Amazon EKS on the AWS Cloud

Quick Start Reference Deployment

This Quick Start was created by Amazon Web Services (AWS). [Quick Starts](http://aws.amazon.com/quickstart/) are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying Amazon Elastic Kubernetes Service (Amazon EKS) clusters.

This Quick Start is for users who want a repeatable, customizable reference deployment for Amazon EKS using AWS CloudFormation.

Amazon EKS on AWS

Using Amazon EKS, you can deploy, manage, and scale containerized applications that run Kubernetes on AWS.

To eliminate a single point of failure, Amazon EKS runs the Kubernetes management infrastructure across multiple Availability Zones. Amazon EKS is certified Kubernetes-conformant, so you can use existing tools and plugins from partners and the Kubernetes community. Applications that run in a standard Kubernetes environment are fully compatible with this deployment and can be migrated to Amazon EKS.

This Quick Start provides AWS CloudFormation templates that deploy the Kubernetes control plane, connect worker nodes to the cluster, and configure a bastion host for cluster administrative operations. Additionally, this deployment provides several [AWS CloudFormation registry resource types](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/registry.html) that let you deploy and manage Kubernetes applications by declaring Kubernetes manifests or Helm charts. This Quick Start also includes optional add-ins from AWS Partners and open-source projects. For more information, see the [Optional add-ins](https://aws-quickstart.github.io/quickstart-amazon-eks/#_optional_add_ins) section.

AWS costs

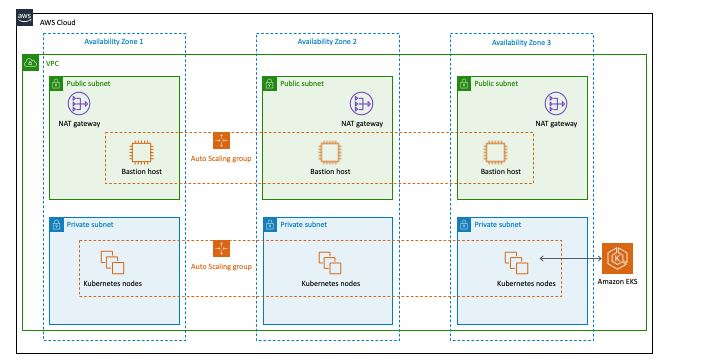
You are responsible for the cost of the AWS services and any third-party licenses used while running this Quick Start. There is no additional cost for using the Quick Start.

The AWS CloudFormation templates for Quick Starts include configuration parameters that you can customize. Some of the settings, such as the instance type, affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you use. Prices are subject to change.

|  |  |
| --- | --- |
|  | After you deploy the Quick Start, [create AWS Cost and Usage Reports](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-gettingstarted-turnonreports.html) to deliver billing metrics to an Amazon Simple Storage Service (Amazon S3) bucket in your account. These reports provide cost estimates based on usage throughout each month and aggregate the data at the end of the month. For more information, see [What are AWS Cost and Usage Reports?](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-costusage.html) |

Architecture

Deploying this Quick Start for a new virtual private cloud (VPC) with default parameters builds the following Amazon EKS environment in the AWS Cloud.

[](https://aws-quickstart.github.io/quickstart-amazon-eks/images/architecture_diagram.png)

*Figure 1. Quick Start architecture for Amazon EKS on AWS*

The Quick Start sets up the following:

* A highly available architecture that spans three Availability Zones.\*
* A VPC configured with public and private subnets, according to AWS best practices, to provide you with your own virtual network on AWS.\*
* In the public subnets, managed NAT gateways to allow outbound internet access for resources in the private subnets.\*
* In one public subnet, a Linux bastion host in an Auto Scaling group to allow inbound Secure Shell (SSH) access to Amazon Elastic Compute Cloud (Amazon EC2) instances in private subnets. The bastion host is also configured with the Kubernetes kubectl command line interface (CLI) for managing the Kubernetes cluster.
* An Amazon EKS cluster, which creates the Kubernetes control plane.
* In the private subnets, a group of Kubernetes nodes.

\* The template that deploys the Quick Start into an existing VPC skips the components marked by asterisks and prompts you for your existing VPC configuration.

Planning the deployment

Specialized knowledge

This deployment requires a moderate level of familiarity with AWS services. If you’re new to AWS, see [Getting Started Resource Center](https://aws.amazon.com/getting-started/) and [AWS Training and Certification](https://aws.amazon.com/training/). These sites provide materials for learning how to design, deploy, and operate your infrastructure and applications on the AWS Cloud.

This Quick Start assumes familiarity with Kubernetes concepts and usage. The sections about authoring templates assume a working knowledge of AWS CloudFormation.

AWS account

If you don’t already have an AWS account, create one at [https://aws.amazon.com](https://aws.amazon.com/) by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.

Your AWS account is automatically signed up for all AWS services. You are charged only for the services you use.

Resource quotas

If necessary, request [service quota increases](https://console.aws.amazon.com/servicequotas/home?region=us-east-2#!/) for the following resources. You might request quota increases to avoid exceeding the default limits for any resources that are shared across multiple deployments. The [Service Quotas console](https://console.aws.amazon.com/servicequotas/home?region=us-east-2#!/) displays your usage and quotas for some aspects of some services. For more information, see [What is Service Quotas?](https://docs.aws.amazon.com/servicequotas/latest/userguide/intro.html) and [AWS service quotas](https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html).

| **Resource** | **Default quota** | **This deployment uses (default configuration)** |
| --- | --- | --- |
| VPCs | 5 per AWS Region | 1 |
| VPC security groups | 300 per account | 3 |
| IAM roles | 1,000 per account | 9 |
| Auto Scaling groups | 200 per Region | 2 |
| t2.medium instances | 20 per Region | 3 |
| t2.micro instances | 20 per Region | 1 |

IAM permissions

Before launching the Quick Start, you must sign in to the AWS Management Console with IAM permissions for the resources that the templates deploy. The *AdministratorAccess* managed policy within IAM provides sufficient permissions, although your organization may choose to use a custom policy with more restrictions. For more information, see [AWS managed policies for job functions](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html).

Deployment options

This Quick Start provides three deployment options:

* **Deploy Amazon EKS into a new VPC (end-to-end deployment)**. This option builds a new AWS environment consisting of the VPC, subnets, NAT gateways, security groups, bastion hosts, and other infrastructure components, and then deploys Amazon EKS into this new VPC.
* **Deploy Amazon EKS into an existing VPC**. This option provisions Amazon EKS in your existing AWS infrastructure.
* **Enable an existing EKS cluster for AWS CloudFormation–based deployments**. This option deploys the necessary infrastructure for AWS CloudFormation to manage Kubernetes resources for an existing cluster.

|  |  |
| --- | --- |
|  | Many advanced or optional configuration items must be configured by launching the [advanced configuration stack](https://fwd.aws/zwGDB) before launching one of the deployment options. |

The Quick Start provides separate templates for these options. It also lets you configure CIDR blocks, instance types, and Amazon EKS settings, as discussed later in this guide.

Deployment steps

Sign in to your AWS account

1. Sign in to your AWS account at [https://aws.amazon.com](https://aws.amazon.com/) with an IAM user role that has the necessary permissions. For more information, see [Planning the deployment](https://aws-quickstart.github.io/quickstart-amazon-eks/#planning-the-deployment), earlier in this guide.
2. Ensure that your AWS account is configured correctly, as discussed in the [Technical requirements](https://aws-quickstart.github.io/quickstart-amazon-eks/#technical-requirements) section.
3. Use the Region selector in the navigation bar to choose the AWS Region where you want to deploy Amazon EKS.
4. Select the key pair that you created earlier. In the navigation pane of the [Amazon EC2 console](https://console.aws.amazon.com/ec2/), choose **Key Pairs**, and then choose your key pair from the list.

Launch the Quick Start

1. Optionally, if you want to configure advanced parameters, launch the [advanced configuration template](https://fwd.aws/6dEQ7).
2. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help with choosing an option, see [Deployment options](https://aws-quickstart.github.io/quickstart-amazon-eks/#_deployment_options), earlier in this guide.

|  |
| --- |
| [Deploy Amazon EKS into a new VPC](https://fwd.aws/6dEQ7) |
| [Deploy Amazon EKS into an existing VPC](https://fwd.aws/e37MA) |
| [Enable EKS based Quick Starts on an existing EKS cluster](https://fwd.aws/VBeX6) |

Deployment can take between 25 and 90 minutes to complete, depending on the chosen deployment option and parameter values.

|  |  |
| --- | --- |
|  | If you deploy Amazon EKS into an existing VPC, ensure that your VPC has private subnets in different Availability Zones for the workload instances. The subnets require egress internet access using a NAT gateway or an HTTP proxy. If you want to use the Kubernetes integration with Elastic Load Balancing, you must tag each private subnet with kubernetes.io/role/internal-elb=true and each public subnet with kubernetes.io/role/elb=true. |

1. Check the Region that’s displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for Amazon EKS is built. The template launches in the US East (Ohio) Region by default.

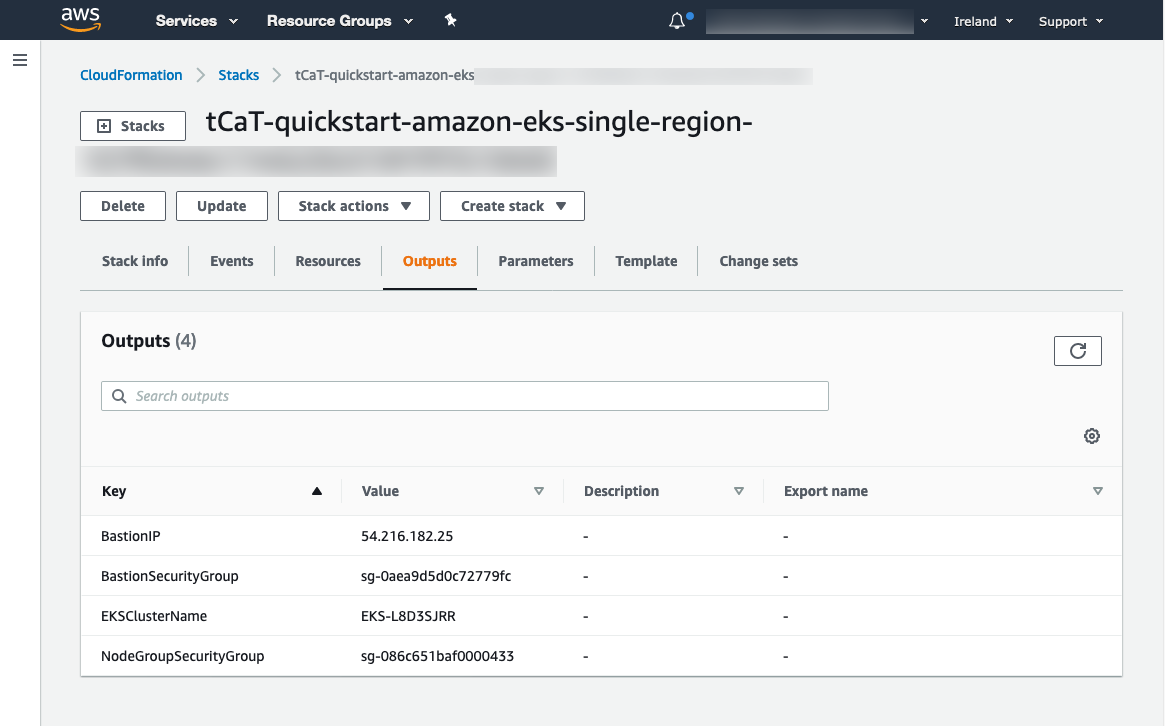
|  |  |
| --- | --- |
|  | Some services are not supported in all AWS Regions. For a current list of supported Regions, see [Amazon Elastic Kubernetes Service endpoints and quotas](https://docs.aws.amazon.com/general/latest/gr/eks.html). |

1. On the **Select template** page, keep the default setting for the template URL, and then choose **Next**.
2. On the **Specify stack details** page, change the stack name if needed. Review the parameters for the template, and provide values for any parameters that require input. For all other parameters, review the default settings, and customize them as necessary.

|  |  |
| --- | --- |
|  | If Amazon EKS is already deployed in your account, ensure that the Per account shared resources parameter is set to **No**. If you deploy a new Amazon EKS instance in the same Region as a previously deployed instance, set Per region shared resources to **No**. |
|  | If you created and intend to use an advanced configuration stack, ensure that you set the value for Config set name to match the value you used when you launched the advanced configuration stack. |

|  |  |
| --- | --- |
|  | Unless you are customizing this Quick Start’s templates for your own deployment projects, we recommend that you keep the default settings for the parameters labeled Quick Start S3 bucket name, Quick Start S3 bucket Region, and Quick Start S3 key prefix. Changing these parameter settings automatically updates code references to point to a new Quick Start location. For more information, see the [AWS Quick Start Contributor’s Guide](https://aws-quickstart.github.io/option1.html). |

1. On the **Configure stack options** page, you can [specify tags](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-resource-tags.html) (key-value pairs) for resources in your stack and [set advanced options](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-add-tags.html). When you’re done, choose **Next**.
2. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the two check boxes to acknowledge that the template creates IAM resources and might require the ability to automatically expand macros.
3. Choose **Create stack** to deploy the stack.
4. Monitor the status of the stack. When the status is **CREATE\_COMPLETE**, the Amazon EKS deployment is ready.
5. Use the values displayed in the **Outputs** tab for the stack, as shown in [Amazon EKS outputs after successful deployment](https://aws-quickstart.github.io/quickstart-amazon-eks/#cfn_outputs), to view the created resources.

[](https://aws-quickstart.github.io/quickstart-amazon-eks/images/cfn_outputs.png)

*Figure 2. Amazon EKS outputs after successful deployment*

Test the deployment

|  |  |
| --- | --- |
|  | These steps must be executed from a network that has access to the Kubernetes API, as configured by the **EKS public access endpoint** and **Kubernetes API public access CIDR** parameters. For more information, see [Installing kubectl](https://docs.aws.amazon.com/eks/latest/userguide/install-kubectl.html). If you enabled the optional bastion host, you can connect to it by using SSH. Use the key pair that you specified during deployment and the IP address from the **Outputs** tab of the AWS CloudFormation stack. The bastion host already has kubectl installed and configured so that it connects to the cluster. To test the CLI, connect to the cluster, and run the following command. |

$ kubectl version

Confirm that the output includes the server version, which indicates a successful connection to the Kubernetes control plane.

Client Version: version.Info\{Major:"1", Minor:"11", GitVersion:"<version number>", GitCommit:"<commit ID>", GitTreeState:"clean", BuildDate:"2018-12-06T01:33:57Z", GoVersion:"go1.10.3", Compiler:"gc", Platform:"linux/amd64"}

Server Version: version.Info\{Major:"1", Minor:"11+", GitVersion:" <version number>", GitCommit:" <commit ID>", GitTreeState:"clean", BuildDate:"2018-12-06T23:13:14Z", GoVersion:"go1.10.3", Compiler:"gc", Platform:"linux/amd64"}

1. Check for a successful connection between the nodes and cluster by running the get nodes command.

$ kubectl get nodes

NAME STATUS ROLES AGE VERSION

ip-10-0-25-239.us-west-2.compute.internal Ready <none> 10m <version number>

ip-10-0-27-244.us-west-2.compute.internal Ready <none> 10m <version number>

ip-10-0-35-29.us-west-2.compute.internal Ready <none> 10m <version number>

Best practices for using Amazon EKS

Use AWS CloudFormation for ongoing management

We recommend using AWS CloudFormation for managing updates and resources that are created by this Quick Start. Using the Amazon EC2 console, CLI, or API to change or delete resources can cause future AWS CloudFormation operations on the stack to behave unexpectedly.

Monitor additional resource usage

This deployment enables users of the Amazon EKS cluster to create elastic load balancers and Amazon EBS volumes as part of their Kubernetes applications. Because these carry additional costs, we recommend that you grant users of the Amazon EKS cluster the minumum permissions required according to [Kubernetes Role Based Access Control (RBAC)](https://kubernetes.io/docs/reference/access-authn-authz/rbac/) and that you monitor resource usage by using the Kubernetes CLI or API to describe persistent volume claims (PVC) and LoadBalancer resources across all namespaces. To disable this functionality, update the ControlPlaneRole IAM role in the child stack to restrict access to the Kubernetes control plane for specific AWS APIs, such as ec2:CreateVolume and elb:CreateLoadBalancer.

Security

Amazon EKS uses AWS IAM to authenticate your Kubernetes cluster, but it still relies on native Kubernetes RBAC. This means that IAM is used only for valid entities. All permissions for interacting with your Amazon EKS cluster’s Kubernetes API are managed by the native Kubernetes RBAC system. We recommend that you grant least-privilege access via Kubernetes RBAC.

Adding Kubernetes users

This Quick Start creates an IAM role that is used to create the Kubernetes control plane. The AWS CloudFormation custom resources and Linux bastion host use the IAM role to provide access to the Kubernetes API. Additional IAM users or roles can be added as Kubernetes administrators (**system:master** kubernetes cluster role) by entering an ARN into the **Additional EKS admin ARN** parameter when you launch this Quick Start. To add users after the stack launches, see [Managing users or IAM roles for your cluster](https://docs.aws.amazon.com/eks/latest/userguide/add-user-role.html).

Managing Kubernetes resources using AWS CloudFormation

This Quick Start includes AWS CloudFormation registry types that enable authoring, creating, and managing Kubernetes-based applications. For an example, see [example-workload template](https://github.com/aws-quickstart/quickstart-aws-eks/blob/master/templates/example-workload.template.yaml).

Optional add-ins

This Quick Start contains optional configurations and add-ins for Kubernetes that enhance the functionality and reduce post-deployment configuration tasks for customers.

Cluster autoscaler

[Cluster autoscaler](https://github.com/kubernetes/autoscaler/tree/master/cluster-autoscaler) automatically adjusts the size of the Kubernetes cluster when there are insufficient resources or nodes.

Managed node group

With Amazon EKS–managed node groups, provisioning and lifecycle management of the nodes is automated. All nodes get provisioned as part of an Auto Scaling group, which means you cannot use the **Cluster autoscaler** option. Nodes are created using the latest Amazon EKS–optimized Amazon Linux 2 AMI.

EFS StorageClass

An optional EFSStorageClass volume provides redundant, persistent storage that is untethered to individual Availability Zones, so it is well suited for high availability, stateful applications that are required to survive an outage. The Amazon EFS volume is available to Kubernetes pods through the [EFS provisioner project](https://github.com/helm/charts/tree/master/stable/efs-provisioner).

There are several configuration options available to tune the performance and throughput of the underlying EFS volume. For more information, see [Amazon EFS Performance](https://docs.aws.amazon.com/efs/latest/ug/performance.html).

FAQ

**Q.** I encountered a **CREATE\_FAILED** error when I launched the Quick Start.

**A.** If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **Disabled**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack’s state is retained, and instances remain running so you can troubleshoot the issue.

|  |  |
| --- | --- |
|  | When you set **Rollback on failure** to **Disabled**, you continue to incur AWS charges for the stack. Ensure that you delete the stack when you finish troubleshooting. |

For more information, see [Troubleshooting AWS CloudFormation](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/troubleshooting.html).

**Q.** A resource type starting with **AWSQS::** failed on stack create, update, or deletion.

**A.** These resources are AWS CloudFormation registry resource types created by the Quick Start. Logs for it are stored in Amazon CloudWatch Logs with a group prefix of **/cloudformation/registry/awsqs-**.

**Q.** I encountered a size limitation error when I deployed the AWS CloudFormation templates.

**A.** We recommend that you launch the Quick Start templates from the links in this guide or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-Amazon S3 location, you might encounter template size limitations when you create the stack. For more information, see [AWS CloudFormation quotas](http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cloudformation-limits.html).

Parameter reference

|  |  |
| --- | --- |
|  | Unless you are customizing the Quick Start templates for your own deployment projects, we recommend that you keep the default settings for the parameters labeled Quick Start S3 bucket name, Quick Start S3 bucket Region, and Quick Start S3 key prefix. Changing these parameter settings automatically updates code references to point to a new Quick Start location. For more information, see the [AWS Quick Start Contributor’s Guide](https://aws-quickstart.github.io/option1.html). |

Launch into a new VPC

| *Table 1. Basic configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Availability Zones (AvailabilityZones) | ***Requires input*** | List of Availability Zones to use for the subnets in the VPC. Three Availability Zones are used for this deployment. |
| Allowed external access CIDR (RemoteAccessCIDR) | ***Requires input*** | CIDR IP range that is permitted to access the instances. We recommend that you set this value to a trusted IP range. |
| SSH key name (KeyPairName) | ***Requires input*** | Name of an existing key pair, which allows you to securely connect to your instance after it launches. |
| Config set name (ConfigSetName) | ***Blank string*** | (Optional) Name used to map advanced parameters to an EKS cluster. If you launched an advanced configuration stack and want to apply its values to this cluster, this name must match the ConfigSetName parameter for the stack. If left blank, a new config set is created using default values. |
| Per-account shared resources (PerAccountSharedResources) | AutoDetect | Choose "No" if you already deployed another EKS Quick Start stack in your AWS account. |
| Per-Region shared resources (PerRegionSharedResources) | AutoDetect | Choose "No" if you already deployed another EKS Quick Start stack in your Region. |

| *Table 2. VPC network configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Number of Availability Zones (NumberOfAZs) | 3 | Number of Availability Zones to use in the VPC. This must match the value entered for the AvailabilityZones parameter. |
| VPC CIDR (VPCCIDR) | 10.0.0.0/16 | CIDR block for the VPC. |
| Private subnet 1 CIDR (PrivateSubnet1CIDR) | 10.0.0.0/19 | CIDR block for private subnet 1, located in Availability Zone 1. |
| Private subnet 2 CIDR (PrivateSubnet2CIDR) | 10.0.32.0/19 | CIDR block for private subnet 2, located in Availability Zone 2. |
| Private subnet 3 CIDR (PrivateSubnet3CIDR) | 10.0.64.0/19 | CIDR block for private subnet 3, located in Availability Zone 3. |
| Public subnet 1 CIDR (PublicSubnet1CIDR) | 10.0.128.0/20 | CIDR block for the public (DMZ) subnet 1, located in Availability Zone 1. |
| Public subnet 2 CIDR (PublicSubnet2CIDR) | 10.0.144.0/20 | CIDR block for the public (DMZ) subnet 2, located in Availability Zone 2. |
| Public subnet 3 CIDR (PublicSubnet3CIDR) | 10.0.160.0/20 | CIDR block for the public (DMZ) subnet 3, located in Availability Zone 3. |

| *Table 3. Amazon EC2 configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Provision bastion host (ProvisionBastionHost) | Enabled | Skip creating a bastion host by choosing "Disabled." |

| *Table 4. Amazon EKS configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| EKS cluster name (EKSClusterName) | ***Blank string*** | (Optional) Name for the EKS cluster. If left blank, one is auto-generated. This must be unique within the Region. |
| EKS public access endpoint (EKSPublicAccessEndpoint) | Disabled | Configure access to the Kubernetes API server endpoint from outside of your VPC. |
| Additional EKS admin ARN (IAM user) (AdditionalEKSAdminUserArn) | ***Blank string*** | (Optional) IAM user ARN to be granted administrative access to the EKS cluster. |
| Additional EKS admin ARN (IAM role) (AdditionalEKSAdminRoleArn) | ***Blank string*** | (Optional) IAM role ARN to be granted administrative access to the EKS cluster. |
| Fargate namespaces (FargateNamespaces) | ***Blank string*** | (Optional) Comma-separated list of namespaces for which Fargate should be enabled. |
| Fargate labels (FargateLabels) | ***Blank string*** | Requires at least one Fargate namespace to be specified. This is a comma-separated list of key-value pod labels. For a pod to run on Fargate, all of the labels must match, and it must run in a namespace defined by "Fargate namespaces." |

| *Table 5. Default EKS node group configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Instance type (NodeInstanceType) | t3.medium | EC2 instance type. |
| Number of nodes (NumberOfNodes) | 3 | Number of Amazon EKS node instances. The default is one for each of the three Availability Zones. |
| Maximum number of nodes (MaxNumberOfNodes) | 3 | Maximum number of Amazon EKS node instances. The default is three. |
| Node group OS (NodeGroupOS) | Amazon Linux 2 | Operating system to use for node instances. Choose "Bottlerocket" for the Amazon purpose-built container OS (unmanaged node groups only). Note that if you choose "Windows," an additional Amazon Linux node group is created. |
| Node group type (NodeGroupType) | Managed | Choose "Unmanaged" to create an Auto Scaling group without using the EKS-managed node groups feature. |
| Node instance family (NodeInstanceFamily) | Standard | Choose the instance family to match the value of "Node instance type." |

| *Table 6. Snyk monitor (AWS Partner security)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Security monitoring integration (SnykIntegration) | Disabled | For more information, see <https://github.com/aws-quickstart/quickstart-eks-snyk/>. |
| Integration ID (SnykIntegrationId) | ***Blank string*** | If the SnykIntegration parameter is set to "Enabled," a value must be provided. For more information, see <https://support.snyk.io/hc/en-us/articles/360003916158-Install-the-Snyk-controller-with-Helm>. |

| *Table 7. New Relic infrastructure (AWS Partner monitoring)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Infrastructure monitoring integration (NewRelicIntegration) | Disabled | For more information, see [https://github.com/aws-quickstart/quickstart-eks-newrelic-infrastructure/."](https://github.com/aws-quickstart/quickstart-eks-newrelic-infrastructure/) |
| License key (NewRelicLicenseKey) | ***Blank string*** | If the NewRelicIntegration parameter is set to "Enabled," a value must be provided. For more information see <https://docs.newrelic.com/docs/accounts/install-new-relic/account-setup/license-key/>. |

| *Table 8. Calico policy [APN security partner]* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Calico policy integration (CalicoIntegration) | Disabled | For more information see <https://www.projectcalico.org/> . |

| *Table 9. Rafay Systems [APN software & internet partner]* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Rafay Systems integration (RafaySysIntegration) | Disabled | For more information see <https://aws-quickstart.github.io/quickstart-eks-rafay-systems/> . |
| Rafay project (RafaySysProject) | defaultproject | This is the name you want to use for you Rafay deployment. |
| Bootstrap S3 bucket (RafaySysBootstrapBucket) | ***Blank string*** | (Optional) S3 bucket to place the the Rafay bootstrap yaml file. If left blank the EKS Quick Start bucket will be used. |
| Bootstrap S3 key (RafaySysBootstrapKey) | ***Blank string*** | (Optional) S3 key to place the the Rafay bootstrap yaml file. If left blank the key will be rafay/<CLUSTER\_NAME>/cluster-bootstrap.yaml. |
| API key (RafaySysApiKey) | ***Blank string*** | Required if using an existing Rafay account. |
| API secret (RafaySysApiSecret) | ***Blank string*** | Required if using an existing Rafay account. |
| First name (RafaySysFirstName) | ***Blank string*** | Required if registering a new Rafay account. |
| Last name (RafaySysLastName) | ***Blank string*** | Required if registering a new Rafay account. |
| Organization name (RafaySysOrganizationName) | ***Blank string*** | Required if registering a new Rafay account. |
| Email (RafaySysEmail) | ***Blank string*** | Required if registering a new Rafay account. |

| *Table 10. HashiCorp Vault (AWS Partner security)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| HashiCorp Vault integration (VaultIntegration) | Disabled | For more information, see <https://github.com/aws-quickstart/quickstart-eks-hashicorp-vault/>. |
| Vault UI ACM SSL certificate ARN (VaultUIACMSSLCertificateArn) | ***Blank string*** | ARN of the load balancer’s ACM SSL certificate. If you don’t provide values for "Domain name" and "Hosted zone id", provide a value for "ACM SSL certificate ARN". |
| Route 53 hosted zone id (VaultUIHostedZoneID) | ***Blank string*** | Route 53-hosted zone ID of the domain name. If you don’t provide an ACMSSLCertificateArn value, the Quick Start creates an ACM certificate for you using HostedZoneID in conjunction with DomainName. |
| Vault UI load balancer DNS name (VaultUIDomainName) | ***Blank string*** | Fully qualified DNS name for the vault-ui service load balancer. If you don’t provide a value for "ACM SSL certificate ARN", use the HostedZoneID. |

| *Table 11. HashiCorp Consul (AWS Partner containers)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| HashiCorp Consul integration (ConsulIntegration) | Disabled | For more information, see <https://github.com/aws-quickstart/quickstart-eks-hashicorp-consul/>. |
| ACM SSL certificate ARN (ConsulUIACMSSLCertificateArn) | ***Blank string*** | ARN of the load balancer’s ACM SSL certificate. If you don’t provide values for "Domain name" and "Hosted zone id", provide a value for "ACM SSL certificate ARN". |
| Route 53 hosted zone id (ConsulUIHostedZoneID) | ***Blank string*** | Route 53-hosted zone ID of the domain name. If you don’t provide an ACMSSLCertificateArn value, the Quick Start creates an ACM certificate for you using HostedZoneID in conjunction with DomainName. |
| Consul UI load balancer DNS name (ConsulUIDomainName) | ***Blank string*** | Fully qualified DNS name for the consul-ui service load balancer. If you don’t provide a value for "ACM SSL certificate ARN", use the HostedZoneID. |

| *Table 12. Rancher management (AWS Partner management)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Rancher management integration (RancherIntegration) | Disabled | For more information, see <https://github.com/aws-quickstart/quickstart-eks-rancher/>. |
| Rancher domain name (RancherDomainName) | aws.private | DNS domain name that users can use to access the Rancher console. |

| *Table 13. Kubernetes add-ins* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| AWS load balancer controller (ALBIngressController) | Enabled | Choose "Disabled" to skip deploying the AWS load balancer controller. |
| Cluster autoscaler (ClusterAutoScaler) | Disabled | Choose "Enabled" to enable Kubernetes cluster autoscaler. |
| EFS storage class (EfsStorageClass) | Disabled | Choose "Enabled" to enable EFS storage class. |
| Prometheus integration (PrometheusIntegration) | Disabled | For more information see <https://prometheus.io/> . |
| Grafana integration (GrafanaIntegration) | Disabled | Grafana requires "Prometheus integration" to be enabled. For more information see <https://www.grafana.com/> . |
| Monitoring stack (MonitoringStack) | None | Enable monitoring stack with "Prometheus+Grafana." Warning: this is a legacy parameter and will be dropped from the next version of this Quick Start. Please use the "Grafana integration" and "Prometheus integration" parameters instead. |

| *Table 14. AWS Quick Start configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Quick Start S3 bucket name (QSS3BucketName) | aws-quickstart | S3 bucket name for the Quick Start assets. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-). |
| Quick Start S3 key prefix (QSS3KeyPrefix) | quickstart-amazon-eks/ | S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), periods (.) and forward slash (/). |
| Quick Start S3 bucket Region (QSS3BucketRegion) | us-east-1 | Region where the Quick Start S3 bucket (QSS3BucketName) is hosted. When using your own bucket, you must specify this value. |
| Test suite (TestSuite) | Disabled | Deploys a test stack that tests Quick Start components. |

Launch into an existing VPC

| *Table 15. Basic configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| VPC ID (VPCID) | ***Requires input*** | ID of your existing VPC (e.g., vpc-0343606e). |
| Private subnet 1 ID (PrivateSubnet1ID) | ***Requires input*** | ID of the private subnet in Availability Zone 1 of your existing VPC (e.g., subnet-fe9a8b32). |
| Private subnet 2 ID (PrivateSubnet2ID) | ***Blank string*** | ID of the private subnet in Availability Zone 2 of your existing VPC (e.g., subnet-be8b01ea). |
| Private subnet 3 ID (PrivateSubnet3ID) | ***Blank string*** | ID of the private subnet in Availability Zone 3 of your existing VPC (e.g., subnet-abd39039). |
| Public subnet 1 ID (PublicSubnet1ID) | ***Blank string*** | ID of the public subnet in Availability Zone 1 of your existing VPC (e.g., subnet-a0246dcd). |
| Public subnet 2 ID (PublicSubnet2ID) | ***Blank string*** | ID of the public subnet in Availability Zone 2 of your existing VPC (e.g., subnet-b1236eea). |
| Public subnet 3 ID (PublicSubnet3ID) | ***Blank string*** | ID of the public subnet in Availability Zone 3 of your existing VPC (e.g., subnet-c3456aba). |
| Allowed external access CIDR (RemoteAccessCIDR) | ***Requires input*** | CIDR IP range that is permitted to access the instances. We recommend that you set this value to a trusted IP range. |
| SSH key name (KeyPairName) | ***Requires input*** | Name of an existing key pair, which allows you to securely connect to your instance after it launches. |
| Config set name (ConfigSetName) | ***Blank string*** | (Optional) Name used to map advanced parameters to an EKS cluster. If you launched an advanced configuration stack and would like to apply it’s values to this cluster, this name must match the "Config set name" parameter in that stack. If left blank, a new config set is created using default values. |
| Per-account shared resources (PerAccountSharedResources) | AutoDetect | Choose "No" if you already deployed another EKS Quick Start stack in your AWS account. |
| Per-Region shared resources (PerRegionSharedResources) | AutoDetect | Choose "No" if you already deployed another EKS Quick Start stack in your Region. |

| *Table 16. Network configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| HTTP proxy (HttpProxy) | ***Blank string*** | (Optional) HTTP(S) proxy configuration. If provided, all worker nodes and pod egress traffic uses this proxy. Example: <http://10.101.0.100:3128/>. |

| *Table 17. Amazon EC2 configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Provision bastion host (ProvisionBastionHost) | Enabled | Choose "Disabled" to skip creating a bastion host. |

| *Table 18. Amazon EKS configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| EKS cluster name (EKSClusterName) | ***Blank string*** | (Optional) Name for the EKS cluster. If left blank, one is auto-generated. This must be unique within the Region. |
| EKS public access endpoint (EKSPublicAccessEndpoint) | Disabled | Configure access to the Kubernetes API server endpoint from outside of your VPC. |
| Additional EKS admin ARN (IAM user) (AdditionalEKSAdminUserArn) | ***Blank string*** | (Optional) IAM user Amazon Resource Name (ARN) to be granted administrative access to the EKS cluster. |
| Additional EKS admin ARN (IAM role) (AdditionalEKSAdminRoleArn) | ***Blank string*** | (Optional) IAM role Amazon Resource Name (ARN) to be granted administrative access to the EKS cluster. |
| Fargate namespaces (FargateNamespaces) | ***Blank string*** | (Optional) Comma-separated list of namespaces for which Fargate should be enabled. |
| Fargate labels (FargateLabels) | ***Blank string*** | Requires at least one Fargate namespace to be specified. This is a comma-separated list of key-value pod labels. For a pod to run on Fargate, all of the labels must match, and it must run in a namespace defined by "Fargate namespaces". |

| *Table 19. Default EKS node group configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Instance type (NodeInstanceType) | t3.medium | EC2 instance type. |
| Number of nodes (NumberOfNodes) | 3 | Number of Amazon EKS node instances. The default is one for each of the three Availability Zones. |
| Maximum number of nodes (MaxNumberOfNodes) | 3 | Maximum number of Amazon EKS node instances. The default is three. |
| Instance family (NodeInstanceFamily) | Standard | Choose the instance family to match the value of "Node instance type." |
| Node group type (NodeGroupType) | Managed | Choose "Unmanaged" to create an Auto Scaling group without using the EKS-managed node groups feature. |
| Node group operating system (NodeGroupOS) | Amazon Linux 2 | Operating system to use for node instances. Note that if you choose "Windows," an additional Amazon Linux node group is created. |

| *Table 20. Snyk monitor (AWS Partner security)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Snyk integration (SnykIntegration) | Disabled | For more information, see <https://github.com/aws-quickstart/quickstart-eks-snyk/>. |
| Integration ID (SnykIntegrationId) | ***Blank string*** | If Snyk is enabled, a value must be provided. For more information, see <https://support.snyk.io/hc/en-us/articles/360003916158-Install-the-Snyk-controller-with-Helm>. |

| *Table 21. New Relic infrastructure (AWS Partner monitoring)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| New Relic integration (NewRelicIntegration) | Disabled | For more information, see <https://github.com/aws-quickstart/quickstart-eks-newrelic-infrastructure/>. |
| License key (NewRelicLicenseKey) | ***Blank string*** | If New Relic is enabled, this must be provided. For more information, see <https://docs.newrelic.com/docs/accounts/install-new-relic/account-setup/license-key>. |

| *Table 22. Calico policy [APN security partner]* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Calico policy integration (CalicoIntegration) | Disabled | For more information see <https://www.projectcalico.org/> . |

| *Table 23. Rafay Systems [APN software & internet partner]* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Rafay Systems integration (RafaySysIntegration) | Disabled | For more information see <https://aws-quickstart.github.io/quickstart-eks-rafay-systems/> . |
| Rafay project (RafaySysProject) | defaultproject | This is the name you want to use for you Rafay deployment. |
| Bootstrap S3 bucket (RafaySysBootstrapBucket) | ***Blank string*** | (Optional) S3 bucket to place the the rafay bootstrap yaml file. If left blank the EKS Quick Start bucket will be used. |
| Bootstrap S3 key (RafaySysBootstrapKey) | ***Blank string*** | (Optional) S3 key to place the the rafay bootstrap yaml file. If left blank the key will be rafay/<CLUSTER\_NAME>/cluster-bootstrap.yaml. |
| API key (RafaySysApiKey) | ***Blank string*** | Required if using an existing Rafay account. |
| API secret (RafaySysApiSecret) | ***Blank string*** | Required if using an existing Rafay account. |
| First name (RafaySysFirstName) | ***Blank string*** | Required if registering a new Rafay account. |
| Last name (RafaySysLastName) | ***Blank string*** | Required if registering a new Rafay account. |
| Organization name (RafaySysOrganizationName) | ***Blank string*** | Required if registering a new Rafay account. |
| Email (RafaySysEmail) | ***Blank string*** | Required if registering a new Rafay account. |

| *Table 24. HashiCorp Vault (AWS Partner security)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| HashiCorp Vault integration (VaultIntegration) | Disabled | For more information, see <https://github.com/aws-quickstart/quickstart-eks-hashicorp-vault/>. |
| Vault UI ACM SSL certificate ARN (VaultUIACMSSLCertificateArn) | ***Blank string*** | ARN of the load balancer’s ACM SSL certificate. If you don’t provide values for "Domain name" and "Hosted zone id", provide a value for "ACM SSL certificate ARN". |
| Route 53 hosted zone id (VaultUIHostedZoneID) | ***Blank string*** | Route 53 Hosted zone ID of the domain name. If you don’t provide an ACMSSLCertificateArn value, the Quick Start creates an ACM certificate for you using HostedZoneID in conjunction with DomainName. |
| Vault UI load balancer DNS name (VaultUIDomainName) | ***Blank string*** | Fully qualified DNS name for the vault-ui service load balancer. If you don’t provide a value for "ACM SSL certificate ARN", use the HostedZoneID. |

| *Table 25. HashiCorp Consul (AWS Partner containers)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| HashiCorp Consul integration (ConsulIntegration) | Disabled | For more information, see <https://github.com/aws-quickstart/quickstart-eks-hashicorp-consul/>. |
| ACM SSL certificate ARN (ConsulUIACMSSLCertificateArn) | ***Blank string*** | ARN of the load balancer’s ACM SSL certificate. If you don’t provide values for "Domain name" and "Hosted zone id", provide a value for "ACM SSL certificate ARN". |
| Route 53 hosted zone id (ConsulUIHostedZoneID) | ***Blank string*** | Route 53-hosted zone ID of the domain name. If you don’t provide an ACMSSLCertificateArn value, the Quick Start creates an ACM certificate for you using HostedZoneID in conjunction with DomainName. |
| Consul UI load balancer DNS name (ConsulUIDomainName) | ***Blank string*** | Fully qualified DNS name for the consul-ui service load balancer. If you don’t provide a value for "ACM SSL certificate ARN", use the HostedZoneID. |

| *Table 26. Rancher management (AWS Partner management)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Rancher management integration (RancherIntegration) | Disabled | For more information, see <https://github.com/aws-quickstart/quickstart-eks-rancher/>. |
| Rancher management domain name (RancherDomainName) | aws.private | DNS domain name that users can use to access the Rancher console. |

| *Table 27. Kubernetes add-ins* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| AWS load balancer controller (ALBIngressController) | Enabled | Choose "Enabled" to deploy the AWS load balancer controller. |
| Cluster autoscaler (ClusterAutoScaler) | Disabled | Choose "Enabled" to enable Kubernetes cluster autoscaler. |
| EFS storage class (EfsStorageClass) | Disabled | Choose "Enabled" to enable EFS storage class. |
| Prometheus integration (PrometheusIntegration) | Disabled | For more information see <https://prometheus.io/> . |
| Grafana integration (GrafanaIntegration) | Disabled | Grafana requires "Prometheus integration" to be enabled. For more information see <https://www.grafana.com/> . |
| Monitoring stack (MonitoringStack) | None | Enable monitoring stack with "Prometheus+Grafana." Warning: this is a legacy parameter and will be dropped from the next version of this Quick Start. Please use the "Grafana integration" and "Prometheus integration" parameters instead. |

| *Table 28. AWS Quick Start configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Quick Start S3 bucket name (QSS3BucketName) | aws-quickstart | S3 bucket name for the Quick Start assets. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-). |
| Quick Start S3 key prefix (QSS3KeyPrefix) | quickstart-amazon-eks/ | S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), periods (.) and forward slash (/). |
| Quick Start S3 bucket Region (QSS3BucketRegion) | us-east-1 | Region where the Quick Start S3 bucket (QSS3BucketName) is hosted. When using your own bucket, you must specify this value. |

Prepare an existing EKS cluster

| *Table 29. EKS cluster details* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| EKS cluster name (KubeClusterName) | ***Requires input*** | Name of the EKS cluster to enable for AWS CloudFormation. |
| VPC ID (VPCID) | ***Requires input*** | ID of the VPC that contains your EKS cluster (e.g., vpc-0343606e). |
| EKS subnet IDs (K8sSubnetIds) | ***Blank string*** | (Optional) Comma-separated list of subnet IDs associated with the EKS cluster. There must be routes to the Kubernetes, AWS CloudFormation, and EKS endpoints. Leave this blank for publicly accessible clusters. |
| HTTP proxy (HttpProxy) | ***Blank string*** | (Optional) HTTP(S) proxy configuration. If you provide a value, all worker nodes and pod egress traffic uses this proxy (e.g., <http://10.101.0.100:3128/>). |
| EKS security group (ControlPlaneSecurityGroup) | ***Blank string*** | (Optional) Security group ID attached to the EKS cluster. This must allow egress traffic to the Kubernetes, AWS CloudFormation, and EKS endpoints. Leave this blank for publicly accessible clusters. |
| Deploy account-level shared resources (PerAccountSharedResources) | AutoDetect | Choose "No" if you already deployed the EKS account shared resources in this AWS account. |
| Deploy Region-level shared resources (PerRegionSharedResources) | AutoDetect | Choose "No" if you already deployed the EKS shared resources stack in your Region. |

| *Table 30. AWS Quick Start configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Quick Start S3 bucket name (QSS3BucketName) | aws-quickstart | S3 bucket name for the Quick Start assets. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-). |
| Quick Start S3 key prefix (QSS3KeyPrefix) | quickstart-amazon-eks/ | S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), periods (.) and forward slash (/). |
| Quick Start S3 bucket Region (QSS3BucketRegion) | us-east-1 | Region where the Quick Start S3 bucket (QSS3BucketName) is hosted. When using your own bucket, you must specify this value. |

Configure advanced options

| *Table 31. Quick Start configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Config set name (ConfigSetName) | ***Requires input*** | (Optional) Name used to map advanced parameters to an EKS cluster. In order to apply the defined parameters, the name must match the name used when launching the main EKS Quick Start. |

| *Table 32. EKS cluster configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Kubernetes version (KubernetesVersion) | 1.18 | Kubernetes control plane version. |
| Kubernetes API public access CIDRs (EKSPublicAccessCIDRs) | 0.0.0.0/0 | These values are used only if the EKSPublicAccessEndpoint parameter is set to "Enabled." These are the public CIDR IP ranges permitted to access the Kubernetes API. They cannot contain private IP ranges. |
| Private access endpoint (EKSPrivateAccessEndpoint) | Enabled | Configure access to the Kubernetes API server endpoint from within your VPC. If this is set to "Disabled," "EKS public access endpoint" must be set to "Enabled." |
| Cluster logging types (EKSClusterLoggingTypes) | api, audit, authenticator, controllerManager, scheduler | EKS cluster control plane logs to be exported to Amazon CloudWatch Logs. |
| Encrypt secrets (EKSEncryptSecrets) | Enabled | Envelope encryption of Kubernetes secrets using KMS. |
| Encrypt secrets KMS key ARN (EKSEncryptSecretsKmsKeyArn) | ***Blank string*** | (Optional) KMS key to use for envelope encryption of Kubernetes secrets. If this parameter is omitted, a key is created for the cluster. The CMK must be symmetric, created in the same Region as the cluster, and if the CMK was created in a different account, the user must have access to the CMK. |
| Enable IAM OIDC provider (IamOidcProvider) | Enabled | Enables IAM roles for Kubernetes service accounts. |

| *Table 33. Default EKS node group configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Name (NodeGroupName) | Default | Name of the EKS node group. |
| Volume size (NodeVolumeSize) | 20 | Size of the node’s root EBS volumes. |
| Custom AMI ID (CustomAmiId) | ***Blank string*** | (Optional) If an AMI ID is specified, it is used instead of the AMI from your OS/Region. |
| Labels (Labels) | ***Blank string*** | (Optional) Comma-separated list of key-value pairs that represent node labels to assign to the node group. Ignore this if "Custom launch template" is provided. |
| Taints (Taints) | ***Blank string*** | (Optional) Comma-separated list of key-value pairs that represent node taints to assign to the node group. Ignore this if "Custom launch template" is provided. |
| Launch template ID (LaunchTemplateId) | ***Blank string*** | (Optional) ID of an existing launch template to use when creating the node group. |
| Launch template version (LaunchTemplateVersion) | ***Blank string*** | Must be specified if the LaunchTemplateId parameter is provided. It cannot be "$Latest" or "$Default." This value sets the launch template version for the node group. |
| Security group ID (NodeSecurityGroupId) | ***Blank string*** | (Optional) Provide the ID of a security group to use for this node group. If this is not specified, one is created. |
| Instance type 2 (NodeInstanceType2) | ***Blank string*** | (Optional) Only applies if the NodeGroupType parameter is set to "Unmanaged." This is the second type of EC2 instance for the nodes. |
| Instance type 3 (NodeInstanceType3) | ***Blank string*** | (Optional) Only applies if the NodeGroupType parameter is set to "Unmanaged." This is the third type of EC2 instance for the nodes. |
| Instance type 4 (NodeInstanceType4) | ***Blank string*** | (Optional) Only applies if the NodeGroupType parameter is set to "Unmanaged." This is the fourth type of EC2 instance for the nodes. |
| On-demand percentage (OnDemandPercentage) | 100 | Only applies if the NodeGroupType parameter is set to "Unmanaged." Set the percentage of on-demand instances and spot instances. With a default of 100, the percentages are 100% for on-demand instances and 0% for spot instances. |

| *Table 34. Bastion configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Operating system (BastionOS) | Amazon-Linux2-HVM | Linux distribution of the bastion host. |
| Bootstrap script (BastionBootstrapScript) | ***Blank string*** | (Optional) Custom initialization script to run during setup. If left blank, the default bootstrap script is used. |
| Instance type (BastionInstanceType) | t3.micro | Instance type for the bastion host. |
| Root volume size (BastionRootVolumeSize) | 10 | Size in GB for the root EBS volume. |
| IAM role name (BastionIAMRoleName) | ***Blank string*** | (Optional) An existing IAM role name to attach to the bastion host. If left blank, a new role is created. |
| Enable TCP forwarding (BastionEnableTCPForwarding) | false | Choose "true" to enable TCP forwarding. |
| Enable X11 forwarding (BastionEnableX11Forwarding) | false | Choose "true" to enable X11 forwarding. |
| Variables (BastionVariables) | ***Blank string*** | (Optional) Comma-separated list of environment variables for bootstrapping. The variables must be in the format KEY=VALUE. VALUE cannot contain commas. |

| *Table 35. HashiCorp Vault (AWS Partner security)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Kubernetes namespace for HashiCorp Vault (VaultKubernetesNameSpace) | vault-server | Kubernetes namespace for HashiCorp Vault. |
| Consul UI Internal or external load balancer? (VaultUILoadBalancerType) | External | Choose whether the load balancer for HashiCorp Vault is internal or external to the VPC. |
| Permitted IP range for Vault UI (VaultUIAccessCIDR) | 127.0.0.1/32 | The CIDR IP range that is permitted to access Vault. Note: A value of 0.0.0.0/0 allows access from ANY IP address. |
| HashiCorp Vault version (VaultVersion) | 1.6.0 | (Optional) |
| HashiCorp Vault deployment size (VaultDeploymentSize) | small | Deployment size of dedicated HashiCorp Vault nodes. |
| HashiCorp Vault server nodes (VaultNodes) | 3 | The number of dedicated Vault server nodes and pods. |

| *Table 36. HashiCorp Consul (AWS Partner containers)* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Kubernetes namespace for HashiCorp Consul (ConsulKubernetesNameSpace) | consul-server | Kubernetes namespace for HashiCorp Consul. |
| Consul UI Internal or external load balancer? (ConsulUILoadBalancerType) | Internal | Choose whether the load balancer for HashiCorp Consul is internal or external to the VPC. |
| Permitted IP range for Consul UI (ConsulUIAccessCIDR) | 127.0.0.1/32 | The CIDR IP range that is permitted to access Consul Note: A value of 0.0.0.0/0 allows access from ANY IP address. |
| HashiCorp Consul version (ConsulVersion) | 1.8.4 | NO\_DESCRIPTION |
| HashiCorp Consul deployment size (ConsulDeploymentSize) | small | Deployment size of dedicated HashiCorp Consul nodes. |
| HashiCorp Consul server nodes (ConsulNodes) | 3 | The number of dedicated Consul server nodes and pods. |

| *Table 37. EFS storage class configuration* | | |
| --- | --- | --- |
| **Parameter label (name)** | **Default value** | **Description** |
| Performance mode (EfsPerformanceMode) | generalPurpose | Only applies if the EfsStorageClass parameter is set to "Enabled." Choose "maxIO" mode to provide greater IOPS with an increased latency. |
| Throughput mode (EfsThroughputMode) | bursting | Only applies if the EfsStorageClass parameter is set to "Enabled." For throughput that is not dependent on the amount of data stored in the file system, choose "provisioned." |
| Provisioned throughput in Mibps (EfsProvisionedThroughputInMibps) | 0 | Only applies if the EfsStorageClass parameter is set to "Enabled." If "EFS throughput mode" is set, the "provisioned" value must be in the 0–1024 range. If it’s set to "bursting," this must be set to 0. |

Send us feedback

To post feedback, submit feature ideas, or report bugs, use the **Issues** section of the [GitHub repository](https://github.com/aws-quickstart/quickstart-amazon-eks) for this Quick Start. To submit code, see the [Quick Start Contributor’s Guide](https://aws-quickstart.github.io/).

Quick Start reference deployments

See the [AWS Quick Start home page](https://aws.amazon.com/quickstart/).

GitHub repository

Visit our [GitHub repository](https://github.com/aws-quickstart/quickstart-amazon-eks) to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

Notices

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether expressed or implied. This document does not create any warranties, representations, contractual commitments, conditions, or assurances from AWS, its affiliates, suppliers, or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at <http://aws.amazon.com/apache2.0/> or in the accompanying "license" file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either expressed or implied. See the License for specific language governing permissions and limitations.