

Cloudera DataFlow AWS Requirements

Date published: 2021-04-06

Date modified: 2024-01-09



Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

AWS requirements for DataFlow.....	4
DataFlow networking in AWS.....	5
Use your own VPC.....	6
Allow CDP to create a VPC.....	7
Limitations on AWS.....	8
AWS restricted policies.....	8
Create IAM roles and instance profile.....	9
Create the restricted policies and attach them to the CDP cross-account role.....	14
Using Customer Managed Keys with DataFlow.....	24
Define a new default KMS key for AWS account level EBS encryption.....	24
Define a new default KMS key for CDP environment level EBS encryption.....	26

AWS requirements for DataFlow

As the administrator for your AWS environment, ensure that the environment meets the requirements for CDP and DataFlow. Then set up your AWS cloud credential and register the environment.

Follow the steps to ensure that your AWS environment meets the CDP and DataFlow requirements:

Understand your AWS account requirements for CDP

- Review the *CDP AWS account requirements*. The link is in the *Related information* section below.
- Verify that your AWS account for CDP has the required resources.
- Verify that you have the permissions to manage these resources.

Understand the DataFlow requirements

- Verify that the following services are available in your environment for DataFlow to use:
 - Network – Amazon VPC
 - Compute – Amazon Elastic Kubernetes Service (EKS)
 - Load Balancing – Amazon ELB Classic Load Balancer
 - Persistent Instance Storage – Amazon Elastic Block Store (EBS)
 - Database – Amazon Relational Database Service (RDS)
- Determine your networking option:
 - Use your own VPC
 - Allow CDP to create a VPC

To understand each option, see: *DataFlow Networking*. The link is in the *Related information* section below.

- Regions:
 - Select a CDP-supported region that also includes the AWS Elastic Kubernetes Service (EKS).

For more information, see: *CDP Supported AWS regions* and the Region Table in *AWS Regional Services*. The links are in the *Related information* section below.

- Ports and outbound network access:
 - Review the port requirements for the CDP default security group. See: *CDP Management Console - Security groups*. The link is in the *Related information* section below.
 - Configure ports for NiFi to access your source and destination systems in the data flow.
 - If you are using a firewall or a security group setting to prevent egress from the workspace, you must ensure that the outbound destinations required by CDF are reachable. For more information, see *Outbound network access destinations for AWS*. The link is in the *Related information* section below.
 - If the egress is blocked to these URLs, then autoscaling fails to pull new images and the instances will have broken pods.

Follow the recommended and minimum required security group settings by AWS. For more information, see *Amazon EKS security group considerations*. The link is in the *Related information* section below.

Set up an AWS Cloud credential

Create a role-based AWS credential that allows CDP to authenticate with your AWS account and has authorization to provision AWS resources on your behalf. Role-based authentication uses an IAM role with an attached IAM policy that has the minimum permissions required to use CDP.

To set up an AWS Cloud credential, see *Creating a role based provisioning credential for AWS*. The link is in the *Related information* section below.

After you have created this IAM policy, register it in CDP as a cloud credential. Reference this credential when you register an AWS environment in CDP environment as described in the next step.

Register an AWS environment in CDP

A CDP user must have the PowerUser role in order to register an environment. An environment determines the specific cloud provider region and virtual network in which resources can be provisioned, and includes the credential that should be used to access the cloud provider account.

To register an AWS environment in CDP, see *CDP AWS Environments*. The link is in the *Related information* section below.

Related Concepts

[DataFlow networking in AWS](#)

Related Information

[CDP AWS account requirements](#)

[CDP Supported AWS regions](#)

[AWS Regional Services](#)

[CDP Management Console - Security groups](#)

[Amazon EKS security group considerations](#)

[Creating a role based provisioning credential for AWS](#)

[CDP AWS Environments](#)

[Outbound network access destinations for AWS](#)

DataFlow networking in AWS

DataFlow supports different networking options depending on how you have set up your VPC and subnets. If you want DataFlow to use specific subnets, make sure that you specify them when registering a CDP environment.

If you specified a mix of public and private subnets during environment registration, DataFlow by default will provision the Kubernetes nodes in the private subnets. For DataFlow to work, the private subnets require outbound internet access. This can be achieved by configuring NAT gateways in separate public subnets and making sure that outbound internet traffic is routed via the NAT gateway. The VPC you are using must have an Internet Gateway set up which ultimately provides internet access to the public subnets. Following this approach allows the DataFlow services running on Kubernetes nodes in your private network to connect to the internet while also preventing inbound connections from the internet.

You can configure DataFlow to either use a private or public load balancer to allow users to connect to flow deployments. Using a private load balancer is possible when your CDP environment contains at least two private subnets. When you are using a private load balancer, you need to ensure connectivity between the client network from where your users are initiating connections and the private subnets in your VPC. This is typically done by setting up VPN access between the private subnets in AWS and the corporate network.

If you want to allow users to connect to flow deployments from the internet you can use the public load balancer option. This option will provision public load balancers in public subnets allowing your users to connect to flow deployments without the need to set up VPN connectivity between the private subnets and your corporate network.



Important: Cloudera recommends that you either use a fully private deployment in private subnets with private load balancers or a mix of private subnets with a public load balancer. Cloudera does not recommend provisioning DataFlow in public subnets.

The image below represents a fully private deployment where Kubernetes nodes and load balancers are deployed in the private subnets.

Use your own VPC

If you choose to use your own VPC, verify that it meets the minimum requirements and review Cloudera's recommended setup.

VPCs can be created and managed from the *VPC console on AWS*. For instructions on how to create a new VPC on AWS, refer to *Create and configure your VPC* in the AWS documentation.

Verify that your VPC meets the following requirements and recommendations:

Minimum requirements

- DataFlow requires at least two subnets, each in a different Availability Zone (AZ). If you require a public endpoint for DataFlow, provision at least one public subnet.
- Ensure that the CIDR block for the subnets is sized appropriately for each DataFlow environment. You must have enough IPs to accommodate:
 - The maximum number of autoscaling compute instances.
 - A fixed overhead of 48 IP addresses for three instances for core DataFlow services.
- You must enable DNS for the VPC.

Cloudera's recommended setup

- Provision two subnets, each in a different Availability Zone (AZ).
 - If you do not require a public endpoint, use two private subnets.
 - If you require a public endpoint, use one private subnet and one public subnet.
- Private subnets should have routable IPs over your internal VPN. If IPs are not routable, private DataFlow endpoints must be accessed via a SOCKS. This is not recommended.
- Tag the VPC and the subnets as shared so that Kubernetes can find them. Also, for load balancers to be able to choose the subnets correctly, you must tag either the private or public subnets.

A tag in AWS consists of a key and a value.

- To tag private subnets, enter `kubernetes.io/role/internal-elb` for the key and `1` for the value.

▼ Tags - optional

Key	Value - optional	
<input type="text" value="kubernetes.io/role/internal-elb"/>	<input type="text" value="1"/>	<input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>		
You can add 48 more tags.		

- To tag public subnets, enter `kubernetes.io/role/elb` for the key and `1` for the value.

▼ Tags - optional

Key	Value - optional	
<input type="text" value="kubernetes.io/role/elb"/>	<input type="text" value="1"/>	<input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>		
You can add 48 more tags.		



Note: The load balancer must be on a public subnet for access to DataFlow. By default, if they are available, DataFlow will configure the EKS to run on private subnets.

Related Information

[VPC Console on AWS](#)

[Create and configure your VPC](#)

Allow CDP to create a VPC

You can choose to create a VPC through CDP.

If you choose to create a VPC through CDP, three subnets will be automatically created.

You will be asked to specify a valid CIDR in IPv4 range that will be used to define the range of private IPs for EC2 instances provisioned into these subnets.

For more information, see the AWS documentation *Amazon EKS - Cluster VPC Considerations* and *Creating a VPC for your Amazon EKS Cluster*. The links are in the *Related information* section below.

Related Information

[Amazon EKS - Cluster VPC Considerations](#)

[Creating a VPC for your Amazon EKS Cluster](#)

Limitations on AWS

Review the default AWS service limits and your current AWS account limits.

By default, AWS imposes certain default limits for AWS services for each user account. Make sure you review your account's current usage status and resource limits before you start provisioning additional resources for CDP and CDF.

For example, depending on your AWS account, you may only be allowed to provision a certain number of EC2 instances. Be sure to review your AWS service limits before you proceed.

For more information, see the AWS documentation: *AWS Service Limits* and *Amazon EC2 Resource Limits*.

DataFlow environments have the following resource limits on AWS:

- Certificate creation (for TLS) uses LetsEncrypt which is limited to 2000 certs/week. As such, a single tenant in CDP can create a maximum of 2000 flows per week.

Related Information

[AWS Service Limits](#)

[Amazon EC2 Resource Limits](#)

[ENI Max Pods](#)

AWS restricted policies

Customers with strict security policies beyond what the default Cloudera cross-account policy permits can enable DataFlow for a CDP environment with more restricted IAM policies. To do so, an administrator must attach the Compute Restricted IAM policy with the cross-account role associated with the CDP environment.

DataFlow uses AWS IAM write permissions to create/delete Roles and Instance Profiles. If due to security requirements you cannot provide IAM write permission in the role's policy, you can set up static pre-created roles and an instance profile. DataFlow makes use of these static pre-created roles and instance-profile while provisioning the cluster.



Note: DataFlow will only be able to use the pre-created Roles and Instance Profile only if the entitlement `LIFTIE_USE_PRECREATED_IAM_RESOURCES` for the tenant in use is set.

To enable DataFlow with restricted IAM policies, perform the following tasks:

1. Create the IAM Roles and Instance Profile pair.
2. Create the CDP cross-account role credential.

Create IAM roles and instance profile

Enable the *LIFTIE_USE_PRECREATED_IAM_RESOURCES* entitlement and then create the IAM roles and instance profile.

Before you begin

Confirm that the *LIFTIE_USE_PRECREATED_IAM_RESOURCES* entitlement is enabled for the tenant in consideration.

Procedure

1. Apply the following CloudFormation template to create the following:

- IAM role called cdp-eks-master-role
- IAM role and instance profile pair called cdp-liftie-instance-profile

Figure 1: CloudFormation Template (YAML)

```
AWSTemplateFormatVersion: 2010-09-09
Description: Creates Liftie IAM resources
Parameters:
  TelemetryLoggingEnabled:
    Description: Telemetry logging is enabled
    Type: String
  TelemetryLoggingBucket:
    Description: Telemetry logging bucket where Liftie logs will be stored.
    Type: String
  TelemetryKmsKeyARN:
    Description: KMS Key ARN For Telemetry logging bucket.
    Type: String
    Default: ""
  TelemetryLoggingRootDir:
    Description: Telemetry logging root directory inside telemetry logging bucket used for storing logs.
    Default: "cluster-logs"
    Type: String
Conditions:
  TelemetryLoggingEnabled:
    Fn::Equals:
      - {Ref: TelemetryLoggingEnabled}
      - true
  KmsKeyARNForTelemetryLoggingBucketIsEmpty: !Not [!Equals [!Ref TelemetryKmsKeyARN, ""]]
Resources:
  AWSServiceRoleForAmazonEKS:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - eks.amazonaws.com
            Action:
              - sts:AssumeRole
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/AmazonEKSServicePolicy
        - arn:aws:iam::aws:policy/AmazonEKSClusterPolicy
```

```

    RoleName: cdp-eks-master-role
NodeInstanceRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: 2012-10-17
      Statement:
        - Effect: Allow
          Principal:
            Service:
              - ec2.amazonaws.com
          Action:
            - sts:AssumeRole
    Path: "/"
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
      - arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
      - arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
    RoleName: cdp-liftie-instance-profile
  Policies:
    - PolicyName: ssm-required
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action:
              - ssm:GetParameters
            Resource:
              - "*"
    - PolicyName: cluster-autoscaler
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action:
              - autoscaling:DescribeAutoScalingGroups
              - autoscaling:DescribeAutoScalingInstances
              - autoscaling:DescribeTags
              - autoscaling:DescribeLaunchConfigurations
              - autoscaling:SetDesiredCapacity
              - autoscaling:TerminateInstanceInAutoScalingGroup
              - ec2:DescribeLaunchTemplateVersions
            Resource:
              - "*"
    - PolicyName: ebs-csi
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action:
              - ec2:CreateSnapshot
              - ec2:AttachVolume
              - ec2:DetachVolume
              - ec2:ModifyVolume
              - ec2:DescribeAvailabilityZones
              - ec2:DescribeInstances
              - ec2:DescribeSnapshots
              - ec2:DescribeTags
              - ec2:DescribeVolumes
              - ec2:DescribeVolumesModifications
            Resource: "*"
          - Effect: Allow
            Action:
              - ec2:CreateTags

```

```

    Resource:
      - "arn:aws:ec2:*:*:volume/*"
      - "arn:aws:ec2:*:*:snapshot/*"
    Condition:
      StringEquals:
        "ec2:CreateAction":
          - CreateVolume
          - CreateSnapshot
- Effect: Allow
  Action:
    - ec2:DeleteTags
  Resource:
    - "arn:aws:ec2:*:*:volume/*"
    - "arn:aws:ec2:*:*:snapshot/*"
- Effect: Allow
  Action:
    - ec2:CreateVolume
  Resource: "*"
  Condition:
    StringLike:
      "aws:RequestTag/ebs.csi.aws.com/cluster": "true"
- Effect: Allow
  Action:
    - ec2:CreateVolume
  Resource: "*"
  Condition:
    StringLike:
      "aws:RequestTag/CSIVolumeName": "*"
- Effect: Allow
  Action:
    - ec2:CreateVolume
  Resource: "*"
  Condition:
    StringLike:
      "aws:RequestTag/kubernetes.io/cluster/*": "owned"
- Effect: Allow
  Action:
    - ec2>DeleteVolume
  Resource: "*"
  Condition:
    StringLike:
      "ec2:ResourceTag/ebs.csi.aws.com/cluster": "true"
- Effect: Allow
  Action:
    - ec2>DeleteVolume
  Resource: "*"
  Condition:
    StringLike:
      "ec2:ResourceTag/CSIVolumeName": "*"
- Effect: Allow
  Action:
    - ec2>DeleteVolume
  Resource: "*"
  Condition:
    StringLike:
      "ec2:ResourceTag/kubernetes.io/created-for/pvc/name":
" * "
- Effect: Allow
  Action:
    - ec2>DeleteSnapshot
  Resource: "*"
  Condition:
    StringLike:
      "ec2:ResourceTag/CSIVolumeSnapshotName": "*"

```

```

- Effect: Allow
  Action:
    - ec2:DeleteSnapshot
  Resource: "*"
  Condition:
    StringLike:
      "ec2:ResourceTag/ebs.csi.aws.com/cluster": "true"
- PolicyName: efs-csi
  PolicyDocument:
    Version: 2012-10-17
    Statement:
      - Effect: Allow
        Action:
          - elasticfilesystem:DescribeAccessPoints
          - elasticfilesystem:DescribeFileSystems
          - elasticfilesystem:DescribeMountTargets
        Resource: "*"
      - Effect: Allow
        Action:
          - elasticfilesystem:CreateAccessPoint
        Resource: "*"
        Condition:
          StringLike:
            "aws:RequestTag/efs.csi.aws.com/cluster": "true"
      - Effect: Allow
        Action:
          - elasticfilesystem:DeleteAccessPoint
        Resource: "*"
        Condition:
          StringEquals:
            "aws:ResourceTag/efs.csi.aws.com/cluster": "true"
- !If
- TelemetryLoggingEnabled
- PolicyName: telemetry-s3-list-bucket
  PolicyDocument:
    Version: 2012-10-17
    Statement:
      - Effect: Allow
        Action:
          - s3:ListBucket
        Resource:
          - !Sub 'arn:aws:s3:::${TelemetryLoggingBucket}'
          - !Sub 'arn:aws:s3:::${TelemetryLoggingBucket}/${TelemetryLoggingRootDir}/*'
      - !Ref 'AWS::NoValue'
- !If
- TelemetryLoggingEnabled
- PolicyName: telemetry-s3-read-write
  PolicyDocument:
    Version: 2012-10-17
    Statement:
      - Effect: Allow
        Action:
          - s3:*Object
          - s3:AbortMultipartUpload
          - s3:GetBucketAcl
        Resource:
          - !Sub 'arn:aws:s3:::${TelemetryLoggingBucket}'
          - !Sub 'arn:aws:s3:::${TelemetryLoggingBucket}/${TelemetryLoggingRootDir}/*'
      - !Ref 'AWS::NoValue'
- !If
- KMSKeyARNForTelemetryLoggingBucketIsEmpty
- PolicyName: s3-kms-read-write-policy

```

```

PolicyDocument:
  Version: 2012-10-17
  Statement:
    - Effect: Allow
      Action:
        - kms:Decrypt
        - kms:GenerateDataKey
      Resource:
        - !Sub ${TelemetryKmsKeyARN}
    - !Ref 'AWS::NoValue'
  - PolicyName: calico-cni
PolicyDocument:
  Version: 2012-10-17
  Statement:
    - Effect: Allow
      Action:
        - ec2:ModifyInstanceAttribute
      Resource:
        - "*"
NodeInstanceProfile:
  Type: AWS::IAM::InstanceProfile
  Properties:
    Path: /
    InstanceProfileName: cdp-liftie-instance-profile
    Roles:
      - !Ref NodeInstanceRole

```

2. In the AWS console Cloudformation wizard, provide values for the following properties:

- Stack Name: Provide an appropriate name. Example: compute-precreated-roles-and-instanceprofile)
- TelemetryLoggingBucket: Name of the log bucket. Example: compute-logging-bucket
- TelemetryLoggingEnabled: Set it to true.
- TelemetryLoggingRootDir: Verify that it is set to the default value cluster-logs.
- TelemetryKMSKeyARN: If the telemetry bucket is encrypted, specify the KMS Key ARN. The default value is null.

CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Specify stack details

Stack name

Stack name

compute-precreated-roles-and-instanceprofile

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

TelemetryLoggingBucket
Telemetry logging bucket where Liftie logs will be stored.

compute-logging-bucket

TelemetryLoggingEnabled
Telemetry logging is enabled

true

TelemetryLoggingRootDir
Telemetry logging root directory inside telemetry logging bucket used for storing logs.

cluster-logs

Cancel Previous Next

- On the last page in the wizard process, click the I acknowledge... checkbox to allow creation of IAM resources with special names.

► Quick-create link

Capabilities

ⓘ The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

☐ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Cancel Previous Create change set **Create stack**

- Click Create stack.

Results

On the CloudFormation **Resources** tab, you find the precreated role and instance profile.

compute-precreated-roles-and-instanceprofile Delete Update Stack actions ▼ Create stack ▼

Stack info Events **Resources** Outputs Parameters Template Change sets

Resources (3)

Search resources

Logical ID ▲	Physical ID ▼	Type ▼	Status ▼	Status reason ▼
AWSServiceRoleForAmazonEKS	cdp-eks-master-role ↗	AWS::IAM::Role	✓ CREATE_COMPLETE	-
NodeInstanceProfile	cdp-liftie-instance-profile	AWS::IAM::InstanceProfile	✓ CREATE_COMPLETE	-
NodeInstanceRole	cdp-liftie-instance-profile ↗	AWS::IAM::Role	✓ CREATE_COMPLETE	-

What to do next

Update the environment role to use the restricted role and policy.

Create the restricted policies and attach them to the CDP cross-account role

Update the environment role to use the Data Hub and Compute restricted policies. You can do this during the environment-creation process or before you enable the environment.

About this task

To enable the DataFlow experience after the environment has been created, an Administrator needs to attach the Compute Restricted IAM policy and the Data Hub restricted policy with the CDP cross-account role associated with the environment.

To use CDF with the most restrictive options available, you need to create a custom Customer Managed Key (CMK) defining it on Environment level. The Compute Restricted IAM policy provided here requires the existence of such a

key. If you want to use CDF with less restrictive options, you can modify the policy in a way that allows Cloudera to create and manage the key for you.

Procedure

1. Go to the **Environments** page.

Environments / Environments

Enable Permission Verification ?

Create Cross-account Access Policy

Copy the following JSON to create an [AWS IAM policy](#)

Default

Minimal

The default role allows for the default set of operations including everything that the minimal role allows for.

```
{  "Statement": [    {      "Sid": "CloudFormationFull",      "Action": [        "cloudformation:*"      ],      "Effect": "Allow",      "Resource": [        "*"      ]    }  ],  "Version": "2012-10-17"}
```

Create Cross-account Access Role

Use Service Manager Account ID and External ID to create an [AWS IAM role](#)

Service Manager Account ID*

External ID*

Cross-account Role ARN *

Enter Cross-account Role ARN

Create Credential

> SHOW CLI COMMAND

2. In the Create Cross-account Access Policy field, attach the Compute Restricted IAM policy:

Replace the following placeholders in the JSON file:

- *[YOUR-ACCOUNT-ID]* with your account ID in use.
- *[YOUR-IAM-ROLE-NAME]* with the IAM restricted role associated with this policy.
- *[YOUR-SUBNET-ARN-*]* supplied during the CDP Environment(s) creation.



Note: Provide all the subnets present in all the CDP Environment(s) that you intend to use it for the experience. If at any point a new CDP Environment is created or an existing one is updated for subnets, provide it here.

- *[YOUR-IDBROKER-ROLE-NAME]* with the ID Broker Role name in use.
- *[YOUR-LOG-ROLE-NAME]* with the Log Role name in use.
- *[YOUR-KMS-CUSTOMER-MANAGED-KEY-ARN]* with KMS key ARN.

```
{
  "Version": "2012-10-17",
  "Id": "ComputePolicy_v8",
  "Statement": [
    {
```

```

    "Sid": "SimulatePrincipalPolicy",
    "Effect": "Allow",
    "Action": [
        "iam:SimulatePrincipalPolicy"
    ],
    "Resource": [
        "arn:aws:iam::[YOUR-ACCOUNT-ID]:role/[YOUR-IAM-ROLE-NAME]"
    ]
},
{
    "Sid": "RestrictedPermissionsViaClouderaRequestTag",
    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation:CreateChangeSet",
        "ec2:createTags",
        "eks:TagResource"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/Cloudera-Resource-Name": [
                "crn:cdp:*"
            ]
        }
    }
},
{
    "Sid": "RestrictedPermissionsViaClouderaResourceTag",
    "Effect": "Allow",
    "Action": [
        "autoscaling:DetachInstances",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling>DeleteTags",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/Cloudera-Resource-Name": [
                "crn:cdp:*"
            ]
        }
    }
},
{
    "Sid": "RestrictedPermissionsViaCloudFormation",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateSecurityGroup",
        "ec2>DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:CreateLaunchTemplate",
        "ec2>DeleteLaunchTemplate",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling>DeleteAutoScalingGroup",

```



```

        "autoscaling:CreateOrUpdateTags",
        "autoscaling:CreateLaunchConfiguration",
        "eks:CreateCluster",
        "eks>DeleteCluster"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": [
                "cloudformation.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "RestrictedEC2PermissionsViaClouderaResourceTag",
    "Effect": "Allow",
    "Action": [
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "ForAnyValue:StringLike": {
            "ec2:ResourceTag/Cloudera-Resource-Name": [
                "crn:cdp:*"
            ]
        }
    }
},
{
    "Sid": "RestrictedIamPermissionsToClouderaResources",
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": [
        "arn:aws:iam::[YOUR-ACCOUNT-ID]:role/[YOUR-IDBROKER-ROLE-NAME]",
        "arn:aws:iam::[YOUR-ACCOUNT-ID]:role/[YOUR-LOG-ROLE-NAME]",
        "arn:aws:iam::[YOUR-ACCOUNT-ID]:role/liftie-*-eks-service-role",
        "arn:aws:iam::[YOUR-ACCOUNT-ID]:role/liftie-*-eks-worker-nodes",
        "arn:aws:iam::[YOUR-ACCOUNT-ID]:role/cdp-eks-master-role",
        "arn:aws:iam::[YOUR-ACCOUNT-ID]:role/cdp-liftie-instance-profile"
    ]
},
{
    "Sid": "RestrictedKMSPermissionsUsingCustomerProvidedKey",
    "Effect": "Allow",
    "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*"
    ],
    "Resource": [
        "[YOUR-KMS-CUSTOMER-MANAGED-KEY-ARN]"
    ]
},

```

```

{
  "Sid": "AllowCreateDeleteTagsForSubnets",
  "Effect": "Allow",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "arn:aws:ec2:[YOUR-SUBNET-REGION]:[YOUR-ACCOUNT-ID]:subnet/*"
  ]
},
{
  "Sid": "OtherPermissionsViaCloudFormation",
  "Effect": "Allow",
  "Action": [
    "autoscaling:DescribeScheduledActions",
    "autoscaling:DescribeTags",
    "autoscaling:DescribeAutoScalingInstances",
    "autoscaling:DescribeLaunchConfigurations",
    "autoscaling:DeleteLaunchConfiguration",
    "autoscaling:DescribeScalingActivities",
    "dynamodb:DescribeTable",
    "ec2:DeletePlacementGroup",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeImages",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstances",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVolumes"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
        "cloudformation.amazonaws.com"
      ]
    }
  }
},
{
  "Sid": "OtherPermissionsViaClouderaResourceTag",
  "Effect": "Allow",
  "Action": [
    "cloudformation:DescribeChangeSet",
    "cloudformation:DeleteChangeSet",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:CancelUpdateStack",
    "cloudformation:ContinueUpdateRollback",
    "cloudformation:ListStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStackResource",
    "cloudformation:DescribeStackResources",
    "cloudwatch:deleteAlarms",
    "cloudwatch:putMetricAlarm",
    "logs:DescribeLogStreams",
    "logs:FilterLogEvents",

```

```

        "ec2:AttachVolume",
        "ec2:CreateNetworkInterface",
        "ec2:CreateVolume",
        "ec2>DeleteVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RunInstances",
        "eks:ListUpdates",
        "eks:UpdateClusterConfig",
        "eks:UpdateClusterVersion",
        "eks:DescribeUpdate",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRoleTags",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:TagRole",
        "iam:UntagRole"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/Cloudera-Resource-Name": [
                "crn:cdp:*"
            ]
        }
    }
},
{
    "Sid": "OtherPermissions",
    "Effect": "Allow",
    "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreatePlacementGroup",
        "ec2>DeleteKeyPair",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:ImportKeyPair",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "eks:DescribeCluster",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetInstanceProfile"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowSsmParams",
    "Effect": "Allow",
    "Action": [
        "ssm:DescribeParameters",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParameterHistory",
        "ssm:GetParametersByPath"
    ]
}

```

```

    ],
    "Resource": [
        "arn:aws:ssm:*:*:parameter/aws/service/eks/optimized-ami/*"
    ]
},
{
    "Sid": "CfDeny",
    "Effect": "Deny",
    "Action": [
        "cloudformation:*"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "ForAnyValue:StringLike": {
            "cloudformation:ImportResourceTypes": [
                "*"
            ]
        }
    }
},
{
    "Sid": "ForAutoscalingLinkedRole",
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": [
        "arn:aws:iam::[YOUR-ACCOUNT-ID]:role/aws-service-role/autoscaling-plans.amazonaws.com/AWSServiceRoleForAutoScalingPlans_EC2AutoScaling"
    ],
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "autoscaling-plans.amazonaws.com"
        }
    }
},
{
    "Sid": "ForEksLinkedRole",
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": [
        "arn:aws:iam::[YOUR-ACCOUNT-ID]:role/aws-service-role/eks.amazonaws.com/AWSServiceRoleForEKS"
    ],
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "eks.amazonaws.com"
        }
    }
}
]
}

```

3. Depending on whether you created a custom Customer Managed Key (CMK) to be used for EBS encryption or you want Cloudera to generate and manage the CMK for you, select one of the following options:
 - Provide own CMK - if you want to use your own custom CMK
 - Let CDP generate CMK - if you want to allow Cloudera to generate and manage your CMK

For Provide own CMK

- a. If you have not already created it, create a custom CMK. Verify that the policy (this is different from the IAM policy) for CMK at KMS has the required additional permissions blocks defined.

For more information, see [Using CMKs with DataFlow](#).

- b. Provide the KMS CMK for volume encryption in the policy section with Sid: RestrictedKMSPermissionsUsingCustomerProvidedKey.

For Let CDP generate CMK

Replace the RestrictedKMSPermissionsUsingCustomerProvidedKey policy section with the following:

```
{
  "Sid": "AllCreateAndManageKMS",
  "Effect": "Allow",
  "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms:Delete*",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
}
```

4. In the Create Cross-account Access Role section, associate the cross-account access role with the Compute Restricted IAM policy.
5. Click Create Credential.
6. Repeat the steps to add the Data Hub restricted policy.

Copy the following Data Hub restricted policy in the Create Cross-account Access Policy field:

Replace the following placeholders in the JSON file:

- `[YOUR-ACCOUNT-ID]` with your account ID in use.
- `[YOUR-IDBROKER-ROLE-NAME]` with your IDBroker role name.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags",
        "ec2:AssociateAddress",
        "ec2:StartInstances",
        "ec2:StopInstances",

```

```

        "ec2:AttachVolume",
        "ec2:DescribeAddresses",
        "ec2:TerminateInstances",
        "ec2>DeleteSecurityGroup"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/Cloudera-Resource-Name": [
                "crn:cdp:*"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "cloudformation:DeleteStack",
        "autoscaling:SuspendProcesses",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:ResumeProcesses",
        "autoscaling:DetachInstances",
        "autoscaling>DeleteAutoScalingGroup",
        "rds:StopDBInstance",
        "rds:StartDBInstance"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/Cloudera-Resource-Name": [
                "crn:cdp:*"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation:GetTemplate",
        "ec2:CreateTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringLike": {
            "aws:RequestTag/Cloudera-Resource-Name": [
                "crn:cdp:*"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2>DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteKeyPair",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2>DeleteLaunchTemplate",
        "ec2:DescribeVolumes",

```

```
"ec2:CreateVolume",
"ec2:DescribeInstances",
"ec2:DescribeRegions",
"ec2:DescribeInstanceTypeOfferings",
"ec2:DescribeInstanceTypes",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcs",
"ec2:DescribeInternetGateways",
"ec2:DescribeVpcEndpoints",
"ec2:describeAddresses",
"ec2:DescribeNatGateways",
"ec2:DescribeVpcEndpointServices",
"ec2:ModifySubnetAttribute",
"ec2:ModifyVpcAttribute",
"ec2:CreatePlacementGroup",
"ec2:DescribePlacementGroups",
"ec2:ImportKeyPair",
"ec2:DescribeLaunchTemplates",
"ec2:CreateLaunchTemplate",
"ec2:RunInstances",
"ec2:DescribeAccountAttributes",
"sts:DecodeAuthorizationMessage",
"cloudformation:DescribeStacks",
"dynamodb:DeleteTable",
"dynamodb:DescribeTable",
"iam:ListInstanceProfiles",
"iam:ListRoles",
"dynamodb:ListTables",
"autoscaling:DescribeAutoScalingGroups",
"autoscaling:DescribeScalingActivities",
"autoscaling:CreateAutoScalingGroup",
"autoscaling:TerminateInstanceInAutoScalingGroup",
"cloudwatch:DeleteAlarms",
"cloudwatch:PutMetricAlarm",
"cloudwatch:DescribeAlarms",
"elasticloadbalancing:CreateLoadBalancer",
"elasticloadbalancing:CreateTargetGroup",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:AddTags",
"elasticloadbalancing:RegisterTargets",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:CreateListener",
"elasticloadbalancing:DeleteListener",
"elasticloadbalancing:DeleteTargetGroup",
"elasticloadbalancing:DeleteLoadBalancer",
"elasticloadbalancing:DeregisterTargets",
"s3:GetBucketLocation",
"cloudformation:DescribeStackEvents",
"cloudformation:DescribeStackResources",
"cloudformation:DescribeStackResource",
"cloudformation:ListStackResources",
"cloudformation:UpdateStack",
"cloudformation:GetTemplate",
"iam:GetInstanceProfile",
"iam:SimulatePrincipalPolicy",
"iam:GetRole",
"rds:AddTagsToResource",
"rds:CreateDBInstance",
"rds:CreateDBSubnetGroup",
```

```

        "rds:DeleteDBInstance",
        "rds:DeleteDBSubnetGroup",
        "rds:ListTagsForResource",
        "rds:RemoveTagsFromResource",
        "rds:CreateDBParameterGroup",
        "rds:DeleteDBParameterGroup",
        "rds:DescribeEngineDefaultParameters",
        "rds:ModifyDBParameterGroup",
        "rds:DescribeDBParameters",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeDBInstances",
        "rds:ModifyDBInstance",
        "rds:DescribeCertificates",
        "kms:ListKeys",
        "kms:ListAliases",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateLaunchTemplateVersion"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": [
      "arn:aws:iam::[YOUR-ACCOUNT-ID]:role/[YOUR-IDBROKER-ROLE-NAME]"
    ]
  },
  {
    "Sid": "IdentityAccessManagementLimited",
    "Action": [
      "iam:CreateServiceLinkedRole"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:iam::*:role/aws-service-role/*"
    ]
  }
]
}

```

Using Customer Managed Keys with DataFlow

By default, DataFlow uses your account level KMS key for EBS storage encryption. You can optionally secure your data with a custom KMS key.

You have two options to implement Customer Managed Keys (CMKs):

- define a new default KMS key for EBS encryption on AWS account level
- define a key on CDF environment level

Define a new default KMS key for AWS account level EBS encryption

When you define a new account level default key in AWS, you need to add policies to your key definition that allow for storage provisioning and fulfilling scaling requests.

About this task



Important: Defining a new default key affects all EBS storage encryption within your account.

Procedure

1. Create a custom encryption key on the AWS Management Console.

The key policy section of the new key must contain additional permissions. Add the three required permission blocks in the example below.

Replace `[***YOUR ACCOUNT ID***]` and `[***YOUR ACCOUNT REGION***]` with your AWS account ID and with the AWS region where you want to deploy CDF, respectively.

```
{
  "Sid": "AllowAutoscalingServiceLinkedRoleForAttachmentOfPer
sistentResources",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::[***YOUR ACCOUNT ID***]:role/aws-se
rvice-role/autoscaling.amazonaws.com/AWSServiceRoleForAutoScaling"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:GrantIsForAWSResource": "true"
    }
  }
},
{
  "Sid": "AllowAutoscalingServiceLinkedRoleUseOfTheCMK",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::[***YOUR ACCOUNT ID***]:role/aws-se
rvice-role/autoscaling.amazonaws.com/AWSServiceRoleForAutoScaling"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow EKS access to EBS.",
  "Effect": "Allow",
  "Principal": {
    "AWS": "*"
  },
  "Action": [
    "kms:CreateGrant",
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
```

```

        "StringEquals": {
            "kms:CallerAccount": "[***YOUR ACCOUNT ID***]",
            "kms:viaService": "ec2.[***YOUR ACCOUNT REGION***].amazonaws.com"
        }
    }
}

```



Important: If you fail to add these permissions, you will encounter failures when enabling DataFlow since it will be unable to provision the necessary encrypted storage using the custom key.

2. Set the newly created key as the default KMS key for EBS encryption.
For more information, see [Default KMS key for EBS encryption](#).
3. If you are also using restricted IAM policies with CDP, make sure you provide the KMS CMK for volume encryption when you [Create the restricted policies and attach them to the CDP cross-account role](#) on page 14.

Define a new default KMS key for CDP environment level EBS encryption

When you define a custom KMS key at the CDP environment level, you need to add policies to your key definition that allow for storage provisioning and fulfilling scaling requests.

Procedure

1. Create a custom encryption key on the AWS Management Console.

The key policy section of the new key must contain additional permissions. Add the three required permission blocks in the example below.

Replace `[***YOUR ACCOUNT ID***]` and `[***YOUR ACCOUNT REGION***]` with your AWS account ID and with the AWS region where you want to deploy CDF, respectively.

```

{
    "Sid": "AllowAutoscalingServiceLinkedRoleForAttachmentOfPersistentResources",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::[***YOUR ACCOUNT ID***]:role/aws-service-role/autoscaling.amazonaws.com/AWSServiceRoleForAutoScaling"
    },
    "Action": "kms:CreateGrant",
    "Resource": "*",
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": "true"
        }
    }
},
{
    "Sid": "AllowAutoscalingServiceLinkedRoleUseOfTheCMK",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::[***YOUR ACCOUNT ID***]:role/aws-service-role/autoscaling.amazonaws.com/AWSServiceRoleForAutoScaling"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ]
},

```

```

    "Resource": "*"
  },
  {
    "Sid": "Allow EKS access to EBS.",
    "Effect": "Allow",
    "Principal": {
      "AWS": "*"
    },
    "Action": [
      "kms:CreateGrant",
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:CallerAccount": "[***YOUR ACCOUNT ID***]",
        "kms:viaService": "ec2.[***YOUR ACCOUNT REGION***].amazonaws.com"
      }
    }
  }
}

```



Important: If you fail to add these permissions, you will encounter failures when enabling DataFlow since it will be unable to provision the necessary encrypted storage using the custom key.

- When registering your CDP environment, follow these steps on the Region, Networking and Security page to assign the custom key:

Customer Managed Encryption Keys

The provided encryption key will be used to encrypt attached volumes and external DBs. Please note that this key will not be used to encrypt cloud storage.

Enable Customer-Managed Keys

Select Encryption Key*

Please select an Encryption Key

- Under Customer-Managed Keys, click Enable Customer-Managed Keys.
- Select the CMK you want to enable for this environment from the Select Encryption Key drop-down list.

For more information on registering a CDP environment, see [Register an AWS environment from CDP UI](#).

- If you are also using restricted IAM policies with CDP, make sure you provide the KMS CMK for volume encryption when you [Create the restricted policies and attach them to the CDP cross-account role](#) on page 14.