u>	Amazon EKS added a new AWS managed policy.	August 23, 2022
<u>Tag resources for billing</u>	Added aws:eks:cluster-name generated cost allocation tag support for all clusters.	August 16, 2022
<u>Fargate profile wildcards</u>	Added support for Fargate profile wildcards in the selector criteria for namespaces, label keys, and label values.	August 16, 2022
<u>Kubernetes version 1.23</u>	Added Kubernetes version 1.23 support for new clusters and version upgrades.	August 11, 2022
<u>View Kubernetes resources in the AWS Management Console</u>	You can now view information about the Kubernetes resources deployed to your cluster using the AWS Management Console.	May 3, 2022
<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the Asia Pacific (Jakarta) (ap-southeast-3) AWS Region.	May 2, 2022
<u>Observation page and ADOT add-on support</u>	Added Observability page and AWS Distro for OpenTelemetry (ADOT).	April 21, 2022
<u>Kubernetes version 1.22 (p. 626)</u>	Added Kubernetes version 1.22 support for new clusters and version upgrades.	April 4, 2022
<u>AWS managed policy updates - New policy</u>	Amazon EKS added a new AWS managed policy.	April 4, 2022
<u>Added Fargate Pod patching details</u>	When upgrading Fargate Pods, Amazon EKS first tries to evict Pods based on your Pod disruption budgets. You can create event rules to react to failed evictions before the Pods are deleted.	April 1, 2022

<u>Full release: Add-on support for Amazon EBS CSI driver</u>	You can now use the AWS Management Console, AWS CLI, and API to manage the Amazon EBS CSI driver.	March 31, 2022
<u>AWS Outposts content update</u>	Instructions to deploy an Amazon EKS cluster on AWS Outposts.	March 22, 2022
<u>AWS managed policy updates - Update to an existing policy</u>	Amazon EKS updated an existing AWS managed policy.	March 21, 2022
<u>Windows containerd support</u>	You can now select the containerd runtime for Windows nodes.	March 14, 2022
<u>Added Amazon EKS Connector considerations to security documentation</u>	Describes the shared responsibility model as it relates to connected clusters.	February 25, 2022
<u>Assign IPv6 addresses to your Pods and services</u>	You can now create a 1.21 or later cluster that assigns IPv6 addresses to your Pods and services.	January 6, 2022
<u>AWS managed policy updates - Update to an existing policy</u>	Amazon EKS updated an existing AWS managed policy.	December 13, 2021
<u>Preview release: Add-on support for Amazon EBS CSI driver</u>	You can now preview using the AWS Management Console, AWS CLI, and API to manage the Amazon EBS CSI driver.	December 9, 2021
<u>Karpenter autoscaler support</u>	You can now use the Karpenter open-source project to autoscale your nodes.	November 29, 2021
<u>Fluent Bit Kubernetes filter support in Fargate logging</u>	You can now use the Fluent Bit Kubernetes filter with Fargate logging.	November 10, 2021
<u>Windows support available in the control plane</u>	Windows support is now available in your control plane. You no longer need to enable it in your data plane.	November 9, 2021
<u>Bottlerocket added as an AMI type for managed node groups</u>	Previously, Bottlerocket was only available as a self-managed node option. Now it can be configured as a managed node group, reducing the effort that's required to meet node compliance requirements.	October 28, 2021

<u>DL1 driver support</u>	Custom Amazon Linux AMIs now support deep learning workloads for Amazon Linux 2. This enablement allows a generic on-premises or cloud baseline configuration.	October 25, 2021
<u>VT1 video support</u>	Custom Amazon Linux AMIs now support VT1 for some distributions. This enablement advertises Xilinx U30 devices on your Amazon EKS cluster.	September 13, 2021
<u>Amazon EKS Connector is now available</u>	You can use Amazon EKS Connector to register and connect any conformant Kubernetes cluster to AWS and visualize it in the Amazon EKS console.	September 8, 2021
<u>Amazon EKS Anywhere is now available</u>	Amazon EKS Anywhere is a new deployment option for Amazon EKS that you can use to create and operate Kubernetes clusters on-premises.	September 8, 2021
<u>Amazon FSx for NetApp ONTAP CSI driver</u>	Added topic that summarizes the Amazon FSx for NetApp ONTAP CSI driver and gives links to other references.	September 2, 2021
<u>Managed node groups now auto-calculates the Amazon EKS recommended maximum Pods for nodes</u>	Managed node groups now auto-calculate the Amazon EKS maximum Pods for nodes that you deploy without a launch template, or with a launch template that you haven't specified an AMI ID in.	August 30, 2021
<u>Remove Amazon EKS management of add-on settings without removing the Amazon EKS add-on software</u>	You can now remove an Amazon EKS add-on without removing the add-on software from your cluster.	August 20, 2021
<u>Create multi-homed Pods using Multus</u>	You can now add multiple network interfaces to a Pod using Multus.	August 2, 2021
<u>Add more IP addresses to your Linux Amazon EC2 nodes</u>	You can now add significantly more IP addresses to your Linux Amazon EC2 nodes. This means that you can run a higher density of Pods on each node.	July 27, 2021

<u>containerd runtime bootstrap</u>	The Amazon EKS optimized accelerated Amazon Linux Amazon Machine Image (AMI) now contains a bootstrap flag that you can use to enable the containerd runtime in Amazon EKS optimized and Bottlerocket AMIs. This flag is available in all supported Kubernetes versions of the AMI.	July 19, 2021
<u>Kubernetes version 1.21 (p. 626)</u>	Added Kubernetes version 1.21 support.	July 19, 2021
<u>Added managed policies topic</u>	A list of all Amazon EKS IAM managed policies and changes that were made to them since June 17, 2021.	June 17, 2021
<u>Use security groups for Pods with Fargate</u>	You can now use security groups for Pods with Fargate, in addition to using them with Amazon EC2 nodes.	June 1, 2021
<u>Added CoreDNS and kube-proxy Amazon EKS add-ons</u>	Amazon EKS can now help you manage the CoreDNS and kube-proxy Amazon EKS add-ons for your cluster.	May 19, 2021
<u>Kubernetes version 1.20 (p. 626)</u>	Added Kubernetes version 1.20 support for new clusters and version upgrades.	May 18, 2021
<u>AWS Load Balancer Controller2.2.0 released</u>	You can now use the AWS Load Balancer Controller to create Elastic Load Balancers using instance or IP targets.	May 14, 2021
<u>Node taints for managed node groups</u>	Amazon EKS now supports adding note taints to managed node groups.	May 11, 2021
<u>Secrets encryption for existing clusters</u>	Amazon EKS now supports adding <u>secrets encryption</u> to existing clusters.	February 26, 2021
<u>Kubernetes version 1.19 (p. 626)</u>	Added Kubernetes version 1.19 support for new clusters and version upgrades.	February 16, 2021
<u>Amazon EKS now supports OpenID Connect (OIDC) identity providers as a method to authenticate users to a version 1.16 or later cluster.</u>	OIDC identity providers can be used with, or as an alternative to AWS Identity and Access Management (IAM).	February 12, 2021

<u>View node and workload resources in the AWS Management Console</u>	You can now view details about your managed, self-managed, and Fargate nodes and your deployed Kubernetes workloads in the AWS Management Console.	December 1, 2020
<u>Deploy Spot Instance types in a managed node group</u>	You can now deploy multiple Spot or On-Demand Instance types to a managed node group.	December 1, 2020
<u>Amazon EKS can now manage specific add-ons for your cluster</u>	You can manage add-ons yourself, or allow Amazon EKS to control the launch and version of an add-on through the Amazon EKS API.	December 1, 2020
<u>Share an ALB across multiple Ingresses</u>	You can now share an AWS Application Load Balancer (ALB) across multiple Kubernetes Ingresses. In the past, you had to deploy a separate ALB for each Ingress.	October 23, 2020
<u>NLB IP target support</u>	You can now deploy a Network Load Balancer with IP targets. This means that you can use an NLB to load balance network traffic to Fargate Pods and directly to Pods that are running on Amazon EC2 nodes.	October 23, 2020
<u>Kubernetes version 1.18 (p. 626)</u>	Added Kubernetes version 1.18 support for new clusters and version upgrades.	October 13, 2020
<u>Specify a custom CIDR block for Kubernetes service IP address assignment.</u>	You can now specify a custom CIDR block that Kubernetes assigns service IP addresses from.	September 29, 2020
<u>Assign security groups to individual Pods</u>	You can now associate different security groups to some of the individual Pods that are running on many Amazon EC2 instance types.	September 9, 2020
<u>Deploy Bottlerocket on your nodes</u>	You can now deploy nodes that are running Bottlerocket .	August 31, 2020
<u>The ability to launch Arm nodes is generally available</u>	You can now launch Arm nodes in managed and self-managed node groups.	August 17, 2020
<u>Managed node group launch templates and custom AMI</u>	You can now deploy a managed node group that uses an Amazon EC2 launch template. The launch template can specify a custom AMI, if you choose.	August 17, 2020

<u>EFS support for AWS Fargate</u>	You can now use Amazon EFS with AWS Fargate.	August 17, 2020
<u>Amazon EKS platform version update</u>	This is a new platform version with security fixes and enhancements. This includes UDP support for services of type LoadBalancer when using Network Load Balancers with Kubernetes version 1.15 or later. For more information, see the Allow UDP for AWS Network Load Balancer issue on GitHub.	August 12, 2020
<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the Africa (Cape Town) (af-south-1) and Europe (Milan) (eu-south-1) AWS Regions.	August 6, 2020
<u>Fargate usage metrics</u>	AWS Fargate provides CloudWatch usage metrics that provide visibility into your account's usage of Fargate On-Demand resources.	August 3, 2020
<u>Kubernetes version 1.17 (p. 626)</u>	Added Kubernetes version 1.17 support for new clusters and version upgrades.	July 10, 2020
<u>Create and manage App Mesh resources from within Kubernetes with the App Mesh controller for Kubernetes</u>	You can create and manage App Mesh resources from within Kubernetes. The controller also automatically injects the Envoy proxy and init containers into Pods that you deploy.	June 18, 2020
<u>Amazon EKS now supports Amazon EC2 Inf1 nodes</u>	You can add Amazon EC2 Inf1 nodes to your cluster.	June 4, 2020
<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the AWS GovCloud (US-East) (us-gov-east-1) and AWS GovCloud (US-West) (us-gov-west-1) AWS Regions.	May 13, 2020
<u>Kubernetes 1.12 is no longer supported on Amazon EKS</u>	Kubernetes version 1.12 is no longer supported on Amazon EKS. Update any 1.12 clusters to version 1.13 or later to avoid service interruption.	May 12, 2020
<u>Kubernetes version 1.16 (p. 626)</u>	Added Kubernetes version 1.16 support for new clusters and version upgrades.	April 30, 2020
<u>Added the AWSServiceRoleForAmazonEKS service-linked role</u>	Added the AWSServiceRoleForAmazonEKS service-linked role.	April 16, 2020

<u>Kubernetes version 1.15 (p. 626)</u>	Added Kubernetes version 1.15 support for new clusters and version upgrades.	March 10, 2020
<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the Beijing (cn-north-1) and Ningxia (cn-northwest-1) AWS Regions.	February 26, 2020
<u>FSx for Lustre CSI driver</u>	Added topic for installing the FSx for Lustre CSI driver on Kubernetes 1.14 Amazon EKS clusters.	December 23, 2019
<u>Restrict network access to the public access endpoint of a cluster</u>	With this update, you can use Amazon EKS to restrict the CIDR ranges that can communicate to the public access endpoint of the Kubernetes API server.	December 20, 2019
<u>Resolve the private access endpoint address for a cluster from outside of a VPC</u>	With this update, you can use Amazon EKS to resolve the private access endpoint of the Kubernetes API server from outside of a VPC.	December 13, 2019
<u>(Beta) Amazon EC2 A1 Amazon EC2 instance nodes</u>	Launch <u>Amazon EC2 A1</u> Amazon EC2 instance nodes that register with your Amazon EKS cluster.	December 4, 2019
<u>Creating a cluster on AWS Outposts</u>	Amazon EKS now supports creating clusters on AWS Outposts.	December 3, 2019
<u>AWS Fargate on Amazon EKS</u>	Amazon EKS Kubernetes clusters now support running Pods on Fargate.	December 3, 2019
<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the Canada (Central) (ca-central-1) AWS Region.	November 21, 2019
<u>Managed node groups</u>	Amazon EKS managed node groups automate the provisioning and lifecycle management of nodes (Amazon EC2 instances) for Amazon EKS Kubernetes clusters.	November 18, 2019
<u>Amazon EKS platform version update</u>	New platform versions to address <u>CVE-2019-11253</u> .	November 6, 2019
<u>Kubernetes 1.11 is no longer supported on Amazon EKS</u>	Kubernetes version 1.11 is no longer supported on Amazon EKS. Please update any 1.11 clusters to version 1.12 or higher to avoid service interruption.	November 4, 2019

<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the South America (São Paulo) (<code>sa-east-1</code>) AWS Region.	October 16, 2019
<u>Windows support</u>	Amazon EKS clusters running Kubernetes version 1.14 now support Windows workloads.	October 7, 2019
<u>Autoscaling</u>	Added a chapter to cover some of the different types of Kubernetes autoscaling that are supported on Amazon EKS clusters.	September 30, 2019
<u>Kubernetes Dashboard update</u>	Updated topic for installing the Kubernetes Dashboard on Amazon EKS clusters to use the beta 2.0 version.	September 28, 2019
<u>Amazon EFS CSI driver</u>	Added topic for installing the Amazon EFS CSI driver on Kubernetes 1.14 Amazon EKS clusters.	September 19, 2019
<u>Amazon EC2 Systems Manager parameter for Amazon EKS optimized AMI ID</u>	Added topic for retrieving the Amazon EKS optimized AMI ID using an Amazon EC2 Systems Manager parameter. The parameter eliminates the need for you to look up AMI IDs.	September 18, 2019
<u>Amazon EKS resource tagging</u>	You can manage the tagging of your Amazon EKS clusters.	September 16, 2019
<u>Amazon EBS CSI driver</u>	Added topic for installing the Amazon EBS CSI driver on Kubernetes 1.14 Amazon EKS clusters.	September 9, 2019
<u>New Amazon EKS optimized AMI patched for CVE-2019-9512 and CVE-2019-9514</u>	Amazon EKS has updated the Amazon EKS optimized AMI to address CVE-2019-9512 and CVE-2019-9514 .	September 6, 2019
<u>Announcing deprecation of Kubernetes 1.11 in Amazon EKS</u>	Amazon EKS discontinued support for Kubernetes version 1.11 on November 4, 2019.	September 4, 2019
<u>Kubernetes version 1.14 (p. 626)</u>	Added Kubernetes version 1.14 support for new clusters and version upgrades.	September 3, 2019

<u>IAM roles for service accounts</u>	With IAM roles for service accounts on Amazon EKS clusters, you can associate an IAM role with a Kubernetes service account. With this feature, you no longer need to provide extended permissions to the node IAM role. This way, Pods on that node can call AWS APIs.	September 3, 2019
<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the Middle East (Bahrain) (me-south-1) AWS Region.	August 29, 2019
<u>Amazon EKS platform version update</u>	New platform versions to address CVE-2019-9512 and CVE-2019-9514 .	August 28, 2019
<u>Amazon EKS platform version update</u>	New platform versions to address CVE-2019-11247 and CVE-2019-11249 .	August 5, 2019
<u>Amazon EKS Region expansion (p. 626)</u>	Amazon EKS is now available in the Asia Pacific (Hong Kong) (ap-east-1) AWS Region.	July 31, 2019
<u>Kubernetes 1.10 no longer supported on Amazon EKS</u>	Kubernetes version 1.10 is no longer supported on Amazon EKS. Update any 1.10 clusters to version 1.11 or higher to avoid service interruption.	July 30, 2019
<u>Added topic on ALB ingress controller</u>	The AWS ALB Ingress Controller for Kubernetes is a controller that causes an ALB to be created when ingress resources are created.	July 11, 2019
<u>New Amazon EKS optimized AMI</u>	Removing unnecessary <code>kubectl</code> binary from AMIs.	July 3, 2019
<u>Kubernetes version 1.13 (p. 626)</u>	Added Kubernetes version 1.13 support for new clusters and version upgrades.	June 18, 2019
<u>New Amazon EKS optimized AMI patched for AWS-2019-005</u>	Amazon EKS has updated the Amazon EKS optimized AMI to address the vulnerabilities that are described in AWS-2019-005 .	June 17, 2019
<u>Announcing discontinuation of support of Kubernetes 1.10 in Amazon EKS</u>	Amazon EKS stopped supporting Kubernetes version 1.10 on July 22, 2019.	May 21, 2019

<u>Amazon EKS platform version update</u>	New platform version for Kubernetes 1.11 and 1.10 clusters to support custom DNS names in the kubelet certificate and improve etcd performance.	May 21, 2019
<u>AWS CLIget-token command (p. 626)</u>	The <code>aws eks get-token</code> command was added to the AWS CLI. You no longer need to install the AWS IAM Authenticator for Kubernetes to create client security tokens for cluster API server communication. Upgrade your AWS CLI installation to the latest version to use this new functionality. For more information, see Installing the AWS Command Line Interface in the AWS Command Line Interface User Guide .	May 10, 2019
<u>Getting started with eksctl</u>	This getting started guide describes how you can install all of the required resources to get started with Amazon EKS using eksctl. This is a simple command line utility for creating and managing Kubernetes clusters on Amazon EKS.	May 10, 2019
<u>Amazon EKS platform version update</u>	New platform version for Kubernetes 1.12 clusters to support custom DNS names in the kubelet certificate and improve etcd performance. This fixes a bug that caused node kubelet daemons to request a new certificate every few seconds.	May 8, 2019
<u>Prometheus tutorial</u>	Added topic for deploying Prometheus to your Amazon EKS cluster.	April 5, 2019
<u>Amazon EKS control plane logging</u>	With this update, you can get audit and diagnostic logs directly from the Amazon EKS control pane. You can use these CloudWatch logs in your account as reference for securing and running clusters.	April 4, 2019
<u>Kubernetes version 1.12 (p. 626)</u>	Added Kubernetes version 1.12 support for new clusters and version upgrades.	March 28, 2019

<u>Added App Mesh getting started guide</u>	Added documentation for getting started with App Mesh and Kubernetes.	March 27, 2019
<u>Amazon EKS API server endpoint private access</u>	Added documentation for disabling public access for your Amazon EKS cluster's Kubernetes API server endpoint.	March 19, 2019
<u>Added topic for installing the Kubernetes Metrics Server</u>	The Kubernetes Metrics Server is an aggregator of resource usage data in your cluster.	March 18, 2019
<u>Added list of related open source projects</u>	These open source projects extend the functionality of Kubernetes clusters running on AWS, including clusters that are managed by Amazon EKS.	March 15, 2019
<u>Added topic for installing Helm locally</u>	The helm package manager for Kubernetes helps you install and manage applications on your Kubernetes cluster. This topic shows how to install and run the helm and tiller binaries locally. That way, you can install and manage charts using the Helm CLI on your local system.	March 11, 2019
<u>Amazon EKS platform version update</u>	New platform version that updates Amazon EKS Kubernetes 1.11 clusters to patch level 1.11.8 to address <u>CVE-2019-1002100</u> .	March 8, 2019
<u>Increased cluster limit</u>	Amazon EKS has increased the number of clusters that you can create in an AWS Region from 3 to 50.	February 13, 2019
<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the Europe (London) (eu-west-2), Europe (Paris) (eu-west-3), and Asia Pacific (Mumbai) (ap-south-1) AWS Regions.	February 13, 2019
<u>New Amazon EKS optimized AMI patched for ALAS-2019-1156</u>	Amazon EKS has updated the Amazon EKS optimized AMI to address the vulnerability that's described in <u>ALAS-2019-1156</u> .	February 11, 2019
<u>New Amazon EKS optimized AMI patched for ALAS2-2019-1141</u>	Amazon EKS has updated the Amazon EKS optimized AMI to address the CVEs that are referenced in <u>ALAS2-2019-1141</u> .	January 9, 2019

Amazon EKS AWS Region expansion (p. 626)	Amazon EKS is now available in the Asia Pacific (Seoul) (ap-northeast-2) AWS Region.	January 9, 2019
Amazon EKS region expansion (p. 626)	Amazon EKS is now available in the following additional AWS Regions: Europe (Frankfurt) (eu-central-1), Asia Pacific (Tokyo) (ap-northeast-1), Asia Pacific (Singapore) (ap-southeast-1), and Asia Pacific (Sydney) (ap-southeast-2).	December 19, 2018
Amazon EKS cluster updates	Added documentation for Amazon EKS cluster Kubernetes version updates and node replacement .	December 12, 2018
Amazon EKS AWS Region expansion (p. 626)	Amazon EKS is now available in the Europe (Stockholm) (eu-north-1) AWS Region.	December 11, 2018
Amazon EKS platform version update	New platform version updating Kubernetes to patch level 1.10.11 to address CVE-2018-1002105 .	December 4, 2018
Added version 1.0.0 support for the ALB ingress controller	The ALB ingress controller releases version 1.0.0 with formal support from AWS.	November 20, 2018
Added support for CNI network configuration	The Amazon VPC CNI plugin for Kubernetes version 1.2.1 now supports custom network configuration for secondary Pod network interfaces.	October 16, 2018
Added support for MutatingAdmissionWebhook and ValidatingAdmissionWebhook	Amazon EKS platform version 1.10-eks.2 now supports MutatingAdmissionWebhook and ValidatingAdmissionWebhook admission controllers.	October 10, 2018
Added partner AMI information	Canonical has partnered with Amazon EKS to create node AMIs that you can use in your clusters.	October 3, 2018
Added instructions for AWS CLIupdate-kubeconfig command	Amazon EKS has added the update-kubeconfig to the AWS CLI to simplify the process of creating a kubeconfig file for accessing your cluster.	September 21, 2018
New Amazon EKS optimized AMIs	Amazon EKS has updated the Amazon EKS optimized AMIs (with and without GPU support) to provide various security fixes and AMI optimizations.	September 13, 2018

<u>Amazon EKS AWS Region expansion (p. 626)</u>	Amazon EKS is now available in the Europe (Ireland) (eu-west-1) Region.	September 5, 2018
<u>Amazon EKS platform version update</u>	New platform version with support for Kubernetes <u>aggregation layer</u> and the <u>Horizontal Pod Autoscaler</u>(HPA).	August 31, 2018
<u>New Amazon EKS optimized AMIs and GPU support</u>	Amazon EKS has updated the Amazon EKS optimized AMI to use a new AWS CloudFormation node template and <u>bootstrap script</u> . In addition, a new <u>Amazon EKS optimized AMI with GPU support</u> is available.	August 22, 2018
<u>New Amazon EKS optimized AMI patched for ALAS2-2018-1058</u>	Amazon EKS has updated the Amazon EKS optimized AMI to address the CVEs that are referenced in <u>ALAS2-2018-1058</u> .	August 14, 2018
<u>Amazon EKS optimized AMI build scripts</u>	Amazon EKS has open-sourced the build scripts that are used to build the Amazon EKS optimized AMI. These build scripts are now available on GitHub.	July 10, 2018
<u>Amazon EKS initial release (p. 626)</u>	Initial documentation for service launch	June 5, 2018