



Red Hat OpenShift

Configuring an AWS account

- [Configuring Route 53](#)
 - [Ingress Operator endpoint configuration for AWS Route 53](#)
- [AWS account limits](#)
- [Required AWS permissions for the IAM user](#)
- [Creating an IAM user](#)
- [IAM Policies and AWS authentication](#)
 - [Default permissions for IAM instance profiles](#)
 - [Specifying an existing IAM role](#)
 - [Using AWS IAM Analyzer to create policy templates](#)
- [Supported AWS Marketplace regions](#)
- [Supported AWS regions](#)
 - [AWS public regions](#)
 - [AWS GovCloud regions](#)
 - [AWS SC2S and C2S secret regions](#)
 - [AWS China regions](#)
- [Next steps](#)

Before you can install OpenShift Container Platform, you must configure an Amazon Web Services (AWS) account.

Configuring Route 53

To install OpenShift Container Platform, the Amazon Web Services (AWS) account you use must have a dedicated public hosted zone in your Route 53 service. This zone must be authoritative for the domain. The Route 53 service provides cluster DNS resolution and name lookup for external connections to the cluster.

Procedure

- Identify your domain, or subdomain, and registrar. You can transfer an existing domain and registrar or obtain a new one through AWS or another source.



If you purchase a new domain through AWS, it takes time for the relevant DNS changes to propagate. For more information about purchasing domains through AWS, see [Registering Domain Names Using Amazon Route 53](#) in the AWS documentation.

- If you are using an existing domain and registrar, migrate its DNS to AWS. See [Making Amazon Route 53 the DNS Service for an Existing Domain](#) in the AWS documentation.
- Create a public hosted zone for your domain or subdomain. See [Creating a Public Hosted Zone](#) in the AWS documentation.

Use an appropriate root domain, such as `openshiftcorp.com`, or subdomain, such as `clusters.openshiftcorp.com`.

- Extract the new authoritative name servers from the hosted zone records. See [Getting the Name Servers for a Public Hosted Zone](#) in the AWS documentation.
- Update the registrar records for the AWS Route 53 name servers that your domain uses. For example, if you registered your domain to a Route 53 service in a different accounts, see the following topic in the AWS documentation: [Adding or Changing Name Servers or Glue Records](#).
- If you are using a subdomain, add its delegation records to the parent domain. This gives Amazon Route 53 responsibility for the subdomain. Follow the delegation procedure outlined by the DNS provider of the parent domain. See [Creating a subdomain that uses Amazon Route 53 as the DNS service without migrating the parent domain](#) in the AWS documentation for an example high level procedure.

Ingress Operator endpoint configuration for AWS Route 53

If you install in either Amazon Web Services (AWS) GovCloud (US) US-West or US-East region, the Ingress Operator uses `us-gov-west-1` region for Route53 and tagging API clients.

The Ingress Operator uses <https://tagging.us-gov-west-1.amazonaws.com> as the tagging API endpoint if a tagging custom endpoint is configured that includes the string 'us-gov-east-1'.

For more information on AWS GovCloud (US) endpoints, see the [Service Endpoints](#) in the AWS documentation about GovCloud (US).



Private, disconnected installations are not supported for AWS GovCloud when you install in the `us-gov-east-1` region.

Example Route 53 configuration

```
platform:
  aws:
    region: us-gov-west-1
    serviceEndpoints:
      - name: ec2
        url: https://ec2.us-gov-west-1.amazonaws.com
      - name: elasticloadbalancing
        url: https://elasticloadbalancing.us-gov-west-1.amazonaws.com
      - name: route53
        url: https://route53.us-gov.amazonaws.com (1)
      - name: tagging
        url: https://tagging.us-gov-west-1.amazonaws.com (2)
```


- 1 Route 53 defaults to <https://route53.us-gov.amazonaws.com> for both AWS GovCloud (US) regions.
- 2 Only the US-West region has endpoints for tagging. Omit this parameter if your cluster is in another region.

AWS account limits

The OpenShift Container Platform cluster uses a number of Amazon Web Services (AWS) components, and the default [Service Limits](#) affect your ability to install OpenShift Container Platform clusters. If you use certain cluster configurations, deploy your cluster in certain AWS regions, or run multiple clusters from your account, you might need to request additional resources for your AWS account.

The following table summarizes the AWS components whose limits can impact your ability to install and run OpenShift Container Platform clusters.

Component	Number of clusters available by default	Default AWS limit	Description
Instance Limits	Varies	Varies	<p>By default, each cluster creates the following instances:</p> <ul style="list-style-type: none">■ One bootstrap machine, which is removed after installation■ Three control plane nodes■ Three worker nodes <p>These instance type counts are within a new account's default limit. To deploy more worker nodes, enable autoscaling, deploy large workloads, or use a different instance type, review your account limits to ensure that your cluster can deploy the machines that you need.</p> <p>In most regions, the worker machines use an <code>m6i.large</code> instance and the bootstrap and control plane machines use <code>m6i.xlarge</code> instances. In some regions, including all regions that do not support these instance types, <code>m5.large</code> and <code>m5.xlarge</code> instances are used instead.</p>

Component	Number of clusters available by default	Default AWS limit	Description
Elastic IPs (EIPs)	0 to 1	5 EIPs per account	<p>To provision the cluster in a highly available configuration, the installation program creates a public and private subnet for each availability zone within a region. Each private subnet requires a NAT Gateway, and each NAT gateway requires a separate elastic IP. Review the AWS region map to determine how many availability zones are in each region. To take advantage of the default high availability, install the cluster in a region with at least three availability zones. To install a cluster in a region with more than five availability zones, you must increase the EIP limit.</p> <div><p>To use the <code>us-east-1</code> region, you must increase the EIP limit for your account.</p></div>
Virtual Private Clouds (VPCs)	5	5 VPCs per region	Each cluster creates its own VPC.
Elastic Load Balancing (ELB/NLB)	3	20 per region	By default, each cluster creates internal and external network load balancers for the master API server and a single Classic Load Balancer for the router. Deploying more Kubernetes <code>Service</code> objects with type <code>LoadBalancer</code> will create additional load balancers .
NAT Gateways	5	5 per availability zone	The cluster deploys one NAT gateway in each availability zone.

Component	Number of clusters available by default	Default AWS limit	Description
Elastic Network Interfaces (ENIs)	At least 12	350 per region	<p>The default installation creates 21 ENIs and an ENI for each availability zone in your region. For example, the <code>us-east-1</code> region contains six availability zones, so a cluster that is deployed in that zone uses 27 ENIs. Review the AWS region map to determine how many availability zones are in each region.</p> <p>Additional ENIs are created for additional machines and ELB load balancers that are created by cluster usage and deployed workloads.</p>
VPC Gateway	20	20 per account	Each cluster creates a single VPC Gateway for S3 access.
S3 buckets	99	100 buckets per account	Because the installation process creates a temporary bucket and the registry component in each cluster creates a bucket, you can create only 99 OpenShift Container Platform clusters per AWS account.
Security Groups	250	2,500 per account	Each cluster creates 10 distinct security groups.

Required AWS permissions for the IAM user



Your IAM user must have the permission `tag:GetResources` in the region `us-east-1` to delete the base cluster resources. As part of the AWS API requirement, the OpenShift Container Platform installation program performs various actions in this region.

When you attach the `AdministratorAccess` policy to the IAM user that you create in Amazon Web Services (AWS), you grant that user all of the required permissions. To deploy all components of an OpenShift Container Platform cluster, the IAM user requires the following permissions:

Required EC2 permissions for installation

- `ec2:AttachNetworkInterface`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CopyImage`
- `ec2:CreateNetworkInterface`
- `ec2:CreateSecurityGroup`
- `ec2:CreateTags`
- `ec2:CreateVolume`
- `ec2>DeleteSecurityGroup`
- `ec2>DeleteSnapshot`
- `ec2>DeleteTags`
- `ec2:DeregisterImage`
- `ec2:DescribeAccountAttributes`
- `ec2:DescribeAddresses`
- `ec2:DescribeAvailabilityZones`
- `ec2:DescribeDhcpOptions`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstanceCreditSpecifications`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypes`

- `ec2:DescribeInternetGateways`
- `ec2:DescribeKeyPairs`
- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribePrefixLists`
- `ec2:DescribePublicIpv4Pools` (only required if `publicIpv4Pool` is specified in `install-config.yaml`)
- `ec2:DescribeRegions`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroupRules`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeTags`
- `ec2:DescribeVolumes`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeVpcClassicLink`
- `ec2:DescribeVpcClassicLinkDnsSupport`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ec2:DisassociateAddress` (only required if `publicIpv4Pool` is specified in `install-config.yaml`)
- `ec2:GetEbsDefaultKmsKeyId`
- `ec2:ModifyInstanceAttribute`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:RevokeSecurityGroupEgress`

- `ec2:RevokeSecurityGroupIngress`
- `ec2:RunInstances`
- `ec2:TerminateInstances`

Required permissions for creating network resources during installation

- `ec2:AllocateAddress`
- `ec2:AssociateAddress`
- `ec2:AssociateDhcpOptions`
- `ec2:AssociateRouteTable`
- `ec2:AttachInternetGateway`
- `ec2:CreateDhcpOptions`
- `ec2:CreateInternetGateway`
- `ec2:CreateNatGateway`
- `ec2:CreateRoute`
- `ec2:CreateRouteTable`
- `ec2:CreateSubnet`
- `ec2:CreateVpc`
- `ec2:CreateVpcEndpoint`
- `ec2:ModifySubnetAttribute`
- `ec2:ModifyVpcAttribute`



If you use an existing Virtual Private Cloud (VPC), your account does not require these permissions for creating network resources.

Required Elastic Load Balancing permissions (ELB) for installation

- `elasticloadbalancing:AddTags`
- `elasticloadbalancing:ApplySecurityGroupsToLoadBalancer`
- `elasticloadbalancing:AttachLoadBalancerToSubnets`
- `elasticloadbalancing:ConfigureHealthCheck`

- `elasticloadbalancing:CreateListener`
- `elasticloadbalancing:CreateLoadBalancer`
- `elasticloadbalancing:CreateLoadBalancerListeners`
- `elasticloadbalancing:CreateTargetGroup`
- `elasticloadbalancing>DeleteLoadBalancer`
- `elasticloadbalancing:DeregisterInstancesFromLoadBalancer`
- `elasticloadbalancing:DeregisterTargets`
- `elasticloadbalancing:DescribeInstanceHealth`
- `elasticloadbalancing:DescribeListeners`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeTags`
- `elasticloadbalancing:DescribeTargetGroupAttributes`
- `elasticloadbalancing:DescribeTargetHealth`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`
- `elasticloadbalancing:ModifyTargetGroup`
- `elasticloadbalancing:ModifyTargetGroupAttributes`
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer`
- `elasticloadbalancing:RegisterTargets`
- `elasticloadbalancing:SetLoadBalancerPoliciesOfListener`
- `elasticloadbalancing:SetSecurityGroups`



OpenShift Container Platform uses both the ELB and ELBv2 API services to provision load balancers. The permission list shows permissions required by both services. A known issue exists in the AWS web console where both services use the same `elasticloadbalancing` action prefix but do not recognize the same actions. You can ignore the warnings about the service not recognizing certain `elasticloadbalancing` actions.

Required IAM permissions for installation

- `iam:AddRoleToInstanceProfile`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam>DeleteInstanceProfile`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:GetRolePolicy`
- `iam:GetUser`
- `iam:ListInstanceProfilesForRole`
- `iam:ListRoles`
- `iam:ListUsers`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `iam:RemoveRoleFromInstanceProfile`
- `iam:SimulatePrincipalPolicy`
- `iam:TagInstanceProfile`
- `iam:TagRole`



If you have not created a load balancer in your AWS account, the IAM user also requires the `iam:CreateServiceLinkedRole` permission.

Required Route 53 permissions for installation

- `route53:ChangeResourceRecordSets`
- `route53:ChangeTagsForResource`
- `route53:CreateHostedZone`
- `route53>DeleteHostedZone`
- `route53:GetChange`
- `route53:GetHostedZone`
- `route53:ListHostedZones`
- `route53:ListHostedZonesByName`
- `route53:ListResourceRecordSets`
- `route53:ListTagsForResource`
- `route53:UpdateHostedZoneComment`

Required Amazon Simple Storage Service (S3) permissions for installation

- `s3:CreateBucket`
- `s3>DeleteBucket`
- `s3:GetAccelerateConfiguration`
- `s3:GetBucketAcl`
- `s3:GetBucketCors`
- `s3:GetBucketLocation`
- `s3:GetBucketLogging`
- `s3:GetBucketObjectLockConfiguration`
- `s3:GetBucketPolicy`
- `s3:GetBucketRequestPayment`

- `s3:GetBucketTagging`
- `s3:GetBucketVersioning`
- `s3:GetBucketWebsite`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3:GetReplicationConfiguration`
- `s3:ListBucket`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketTagging`
- `s3:PutEncryptionConfiguration`

S3 permissions that cluster Operators require

- `s3:DeleteObject`
- `s3:GetObject`
- `s3:GetObjectAcl`
- `s3:GetObjectTagging`
- `s3:GetObjectVersion`
- `s3:PutObject`
- `s3:PutObjectAcl`
- `s3:PutObjectTagging`

Required permissions to delete base cluster resources

- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DeleteNetworkInterface`
- `ec2:DeletePlacementGroup`
- `ec2:DeleteVolume`
- `elasticloadbalancing:DeleteTargetGroup`

- `elasticloadbalancing:DescribeTargetGroups`
- `iam:DeleteAccessKey`
- `iam:DeleteUser`
- `iam:DeleteUserPolicy`
- `iam:ListAttachedRolePolicies`
- `iam:ListInstanceProfiles`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`
- `s3:DeleteObject`
- `s3:ListBucketVersions`
- `tag:GetResources`

Required permissions to delete network resources

- `ec2:DeleteDhcpOptions`
- `ec2:DeleteInternetGateway`
- `ec2:DeleteNatGateway`
- `ec2:DeleteRoute`
- `ec2:DeleteRouteTable`
- `ec2:DeleteSubnet`
- `ec2:DeleteVpc`
- `ec2:DeleteVpcEndpoints`
- `ec2:DetachInternetGateway`
- `ec2:DisassociateRouteTable`
- `ec2:ReleaseAddress`
- `ec2:ReplaceRouteTableAssociation`



If you use an existing VPC, your account does not require these permissions to delete network resources. Instead, your account only requires the `tag:UntagResources` permission to delete network resources.

Optional permissions for installing a cluster with a custom Key Management Service (KMS) key

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:Encrypt`
- `kms:GenerateDataKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:ListGrants`
- `kms:RevokeGrant`

Required permissions to delete a cluster with shared instance roles

- `iam:UntagRole`

Additional IAM and S3 permissions that are required to create manifests

- `iam:GetUserPolicy`
- `iam:ListAccessKeys`
- `iam:PutUserPolicy`
- `iam:TagUser`
- `s3:AbortMultipartUpload`
- `s3:GetBucketPublicAccessBlock`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutLifecycleConfiguration`



If you are managing your cloud provider credentials with mint mode, the IAM user also requires the `iam:CreateAccessKey` and `iam:CreateUser` permissions.

Optional permissions for instance and quota checks for installation

- `ec2:DescribeInstanceTypeOfferings`
- `servicequotas:ListAWSDefaultServiceQuotas`

Optional permissions for the cluster owner account when installing a cluster on a shared VPC

- `sts:AssumeRole`

Required permissions for enabling Bring your own public IPv4 addresses (BYOIP) feature for installation

- `ec2:DescribePublicIpv4Pools`
- `ec2:DisassociateAddress`

Creating an IAM user

Each Amazon Web Services (AWS) account contains a root user account that is based on the email address you used to create the account. This is a highly-privileged account, and it is recommended to use it for only initial account and billing configuration, creating an initial set of users, and securing the account.

Before you install OpenShift Container Platform, create a secondary IAM administrative user. As you complete the [Creating an IAM User in Your AWS Account](#) procedure in the AWS documentation, set the following options:

Procedure

- Specify the IAM user name and select `Programmatic access`.
- Attach the `AdministratorAccess` policy to ensure that the account has sufficient permission to create the cluster. This policy provides the cluster with the ability to grant credentials to each OpenShift Container Platform component. The cluster grants the components only the credentials that they require.



While it is possible to create a policy that grants the all of the required AWS permissions and attach it to the user, this is not the preferred option. The cluster will not have the ability to grant additional credentials to individual components, so the same credentials are used by all components.

- Optional: Add metadata to the user by attaching tags.
- Confirm that the user name that you specified is granted the `AdministratorAccess` policy.
- Record the access key ID and secret access key values. You must use these values when you configure your local machine to run the installation program.



You cannot use a temporary session token that you generated while using a multi-factor authentication device to authenticate to AWS when you deploy a cluster. The cluster continues to use your current AWS credentials to create AWS resources for the entire life of the cluster, so you must use key-based, long-term credentials.

IAM Policies and AWS authentication

By default, the installation program creates instance profiles for the bootstrap, control plane, and compute instances with the necessary permissions for the cluster to operate.

However, you can create your own IAM roles and specify them as part of the installation process. You might need to specify your own roles to deploy the cluster or to manage the cluster after installation. For example:

- Your organization's security policies require that you use a more restrictive set of permissions to install the cluster.
- After the installation, the cluster is configured with an Operator that requires access to additional services.

If you choose to specify your own IAM roles, you can take the following steps:

- Begin with the default policies and adapt as required. For more information, see "Default permissions for IAM instance profiles".
- Use the AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) to create a policy template that is based on the cluster's activity. For more information see, "Using AWS IAM Analyzer to create policy templates".

Default permissions for IAM instance profiles

By default, the installation program creates IAM instance profiles for the bootstrap, control plane and worker instances with the necessary permissions for the cluster to operate.

The following lists specify the default permissions for control plane and compute machines:

Default IAM role permissions for control plane instance profiles

- `ec2:AttachVolume`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateSecurityGroup`
- `ec2:CreateTags`
- `ec2:CreateVolume`
- `ec2>DeleteSecurityGroup`
- `ec2>DeleteVolume`
- `ec2:Describe*`
- `ec2:DetachVolume`
- `ec2:ModifyInstanceAttribute`
- `ec2:ModifyVolume`
- `ec2:RevokeSecurityGroupIngress`
- `elasticloadbalancing:AddTags`
- `elasticloadbalancing:AttachLoadBalancerToSubnets`
- `elasticloadbalancing:ApplySecurityGroupsToLoadBalancer`

- `elasticloadbalancing:CreateListener`
- `elasticloadbalancing:CreateLoadBalancer`
- `elasticloadbalancing:CreateLoadBalancerPolicy`
- `elasticloadbalancing:CreateLoadBalancerListeners`
- `elasticloadbalancing:CreateTargetGroup`
- `elasticloadbalancing:ConfigureHealthCheck`
- `elasticloadbalancing>DeleteListener`
- `elasticloadbalancing>DeleteLoadBalancer`
- `elasticloadbalancing>DeleteLoadBalancerListeners`
- `elasticloadbalancing>DeleteTargetGroup`
- `elasticloadbalancing:DeregisterInstancesFromLoadBalancer`
- `elasticloadbalancing:DeregisterTargets`
- `elasticloadbalancing:Describe*`
- `elasticloadbalancing:DetachLoadBalancerFromSubnets`
- `elasticloadbalancing:ModifyListener`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`
- `elasticloadbalancing:ModifyTargetGroup`
- `elasticloadbalancing:ModifyTargetGroupAttributes`
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer`
- `elasticloadbalancing:RegisterTargets`
- `elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer`
- `elasticloadbalancing:SetLoadBalancerPoliciesOfListener`
- `kms:DescribeKey`

Default IAM role permissions for compute instance profiles

- `ec2:DescribeInstances`
- `ec2:DescribeRegions`

Specifying an existing IAM role

Instead of allowing the installation program to create IAM instance profiles with the default permissions, you can use the `install-config.yaml` file to specify an existing IAM role for control plane and compute instances.

Prerequisites

- You have an existing `install-config.yaml` file.

Procedure

- Update `compute.platform.aws.iamRole` with an existing role for the compute machines.

Sample `install-config.yaml` file with an IAM role for compute instances

```
compute:
- hyperthreading: Enabled
  name: worker
  platform:
    aws:
      iamRole: ExampleRole
```

- Update `controlPlane.platform.aws.iamRole` with an existing role for the control plane machines.

Sample `install-config.yaml` file with an IAM role for control plane instances

```
controlPlane:
  hyperthreading: Enabled
  name: master
  platform:
    aws:
      iamRole: ExampleRole
```

- Save the file and reference it when installing the OpenShift Container Platform cluster.



To change or update an IAM account after the cluster has been installed, see [RHOC P 4 AWS cloud-credentials access key is expired](#) (Red Hat Knowledgebase).

Additional resources

- Deploying the cluster

Using AWS IAM Analyzer to create policy templates

The minimal set of permissions that the control plane and compute instance profiles require depends on how the cluster is configured for its daily operation.

One way to determine which permissions the cluster instances require is to use the AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) to create a policy template:

- A policy template contains the permissions the cluster has used over a specified period of time.
- You can then use the template to create policies with fine-grained permissions.

Procedure

The overall process could be:

- Ensure that CloudTrail is enabled. CloudTrail records all of the actions and events in your AWS account, including the API calls that are required to create a policy template. For more information, see the AWS documentation for [working with CloudTrail](#).
- Create an instance profile for control plane instances and an instance profile for compute instances. Be sure to assign each role a permissive policy, such as PowerUserAccess. For more information, see the AWS documentation for [creating instance profile roles](#).
- Install the cluster in a development environment and configure it as required. Be sure to deploy all of applications the cluster will host in a production environment.
- Test the cluster thoroughly. Testing the cluster ensures that all of the required API calls are logged.
- Use the IAM Access Analyzer to create a policy template for each instance profile. For more information, see the AWS documentation for [generating policies based on the CloudTrail logs](#).

- Create and add a fine-grained policy to each instance profile.
- Remove the permissive policy from each instance profile.
- Deploy a production cluster using the existing instance profiles with the new policies.



You can add [IAM Conditions](#) to your policy to make it more restrictive and compliant with your organization security requirements.

Supported AWS Marketplace regions

Installing an OpenShift Container Platform cluster using an AWS Marketplace image is available to customers who purchase the offer in North America.

While the offer must be purchased in North America, you can deploy the cluster to any of the following supported partitions:

- Public
- GovCloud



Deploying a OpenShift Container Platform cluster using an AWS Marketplace image is not supported for the AWS secret regions or China regions.

Supported AWS regions

You can deploy an OpenShift Container Platform cluster to the following regions.



Your IAM user must have the permission `tag:GetResources` in the region `us-east-1` to delete the base cluster resources. As part of the AWS API requirement, the OpenShift Container Platform installation program performs various actions in this region.

AWS public regions

The following AWS public regions are supported:

- af-south-1 (Cape Town)
- ap-east-1 (Hong Kong)
- ap-northeast-1 (Tokyo)
- ap-northeast-2 (Seoul)
- ap-northeast-3 (Osaka)
- ap-south-1 (Mumbai)
- ap-south-2 (Hyderabad)
- ap-southeast-1 (Singapore)
- ap-southeast-2 (Sydney)
- ap-southeast-3 (Jakarta)
- ap-southeast-4 (Melbourne)
- ca-central-1 (Central)
- ca-west-1 (Calgary)
- eu-central-1 (Frankfurt)
- eu-central-2 (Zurich)
- eu-north-1 (Stockholm)
- eu-south-1 (Milan)
- eu-south-2 (Spain)
- eu-west-1 (Ireland)
- eu-west-2 (London)
- eu-west-3 (Paris)
- il-central-1 (Tel Aviv)
- me-central-1 (UAE)

- `me-south-1` (Bahrain)
- `sa-east-1` (São Paulo)
- `us-east-1` (N. Virginia)
- `us-east-2` (Ohio)
- `us-west-1` (N. California)
- `us-west-2` (Oregon)

AWS GovCloud regions

The following AWS GovCloud regions are supported:

- `us-gov-west-1`
- `us-gov-east-1`

AWS SC2S and C2S secret regions

The following AWS secret regions are supported:

- `us-isob-east-1` Secret Commercial Cloud Services (SC2S)
- `us-iso-east-1` Commercial Cloud Services (C2S)

AWS China regions

The following AWS China regions are supported:

- `cn-north-1` (Beijing)
- `cn-northwest-1` (Ningxia)

Next steps

- Install an OpenShift Container Platform cluster:
 - [Quickly install a cluster](#) with default options on installer-provisioned infrastructure
 - [Install a cluster with cloud customizations on installer-provisioned infrastructure](#)

- Install a cluster with network customizations on installer-provisioned infrastructure
- Installing a cluster on user-provisioned infrastructure in AWS by using CloudFormation templates



Copyright © 2024 Red Hat, Inc.