

# Modular and Scalable Amazon EKS Architecture

## Quick Start Reference Deployment

*February 2019*  
*([last update](#): March 2020)*

*Jay McConnell, AWS Quick Start team*

Visit our [GitHub repository](#) for source files and to post feedback, report bugs, or submit feature ideas for this Quick Start.

### Contents

Overview .....	2
Amazon EKS.....	2
Cost.....	3
Architecture .....	3
Planning the deployment .....	5
Specialized knowledge .....	5
AWS account .....	5
Technical requirements .....	5
Deployment options.....	6
Deployment steps .....	7
Step 1. Sign in to your AWS account.....	7
Step 2. Launch the Quick Start .....	7
Option 1: Parameters for deploying Amazon EKS into a new VPC .....	9
Option 2: Parameters for deploying Amazon EKS into an existing VPC .....	12
Step 3. Test the deployment .....	16

Best practices for using Amazon EKS .....	16
Use AWS CloudFormation for ongoing management.....	16
Monitor additional resource usage.....	17
Security .....	17
Adding Kubernetes users .....	17
Managing Kubernetes resources using AWS CloudFormation .....	17
Optional add-ins.....	18
Cluster autoscaler.....	18
Managed Node Group.....	18
EFS StorageClass .....	18
FAQ.....	18
Send us feedback .....	19
Additional resources .....	19
Document revisions.....	20

This Quick Start was created by Solutions Architects at Amazon Web Services (AWS).

[Quick Starts](#) 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 are looking for a repeatable, customizable reference deployment for Amazon EKS using AWS CloudFormation.

## Amazon EKS

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

Amazon EKS runs the Kubernetes management infrastructure for you across multiple AWS Availability Zones to eliminate a single point of failure. Amazon EKS is certified

Kubernetes-conformant, so you can use existing tooling and plugins from partners and the Kubernetes community. Applications running on any standard Kubernetes environment are fully compatible and can be migrated to Amazon EKS.

This reference deployment provides AWS CloudFormation templates to deploy the Kubernetes control plane, connect worker nodes to the cluster, and configure a bastion host for cluster admin operations. Additionally, the Quick Start deployment provides [custom resources](#) that enable you to deploy and manage your Kubernetes applications using AWS CloudFormation by declaring Kubernetes manifests or Helm charts directly in AWS CloudFormation templates. The included Cluster Autoscaler and Amazon Elastic File System (Amazon EFS) storage options are made possible by this mechanism and are discussed in detail in the [Optional add-ins](#) section.

## Cost

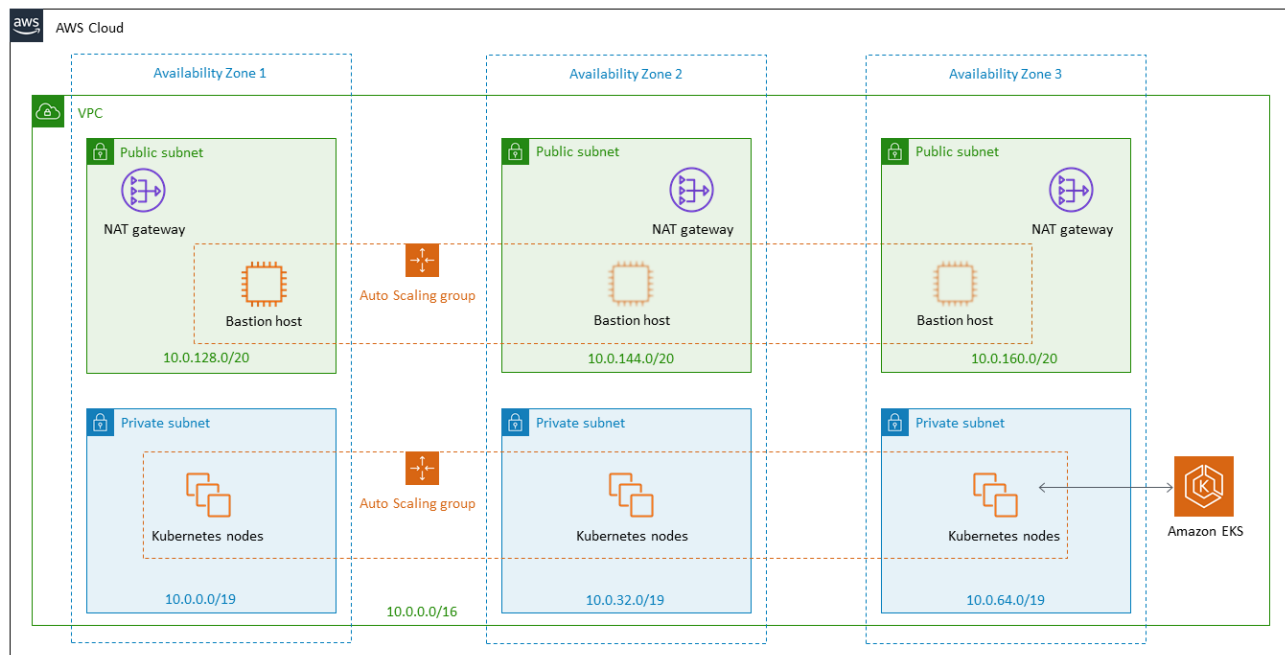
You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

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

**Tip:** After you deploy the Quick Start, we recommend that you enable the [AWS Cost and Usage Report](#) to track costs associated with the Quick Start. This report delivers billing metrics to an S3 bucket in your account. It provides cost estimates based on usage throughout each month, and finalizes the data at the end of the month. For more information about the report, see the [AWS documentation](#).

## 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.



**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 provides 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 Quick Start assumes familiarity with Kubernetes concepts and usage. Sections that cover building AWS CloudFormation templates using the provided custom resources assume knowledge of authoring AWS CloudFormation templates.

This deployment guide also requires a moderate level of familiarity with AWS services. If you're new to AWS, visit the [Getting Started Resource Center](#) and the [AWS Training and Certification website](#) for materials and programs that can help you develop the skills to design, deploy, and operate your infrastructure and applications on the AWS Cloud.

### AWS account

If you don't already have an AWS account, create one at <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.

### Technical requirements

Before you launch the Quick Start, your account must be configured as specified in the following table. Otherwise, deployment might fail.

#### [Resources](#)

If necessary, request [service quota increases](#) for the following resources. You might need to do this if an existing deployment uses these resources, and you might exceed the default quotas with this deployment. The [Service Quotas console](#) displays your usage and quotas for some aspects of some services. For more information, see the [AWS documentation](#).

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

<a href="#">Regions</a>	Amazon EKS and Amazon EFS aren't currently supported in all AWS Regions. For a current list of supported Regions, see <a href="#">Service Endpoints and Quotas</a> in the AWS documentation.
<a href="#">Key pair</a>	<p>Make sure that at least one Amazon EC2 key pair exists in your AWS account in the Region where you are planning to deploy the Quick Start. Make note of the key pair name. You'll be prompted for this information during deployment. To create a key pair, follow the <a href="#">instructions in the AWS documentation</a>.</p> <p>If you're deploying the Quick Start for testing or proof-of-concept purposes, we recommend that you create a new key pair instead of specifying a key pair that's already being used by a production instance.</p>
<a href="#">Amazon S3 URLs</a>	If you're copying the templates to your own S3 bucket for deployment, make sure that you update the <code>QSS3Bucket</code> and <code>QSS3Prefix</code> parameters to reflect the location of the files in your bucket. <b>Otherwise, deployment may fail or behave unexpectedly.</b>
<a href="#">IAM permissions</a>	To deploy the Quick Start, you must log in to the AWS Management Console with IAM permissions for the resources and actions the templates will deploy. The <i>AdministratorAccess</i> managed policy within IAM provides sufficient permissions, although your organization may choose to use a custom policy with more restrictions.
<a href="#">S3 buckets</a>	Unique S3 bucket names are automatically generated based on the account number and Region. If you delete a stack, <b>the logging buckets are not deleted</b> (to support security review). If you plan to re-deploy this Quick Start in the same Region, you must first manually delete the S3 buckets that were created during the previous deployment; <b>otherwise, the re-deployment will fail.</b>

## Deployment options

This Quick Start provides two 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.

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

### Step 1. Sign in to your AWS account

1. Sign in to your AWS account at <https://aws.amazon.com> with an IAM user role that has the necessary permissions. For details, see [Planning the deployment](#) earlier in this guide.
2. Make sure that your AWS account is configured correctly, as discussed in the [Technical requirements](#) section.
3. Use the Region selector in the navigation bar to choose the AWS Region where you want to deploy Amazon EKS.

**Note:** Amazon EKS and Amazon EFS aren't currently supported in all AWS Regions. For a current list of supported Regions, see the [endpoints and quotas webpage](#).

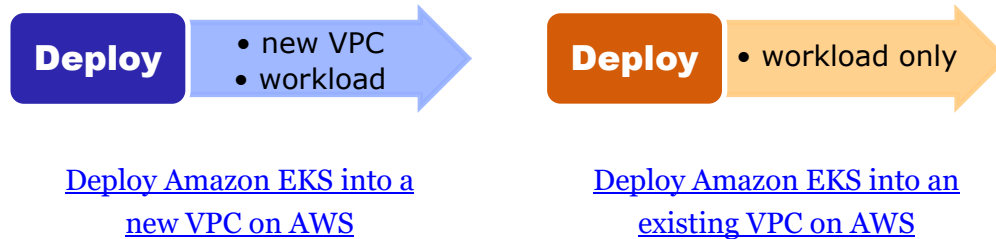
4. Select the key pair that you created earlier. In the navigation pane of the [Amazon EC2 console](#), choose **Key Pairs**, and then choose your key pair from the list.

### Step 2. Launch the Quick Start

**Notes:** The instructions in this section reflect the older version of the AWS CloudFormation console. If you're using the redesigned console, some of the user interface elements might be different.

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option, see [deployment options](#) earlier in this guide.



**Important:** If you're deploying Amazon EKS into an existing VPC, make sure that your VPC has three private subnets in different Availability Zones for the workload instances. These subnets require [NAT gateways or NAT instances](#) in their route tables, to allow the instances to download packages and software without exposing them to the internet. You will also need to tag each private subnet with the tag `kubernetes.io/role/internal-elb=true` and each public subnet with the tag `kubernetes.io/role/elb=true` if you want to use the Kubernetes integration with Elastic Load Balancing.

Each deployment takes about 25 minutes to complete.

2. 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 where Amazon EKS will be built. The template is launched in the US East (Ohio) Region by default.

**Note:** Amazon EKS and Amazon EFS aren't currently supported in all AWS Regions. For a current list of supported Regions, see the [endpoints and quotas webpage](#).

3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.
4. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary.

In the following tables, parameters are listed by category and described separately for the two deployment options:



- [Parameters for deploying Amazon EKS into a new VPC](#)
- [Parameters for deploying Amazon EKS into an existing VPC](#)

When you finish reviewing and customizing the parameters, choose **Next**.

## OPTION 1: PARAMETERS FOR DEPLOYING AMAZON EKS INTO A NEW VPC

[View template](#)

*VPC network configuration:*

Parameter label (name)	Default	Description
<b>Availability Zones</b> (AvailabilityZones)	<i>Requires input</i>	The list of Availability Zones to use for the subnets in the VPC. Three Availability Zones are used for this deployment, and the logical order of your selections is preserved.
<b>VPC CIDR</b> (VPCCIDR)	10.0.0.0/16	The CIDR block for the VPC.
<b>Private subnet 1 CIDR</b> (PrivateSubnet1CIDR)	10.0.0.0/19	The CIDR block for private subnet 1 located in Availability Zone 1.
<b>Private subnet 2 CIDR</b> (PrivateSubnet2CIDR)	10.0.32.0/19	The CIDR block for private subnet 2 located in Availability Zone 2.
<b>Private subnet 3 CIDR</b> (PrivateSubnet3CIDR)	10.0.64.0/19	The CIDR block for private subnet 3 located in Availability Zone 3.
<b>Public subnet 1 CIDR</b> (PublicSubnet1CIDR)	10.0.128.0/20	The CIDR block for the public (DMZ) subnet 1 located in Availability Zone 1.
<b>Public subnet 2 CIDR</b> (PublicSubnet2CIDR)	10.0.144.0/20	The CIDR block for the public (DMZ) subnet 2 located in Availability Zone 2.
<b>Public subnet 3 CIDR</b> (PublicSubnet3CIDR)	10.0.160.0/20	The CIDR block for the public (DMZ) subnet 3 located in Availability Zone 3.
<b>Allowed external access CIDR</b> (RemoteAccessCIDR)	<i>Requires input</i>	The CIDR IP range that is permitted to access the instances. We recommend that you set this value to a trusted IP range.

*Amazon EC2 configuration:*

Parameter label (name)	Default	Description
<b>SSH key name</b> (KeyPairName)	<i>Requires input</i>	The name of an existing public/private key pair, which allows you to securely connect to your instance after it launches.

*Amazon EKS configuration:*

Parameter label (name)	Default	Description
<b>Nodes instance type</b> (NodeInstanceType)	t3.medium	The type of EC2 instance for the node instances.
<b>Number of nodes</b> (NumberOfNodes)	3	The number of Amazon EKS node instances. The default is one for each of the three Availability Zones.
<b>Node group name</b> (NodeGroupName)	Default	The name for the EKS node group.
<b>Node volume size</b> (NodeVolumeSize)	20	The size for the node's root Amazon Elastic Block Store (Amazon EBS) volumes.
<b>Managed node group</b> (ManagedNodeGroup)	no	Choose if you want to use a managed node group. If you choose <b>yes</b> , you must select Kubernetes version 1.14 or higher.
<b>Managed node group AMI type</b> (ManagedNodeGroupAMIType)	AL2_x86_64	Select one of the two AMI types for your managed node group (only applies if you chose <b>yes</b> for <code>ManagedNodeGroup</code> ). GPU instance types should use the <code>AL2_x86_64_GPU</code> AMI type, which uses the Amazon EKS–optimized Linux AMI with GPU support. Non-GPU instances should use the <code>AL2_x86_64</code> AMI type, which uses the Amazon EKS–optimized Linux AMI.
<b>Additional EKS admin ARNs</b> (AdditionalEKSAAdminArns)	<i>Optional</i>	The comma-separated list of IAM user/role Amazon Resource Names (ARNs) to be granted administrator access to the EKS cluster.
<b>Kubernetes version</b> (KubernetesVersion)	1.15	The Kubernetes control plane version. The supported versions for this Quick Start are 1.13, 1.14, and 1.15.

*Optional Kubernetes add-ins:*

Parameter label (name)	Default	Description
<b>Cluster autoscaler</b> (ClusterAutoScaler)	Disabled	Choose <b>Enabled</b> to enable Kubernetes cluster autoscaler.
<b>EFS storage class</b> (EfsStorageClass)	Disabled	Choose <b>Enabled</b> to enable EFS storage class, which will create the required EFS volume.
<b>EFS performance mode</b> (EfsPerformanceMode)	generalPurpose	Choose <b>maxIO</b> mode to provide greater IOPS with an increased latency. Only has an effect when <code>EfsStorageClass</code> is enabled.
<b>EFS throughput mode</b> (EfsThroughputMode)	bursting	Choose <b>provisioned</b> for throughput that is not dependent on the amount of data stored in the file system. Only has an effect when <code>EfsStorageClass</code> is enabled.
<b>EFS provisioned throughput in Mibps</b> (EfsProvisionedThroughputInMibps)	0	Set to <b>0</b> if <code>EfsThroughputMode</code> is set to <code>bursting</code> . Only has an effect when <code>EfsStorageClass</code> is enabled.

*AWS Quick Start configuration:*

Parameter label (name)	Default	Description
<b>Quick Start S3 bucket name</b> (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 (-).
<b>Quick Start S3 key prefix</b> (QSS3KeyPrefix)	quickstart-amazon-eks/	S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).
<b>Lambda zips bucket name</b> (LambdaZipsBucketName)	<i>Optional</i>	The name of the S3 bucket where the Lambda .zip files should be placed. If you leave this parameter blank, an S3 bucket will be created.

## OPTION 2: PARAMETERS FOR DEPLOYING AMAZON EKS INTO AN EXISTING VPC

[View template](#)

*Network configuration:*

Parameter label (name)	Default	Description
<b>VPC ID</b> (VPCID)	<i>Requires input</i>	The ID of your existing VPC (e.g., vpc-0343606e).
<b>Private subnet 1 ID</b> (PrivateSubnet1ID)	<i>Requires input</i>	The ID of the private subnet in Availability Zone 1 in your existing VPC (e.g., subnet-fe9a8b32).
<b>Private subnet 2 ID</b> (PrivateSubnet2ID)	<i>Requires input</i>	The ID of the private subnet in Availability Zone 2 in your existing VPC (e.g., subnet-be8b01ea).
<b>Private subnet 3 ID</b> (PrivateSubnet3ID)	<i>Requires input</i>	The ID of the private subnet in Availability Zone 3 in your existing VPC (e.g., subnet-abd39039).
<b>Public subnet 1 ID</b> (PublicSubnet1ID)	<i>Requires input</i>	The ID of the public subnet in Availability Zone 1 in your existing VPC (e.g., subnet-a0246dcd).
<b>Public subnet 2 ID</b> (PublicSubnet2ID)	<i>Requires input</i>	The ID of the public subnet in Availability Zone 2 in your existing VPC (e.g., subnet-b1236eea).
<b>Public subnet 3 ID</b> (PublicSubnet3ID)	<i>Requires input</i>	The ID of the public subnet in Availability Zone 3 in your existing VPC (e.g., subnet-c3456aba).
<b>Allowed external access CIDR</b> (RemoteAccessCIDR)	<i>Requires input</i>	The CIDR IP range that is permitted to access the instances. We recommend that you set this value to a trusted IP range.

*Amazon EC2 configuration:*

Parameter label (name)	Default	Description
<b>SSH key name</b> (KeyPairName)	<i>Requires input</i>	The name of an existing public/private key pair, which allows you to securely connect to your instance after it launches.

*Amazon EKS configuration:*

Parameter label (name)	Default	Description
<b>Nodes instance type</b> (NodeInstanceType)	t3.medium	The type of EC2 instance for the node instances
<b>Number of nodes</b> (NumberOfNodes)	3	The number of EKS node instances. The default is one for each of the three Availability Zones.
<b>Node group name</b> (NodeGroupName)	Default	The name for the EKS node group.
<b>Node volume size</b> (NodeVolumeSize)	20	The size for the node's root EBS volumes.
<b>Managed node group</b> (ManagedNodeGroup)	no	Choose if you want to use a managed node group. If you choose <b>yes</b> , you must select Kubernetes version 1.14 or higher.
<b>Managed node group AMI type</b> (ManagedNodeGroupAMIType)	AL2_x86_64	Select one of the two AMI types for your managed node group (only applies if you chose <b>yes</b> for <code>ManagedNodeGroup</code> ). GPU instance types should use the <code>AL2_x86_64_GPU</code> AMI type, which uses the Amazon EKS–optimized Linux AMI with GPU support. Non-GPU instances should use the <code>AL2_x86_64</code> AMI type, which uses the Amazon EKS–optimized Linux AMI.
<b>Additional EKS admin ARNs</b> (AdditionalEKSAAdminArns)	<i>Optional</i>	The comma separated list of IAM user/role ARNs to be granted admin access to the EKS cluster
<b>Kubernetes version</b> (KubernetesVersion)	1.15	The Kubernetes control plane version. The supported versions for this Quick Start are 1.13, 1.14, and 1.15.

*Optional Kubernetes add-ins:*

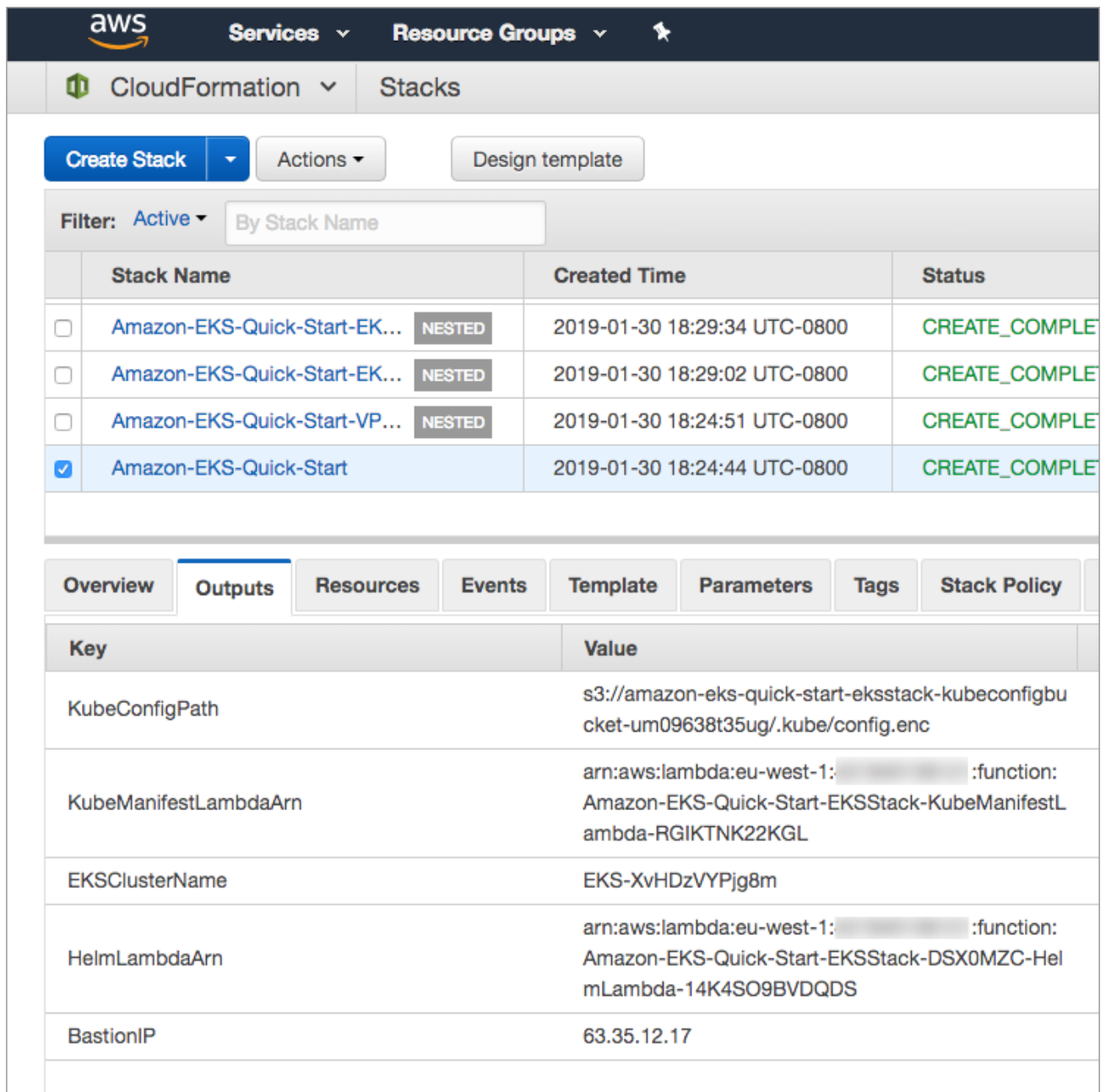
Parameter label (name)	Default	Description
<b>Cluster autoscaler</b> (ClusterAutoScaler)	Disabled	Choose <b>Enabled</b> to enable Kubernetes cluster autoscaler.
<b>EFS storage class</b> (EfsStorageClass)	Disabled	Choose <b>Enabled</b> to enable EFS storage class, which will create the required EFS volume.
<b>EFS performance mode</b> (EfsPerformanceMode)	generalPurpose	Choose <b>maxIO</b> mode to provide greater IOPS with an increased latency. Only has an effect when <code>EfsStorageClass</code> is enabled.
<b>EFS throughput mode</b> (EfsThroughputMode)	bursting	Choose <b>provisioned</b> for throughput that is not dependent on the amount of data stored in the file system. Only has an effect when <code>EfsStorageClass</code> is enabled.
<b>EFS provisioned throughput in Mibps</b> (EfsProvisionedThroughputInMibps)	0	Set to <b>0</b> if <code>EfsThroughputMode</code> is set to <code>bursting</code> . Only has an effect when <code>EfsStorageClass</code> is enabled.

*AWS Quick Start configuration:*

Parameter label (name)	Default	Description
<b>Quick Start S3 bucket name</b> (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 (-).
<b>Quick Start S3 key prefix</b> (QSS3KeyPrefix)	quickstart-amazon-eks/	S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).
<b>Lambda zips bucket name</b> (LambdaZipsBucketName)	<i>Optional</i>	The name of the S3 bucket where the Lambda .zip files should be placed. If you leave this parameter blank, an S3 bucket will be created.

- On the **Options** page, you can [specify tags](#) (key-value pairs) for resources in your stack and [set advanced options](#). When you're done, choose **Next**.
- On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the two check boxes to acknowledge that the template will create IAM resources and that it might require the capability to auto-expand macros.

7. Choose **Create** to deploy the stack.
8. Monitor the status of the stack. When the status is **CREATE\_COMPLETE**, the Amazon EKS cluster is ready.
9. Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.



The screenshot shows the AWS CloudFormation console interface. At the top, there's a navigation bar with 'AWS', 'Services', and 'Resource Groups'. Below this, the 'CloudFormation' service is selected, and the 'Stacks' tab is active. A 'Create Stack' button is visible. Below the buttons, there's a filter section with 'Filter: Active' and a search box 'By Stack Name'. A table lists several stacks, all with a status of 'CREATE\_COMPLETE'. The selected stack is 'Amazon-EKS-Quick-Start'.

Stack Name	Created Time	Status
Amazon-EKS-Quick-Start-EK... NESTED	2019-01-30 18:29:34 UTC-0800	CREATE_COMPLETE
Amazon-EKS-Quick-Start-EK... NESTED	2019-01-30 18:29:02 UTC-0800	CREATE_COMPLETE
Amazon-EKS-Quick-Start-VP... NESTED	2019-01-30 18:24:51 UTC-0800	CREATE_COMPLETE
Amazon-EKS-Quick-Start	2019-01-30 18:24:44 UTC-0800	CREATE_COMPLETE

Below the stack list, the 'Outputs' tab is selected. It shows a table with the following outputs:

Key	Value
KubeConfigPath	s3://amazon-eks-quick-start-eksstack-kubeconfigbucket-um09638t35ug/.kube/config.enc
KubeManifestLambdaArn	arn:aws:lambda:eu-west-1: [redacted]:function: Amazon-EKS-Quick-Start-EKSStack-KubeManifestLambda-RGIKTNK22KGL
EKSClusterName	EKS-XvHDzVYPjg8m
HelmLambdaArn	arn:aws:lambda:eu-west-1: [redacted]:function: Amazon-EKS-Quick-Start-EKSStack-DSX0MZC-HelmLambda-14K4SO9BVDQDS
BastionIP	63.35.12.17

**Figure 2: Amazon EKS outputs after successful deployment**

### Step 3. Test the deployment

1. Connect to the bastion host by using SSH with the key pair that you specified during deployment and the IP address in that is displayed on the **Outputs** tab of the AWS CloudFormation stack.
2. The bastion host already has `kubectl` installed and configured to be able to connect to the cluster. To test the CLI's ability to connect to the cluster, run the following command.

```
$ kubectl version
```

Confirm that the output includes the `Server Version`, which indicates a successful connection 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"}
```

3. Now check that the nodes have successfully connected to the 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 to manage updating and deleting the resources that are created by this Quick Start. Using the Amazon EC2 console, CLI, or API to change or delete created by this Quick Start 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 be able to create ELB load balancers and Amazon EBS volumes as part of their Kubernetes applications. As these carry additional costs, we recommend that you grant users of the Amazon EKS cluster only the permissions they require via [Kubernetes Role Based Access Control \(RBAC\)](#) and that you monitor the resource usage by using the Kubernetes CLI or the Kubernetes API to describe the persistent volume claims (PVC) and LoadBalancer resources across all namespaces. To disable this functionality, you can update the `ControlPlaneRole` IAM role created in the IAM child stack to deny the Kubernetes control plane access to specific AWS APIs like `ec2:CreateVolume` or `elb:CreateLoadBalancer`.

## Security

Amazon EKS uses IAM to provide authentication to your Kubernetes cluster (through the AWS IAM Authenticator for Kubernetes), but it still relies on native Kubernetes RBAC for authorization. This means that IAM is used only for authentication of valid IAM entities. All permissions for interacting with your Amazon EKS cluster's Kubernetes API are managed through 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 the Linux bastion host use the IAM role to provide access to the Kubernetes API. Additional IAM users or roles can be added as Kubernetes admin users (`system:master`) by entering a comma-separated list of ARNs into the `AdditionalEKSAAdminArns` parameter when you launch this Quick Start. To add users after the stack has launched, connect by using SSH into the bastion host and follow the steps in the [Amazon EKS documentation](#).

## Managing Kubernetes resources using AWS CloudFormation

This Quick Start includes Lambda functions that can be used as custom resources to enable authoring, creating, and managing Kubernetes-based applications using AWS CloudFormation. For example usage, see the [example-workload template](#). The needed Lambda function ARNs can be retrieved from the outputs of the **Functions** stack that was deployed when the Quick Start was launched.

## Optional add-ins

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

### Cluster autoscaler

[Cluster autoscaler](#) automatically adjusts the size of the Kubernetes cluster when there are insufficient resources or nodes that have been underutilized for an extended period of time.

### Managed node group

With Amazon EKS–managed node groups, the 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 of the QuickStart. 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 not tied to an individual Availability Zone and is well suited for highly available stateful applications that are required to survive an Availability Zone outage. The Amazon EFS volume is made available to Kubernetes pods by the [EFS provisioner project](#).

There are several configuration options available to tune the performance and throughput of the underlying EFS volume. For details, see the [Amazon EFS documentation](#).

## 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 **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack’s state will be retained and the instances will be left running, so you can troubleshoot the issue.

**Important:** When you set **Rollback on failure** to **No**, you will continue to incur AWS charges for this stack. Please make sure to delete the stack when you finish troubleshooting.

For additional information, see [Troubleshooting AWS CloudFormation](#) on the AWS website.

**Q.** The `Custom::KubeManifest/Custom::Helm` resources failed on stack create, update, or deletion.

**A.** These resources are backed by Lambda functions that are defined in the **Functions** stack. Their logs are stored in Amazon CloudWatch Logs and can be accessed by navigating to the Lambda console, selecting the relevant Lambda function and choosing **Open in CloudWatch Logs**.

**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-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the [AWS documentation](#).

## Send us feedback

To post feedback, submit feature ideas, or report bugs, use the **Issues** section of the [GitHub repository](#) for this Quick Start. If you'd like to submit code, please review the [Quick Start Contributor's Guide](#).

## Additional resources

### AWS resources

- [Getting Started Resource Center](#)
- [AWS General Reference](#)
- [AWS Glossary](#)

### AWS services

- [Amazon EKS](#)
- [AWS CloudFormation](#)
- [Amazon EC2](#)
- [IAM](#)

- [Amazon VPC](#)
- [AWS Lambda](#)
- [Amazon CloudWatch Logs](#)
- [Amazon EBS](#)
- [AWS Elastic Load Balancing](#)
- [Amazon EFS](#)

### Kubernetes documentation

- [Homepage](#)
- [awsElasticBlockStore volumes](#)
- [Type LoadBalancer services](#)
- [Cluster Autoscaler](#)
- [EFS provisioner](#)

### Other Quick Start reference deployments

- [AWS Quick Start home page](#)

## Document revisions

Date	Change	In sections
<b>March 2020</b>	Updated the Kubernetes versions	Step 2. Launch the Quick Start; Optional add-ins
<b>June 2019</b>	Added support for optional Kubernetes add-ins; updated the Kubernetes versions	Overview; Step 2. Launch the Quick Start; Optional add-ins
<b>February 2019</b>	Initial publication	—

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

### **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 express 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 "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.