Kubernetes clusters documentation

Kubernetes clusters

NetApp
June 02, 2022

This PDF was generated from https://docs.netapp.com/us-en/cloud-manager-kubernetes/index.html on June 02, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Kubernetes clusters documentation . . . 1
What's new with Kubernetes in Cloud Manager . . . 2
4 May 2022 . . . 2
4 April 2022 . . . 2
27 February 2022 . . . 2
11 January 2022 . . . 2
28 November 2021 . . . 3
Get started . . . 4
Kubernetes data management in Cloud Manager . . . 4
Get started with Kubernetes clusters . . . 4
Requirements . . . 6
Requirements for Kubernetes clusters in AWS . . . 6
Requirements for Kubernetes clusters in Azure . . . 15
Requirements for Kubernetes clusters in Google Cloud . . . 22
Add Kubernetes clusters . . . 29
Add an Amazon Kubernetes cluster to Cloud Manager . . . 29
Add an Azure Kubernetes cluster to Cloud Manager . . . 31
Add a Google Cloud Kubernetes cluster to Cloud Manager . . . 34
Manage Kubernetes clusters . . . 38
Features . . . 38
Install Astra Trident . . . 38
Manage storage classes . . . 39
View persistent volumes . . . 43
Remove Kubernetes clusters from the workspace . . . 44
Use NetApp cloud data services with Kubernetes clusters . . . 44
Knowledge and support . . . 46
Register for support . . . 46
Get help . . . 47
Legal notices . . . 49
Copyright . . . 49
Trademarks . . . 49
Patents . . . 49
Privacy policy . . . 49
Open source . . . 49

Kubernetes clusters documentation

What's new with Kubernetes in Cloud Manager

Learn what's new in Kubernetes in Cloud Manager.

4 May 2022

Drag and drop to add storage class

You can now drag your Kubernetes cluster and drop it onto the Cloud Volumes ONTAP working environment to add a storage class directly from the Canvas.

Add storage class

4 April 2022

Manage Kubernetes clusters using the Cloud Manager resource page

Kubernetes cluster management now has enhanced integration directly from the cluster working environment. A new Quick start gets you up and running quickly.

You can now take the following actions from the cluster resource page.

- Install Astra Trident
- Add storage classes
- View persistent volumes
- Remove clusters
- Enable data services

27 February 2022

Support for Kubernetes clusters in Google Cloud

You can now add and manage managed Google Kubernetes Engine (GKE) clusters and self-managed Kubernetes clusters in Google Cloud using Cloud Manager.

Learn how to get started with Kubernetes clusters in Google Cloud.

11 January 2022

Support for Kubernetes clusters in Azure

You can now add and manage managed Azure Kubernetes clusters (AKS) and self-managed Kubernetes clusters in Azure using Cloud Manager.

Getting started with Kubernetes clusters in Azure

28 November 2021

Support for Kubernetes clusters in AWS

You can now add your managed-Kubernetes clusters to Cloud Manager's Canvas for advanced data management.

- Discover Amazon EKS clusters
- Back up persistent volumes using Cloud Backup

Learn more about Kubernetes support.

The existing Kubernetes service (available through the **K8s** tab) has been deprecated and will be removed in a future release.

Get started

Kubernetes data management in Cloud Manager

Astra Trident is a fully-supported open source project maintained by NetApp. Astra Trident integrates natively with Kubernetes and its Persistent Volume framework to seamlessly provision and manage volumes from systems running any combination of NetApp storage platforms. Learn more about Trident.

Features

You can directly manage your Kubernetes clusters using Cloud Manager.

- Install Astra Trident.
- Add and manage clusters as part of your hybrid cloud infrastructure.
- Add and manage storage classes and connect them to Working Environments.
- Back up persistent volumes using Cloud Backup Service.

Supported Kubernetes deployments

Cloud Manager supports managed-Kubernetes clusters running in:

- Amazon Elastic Kubernetes Service (Amazon EKS)
- Microsoft Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)

Supported Astra Trident deployments

One of the four most recent versions of Astra Trident is required. You can install Astra Trident directly from Cloud Manager. You should review the prerequisites prior to installation.

To upgrade Astra Trident, upgrade with the operator.

Supported backend storage

NetApp's Astra Trident must be installed on each Kubernetes cluster and Cloud Volumes ONTAP must be configured as backend storage for the clusters.

Cost

There are no charges to *discover* your Kubernetes clusters in Cloud Manager, but you will be charged when you back up persistent volumes using Cloud Backup Service.

Get started with Kubernetes clusters

Add Kubernetes clusters to Cloud Manager for advanced data management in a few quick steps.

Quick start

Get started quickly by following these steps.

Review prerequisites

Ensure your environment meets the prerequisites for your cluster type.

Requirements for Kubernetes clusters in AWS

Requirements for Kubernetes clusters in Azure

Requirements for Kubernetes clusters in Google Cloud

Add your Kubernetes clusters to Cloud Manager

You can add Kubernetes clusters and connect them to a Working Environment using Cloud Manager.

Add an Amazon Kubernetes cluster

Add an Azure Kubernetes cluster

Add a Google Cloud Kubernetes cluster

Start provisioning Persistent Volumes

Request and manage Persistent Volumes using native Kubernetes interfaces and constructs. Cloud Manager creates NFS and iSCSI storage classes that you can use when provisioning Persistent Volumes.

Learn more about provisioning your first volume with Astra Trident.

Manage your clusters using Cloud Manager

After adding Kubernetes clusters to Cloud Manager, you can manage the clusters from the Cloud Manager resource page.

Learn how to manage Kubernetes clusters.

Requirements

Requirements for Kubernetes clusters in AWS

You can add managed Amazon Elastic Kubernetes Service (EKS) clusters or self-managed Kubernetes clusters on AWS to Cloud Manager. Before you can add the clusters to Cloud Manager, you need to ensure that the following requirements are met.

This topic uses *Kubernetes cluster* where configuration is the same for EKS and self-managed Kubernetes clusters. The cluster type is specified where configuration differs.

Requirements

Astra Trident

One of the four most recent versions of Astra Trident is required. You can install Astra Trident directly from Cloud Manager. You should review the prerequisites prior to installing Astra Trident.

To upgrade Astra Trident, upgrade with the operator.

Cloud Volumes ONTAP

Cloud Volumes ONTAP for AWS must be set up as backend storage for the cluster. Go to the Astra Trident docs for configuration steps.

Cloud Manager Connector

A Connector must be running in AWS with the required permissions. Learn more below.

Network connectivity

Network connectivity is required between the Kubernetes cluster and the Connector and between the Kubernetes cluster and Cloud Volumes ONTAP. Learn more below.

RBAC authorization

The Cloud Manager Connector role must be authorized on each Kubernetes cluster. Learn more below.

Prepare a Connector

A Cloud Manager Connector is required in AWS to discover and manage Kubernetes clusters. You'll need to create a new Connector or use an existing Connector that has the required permissions.

Create a new Connector

Follow the steps in one of the links below.

- Create a Connector from Cloud Manager (recommended)
- Create a Connector from the AWS Marketplace
- Install the Connector on an existing Linux host in AWS

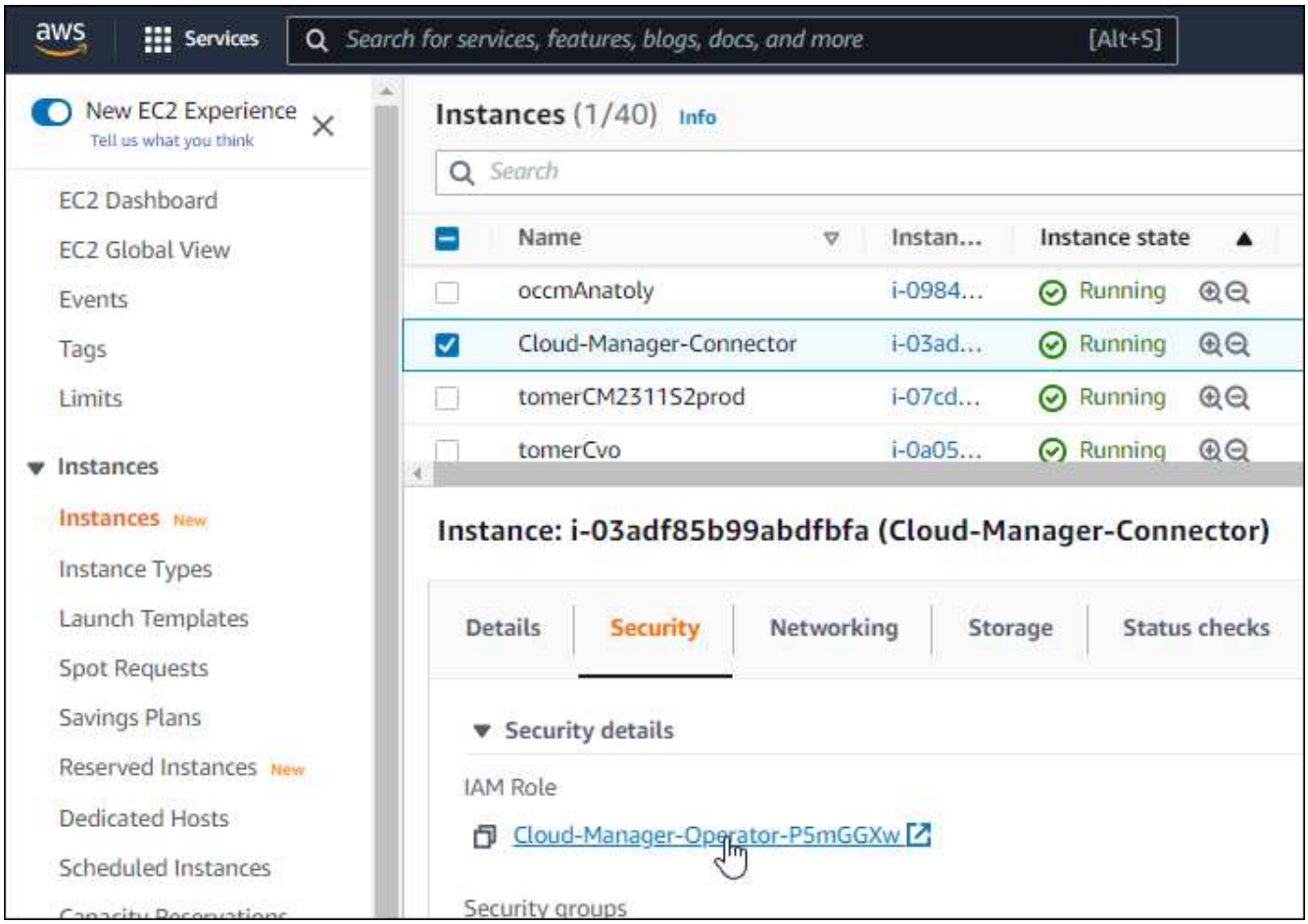
Add the required permissions to an existing Connector

Starting in the 3.9.13 release, any *newly* created Connectors include three new AWS permissions that enable discovery and management of Kubernetes clusters. If you created a Connector prior to this release, then you'll

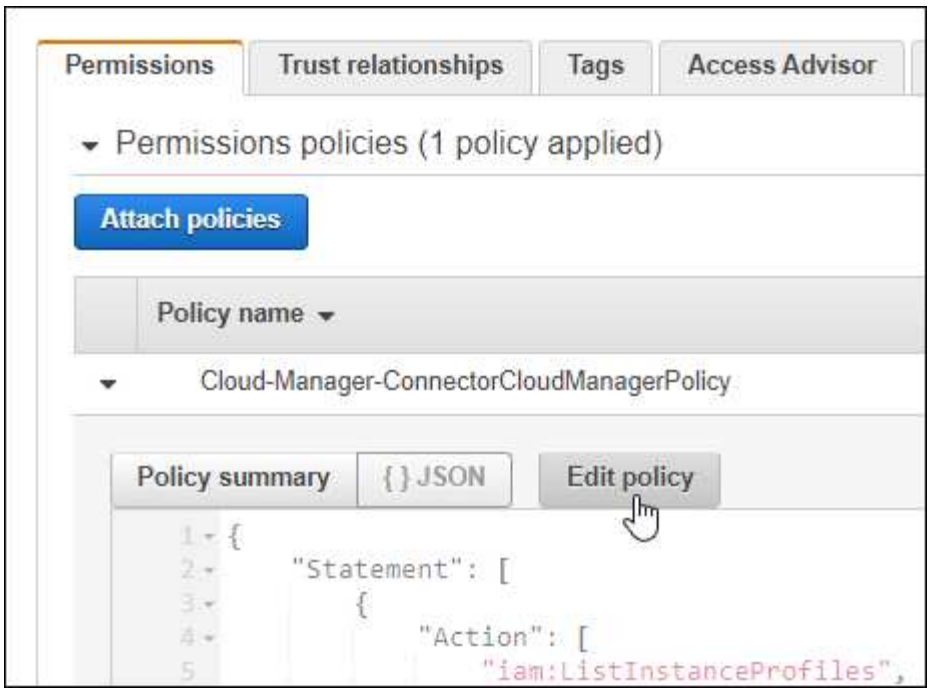
need to modify the existing policy for the Connector's IAM role to provide the permissions.

Steps

1. Go the AWS console and open the EC2 service.
2. Select the Connector instance, click **Security**, and click the name of the IAM role to view the role in the IAM service.



3. In the **Permissions** tab, expand the policy and click **Edit policy**.



4. Click **JSON** and add the following permissions under the first set of actions:

```
"eks:ListClusters",
"eks:DescribeCluster,"
"iam:GetInstanceProfile"
```

View the full JSON format for the policy.

5. Click **Review policy** and then click **Save changes**.

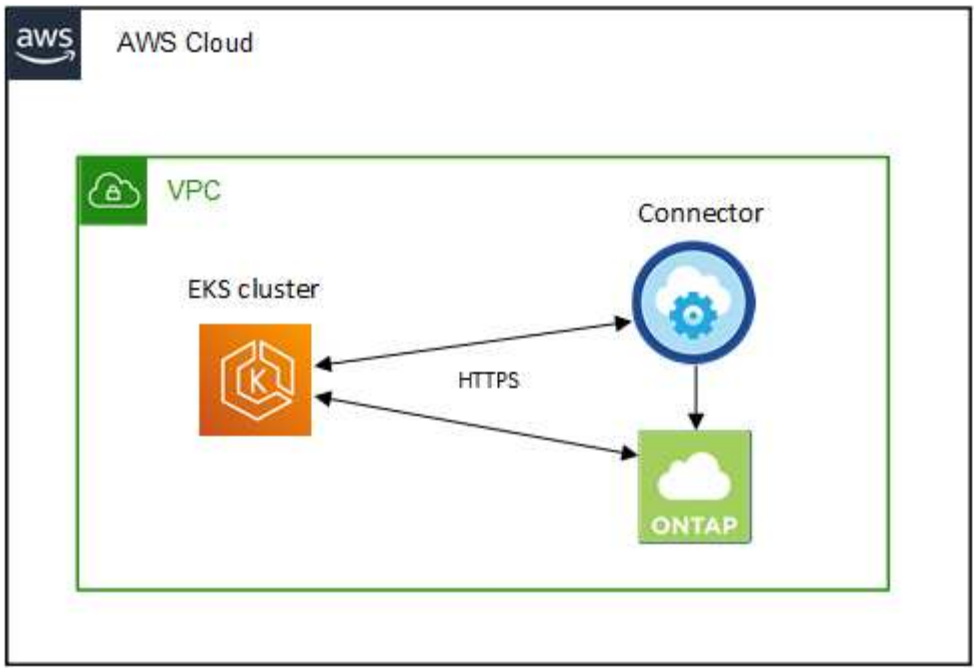
Review networking requirements

You need to provide network connectivity between the Kubernetes cluster and the Connector and between the Kubernetes cluster and the Cloud Volumes ONTAP system that provides backend storage to the cluster.

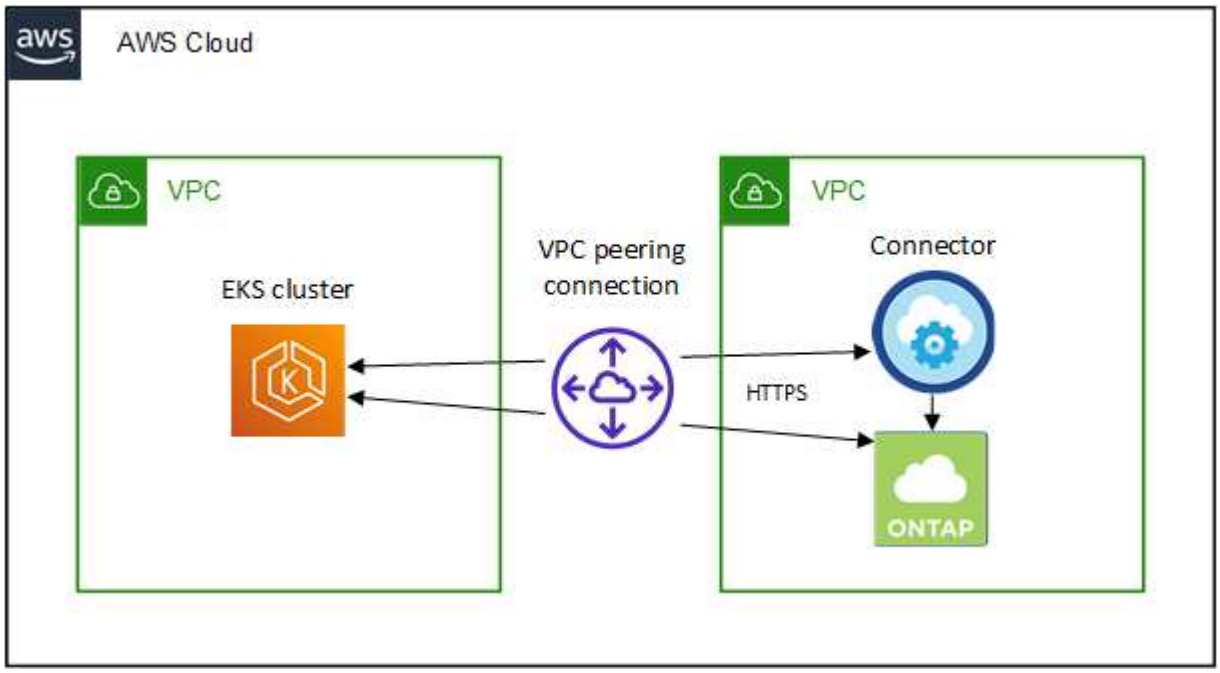
- Each Kubernetes cluster must have an inbound connection from the Connector
- The Connector must have an outbound connection to each Kubernetes cluster over port 443

The simplest way to provide this connectivity is to deploy the Connector and Cloud Volumes ONTAP in the same VPC as the Kubernetes cluster. Otherwise, you need to set up a VPC peering connection between the different VPCs.

Here's an example that shows each component in the same VPC.



And here's another example that shows an EKS cluster running in a different VPC. In this example, VPC peering provides a connection between the VPC for the EKS cluster and the VPC for the Connector and Cloud Volumes ONTAP.



Set up RBAC authorization

You need to authorize the Connector role on each Kubernetes cluster so the Connector can discover and manage a cluster.

Different authorization is required to enable different functionality.

Backup and restore

Backup and restore requires only basic authorization.

Add storage classes

Expanded authorization is required to add storage classes using Cloud Manager.

Install Astra trident

You need to provide full authorization for Cloud Manager to install Astra Trident.

When installing Astra Trident, Cloud Manager installs the Astra Trident backend and Kubernetes secret that contains the credentials Astra Trident needs to communicate with the storage cluster.

Steps

1. Create a cluster role and role binding.
    a. Create a YAML file that includes the following text based on your authorization requirements.

Backup/restore

Add basic authorization to enable backup and restore for Kubernetes clusters.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
        - ''
      resources:
        - namespaces
      verbs:
        - list
    - apiGroups:
        - ''
      resources:
        - persistentvolumes
      verbs:
        - list
    - apiGroups:
        - ''
      resources:
        - pods
        - pods/exec
      verbs:
        - get
        - list
    - apiGroups:
        - ''
      resources:
        - persistentvolumeclaims
      verbs:
        - list
        - create
    - apiGroups:
        - storage.k8s.io
      resources:
        - storageclasses
      verbs:
        - list
    - apiGroups:
        - trident.netapp.io
      resources:
        - tridentbackends
```

```
      verbs:
          - list
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentorchestrators
      verbs:
          - get
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
subjects:
    - kind: Group
      name: cloudmanager-access-group
      apiGroup: rbac.authorization.k8s.io
roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
    apiGroup: rbac.authorization.k8s.io
```

Storage classes

Add expanded authorization to add storage classes using Cloud Manager.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
          - ''
      resources:
          - secrets
          - namespaces
          - persistentvolumeclaims
          - persistentvolumes
          - pods
          - pods/exec
      verbs:
          - get
          - list
          - create
          - delete
    - apiGroups:
```

```
          - storage.k8s.io
      resources:
          - storageclasses
      verbs:
          - get
          - create
          - list
          - delete
          - patch
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentbackends
          - tridentorchestrators
          - tridentbackendconfigs
      verbs:
          - get
          - list
          - create
          - delete
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
subjects:
    - kind: Group
      name: cloudmanager-access-group
      apiGroup: rbac.authorization.k8s.io
roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
    apiGroup: rbac.authorization.k8s.io
```

Install Trident

Use the command line to provide full authorization and enable Cloud Manager to install Astra Trident.

```
eksctl create iamidentitymapping --cluster < > --region < > --arn
< > --group "system:masters" --username
system:node:{{EC2PrivateDNSName}}
```

b. Apply the configuration to a cluster.

```
kubectl apply -f <file-name>
```

2. Create an identity mapping to the permissions group.

Use eksctl

Use eksctl to create an IAM identity mapping between a cluster and the IAM role for the Cloud Manager Connector.

Go to the eksctl documentation for full instructions.

An example is provided below.

```
eksctl create iamidentitymapping --cluster <eksCluster> --region
<us-east-2> --arn <ARN of the Connector IAM role> --group
cloudmanager-access-group --username
system:node:{{EC2PrivateDNSName}}
```

Edit aws-auth

Directly edit the aws-auth ConfigMap to add RBAC access to the IAM role for the Cloud Manager Connector.

Go to the AWS EKS documentation for full instructions.

An example is provided below.

```
apiVersion: v1
data:
  mapRoles: |
    - groups:
      - cloudmanager-access-group
      rolearn: <ARN of the Connector IAM role>
     username: system:node:{{EC2PrivateDNSName}}
kind: ConfigMap
metadata:
  creationTimestamp: "2021-09-30T21:09:18Z"
  name: aws-auth
  namespace: kube-system
  resourceVersion: "1021"
  selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth
  uid: dcc31de5-3838-11e8-af26-02e00430057c
```

Requirements for Kubernetes clusters in Azure

You can add and manage managed Azure Kubernetes clusters (AKS) and self-managed Kubernetes clusters in Azure using Cloud Manager. Before you can add the clusters to Cloud Manager, ensure the following requirements are met.

This topic uses *Kubernetes cluster* where configuration is the same for AKS and self-managed Kubernetes clusters. The cluster type is specified where configuration differs.

Requirements

Astra Trident

One of the four most recent versions of Astra Trident is required. You can install Astra Trident directly from Cloud Manager. You should review the prerequisites prior to installing Astra Trident.

To upgrade Astra Trident, upgrade with the operator.

Cloud Volumes ONTAP

Cloud Volumes ONTAP must be set up as backend storage for the cluster. Go to the Astra Trident docs for configuration steps.

Cloud Manager Connector

A Connector must be running in Azure with the required permissions. Learn more below.

Network connectivity

Network connectivity is required between the Kubernetes cluster and the Connector and between the Kubernetes cluster and Cloud Volumes ONTAP. Learn more below.

RBAC authorization

Cloud Manager supports RBAC-enabled clusters with and without Active Directory. The Cloud Manager Connector role must be authorized on each Azure cluster. Learn more below.

Prepare a Connector

A Cloud Manager Connector in Azure is required to discover and manage Kubernetes clusters. You'll need to create a new Connector or use an existing Connector that has the required permissions.

Create a new Connector

Follow the steps in one of the links below.

- Create a Connector from Cloud Manager (recommended)
- Create a Connector from the Azure Marketplace
- Install the Connector on an existing Linux host

Add the required permissions to an existing Connector (to discover a managed AKS cluster)

If you want to discover a managed AKS cluster, you might need to modify the custom role for the Connector to provide the permissions.

Steps

1. Identify the role assigned to the Connector virtual machine:
    a. In the Azure portal, open the Virtual machines service.
    b. Select the Connector virtual machine.
    c. Under Settings, select **Identity**.
    d. Click **Azure role assignments**.
    e. Make note of the custom role assigned to the Connector virtual machine.
2. Update the custom role:
    a. In the Azure portal, open your Azure subscription.
    b. Click **Access control (IAM) > Roles**.
    c. Click the ellipsis (…) for the custom role and then click **Edit**.
    d. Click JSON and add the following permissions:

```
"Microsoft.ContainerService/managedClusters/listClusterUserCredential
/action"
"Microsoft.ContainerService/managedClusters/read"
```

    e. Click **Review + update** and then click **Update**.

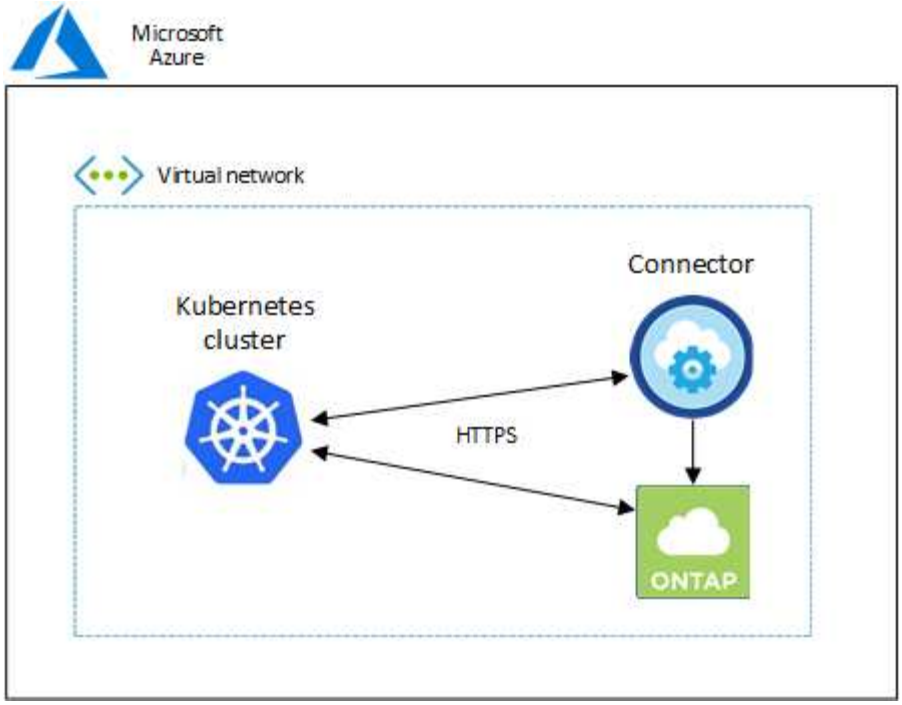
Review networking requirements

You need to provide network connectivity between the Kubernetes cluster and the Connector and between the Kubernetes cluster and the Cloud Volumes ONTAP system that provides backend storage to the cluster.

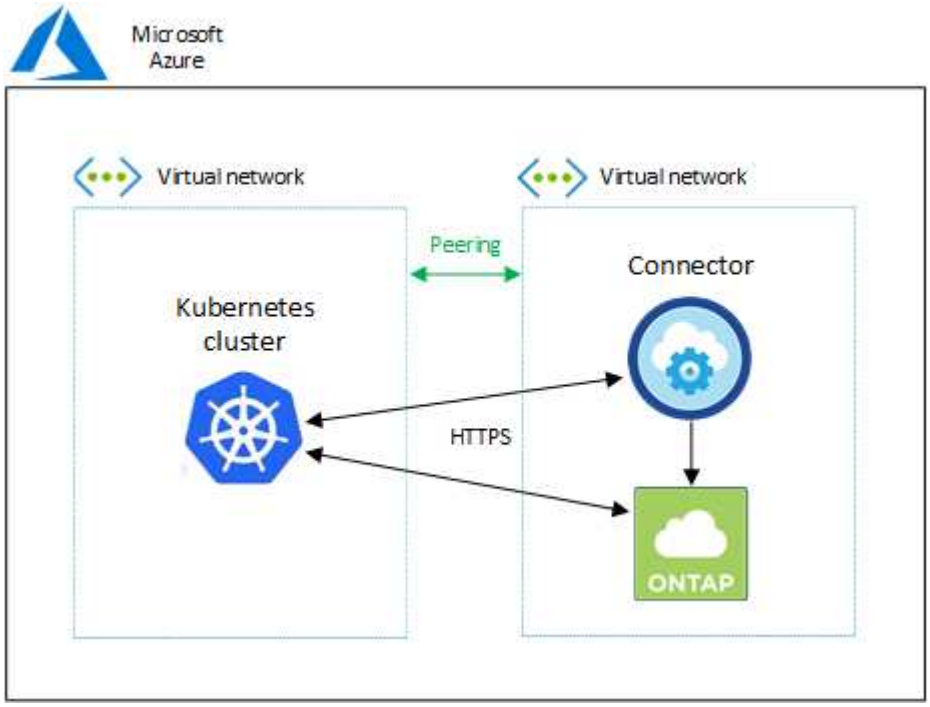
- Each Kubernetes cluster must have an inbound connection from the Connector
- The Connector must have an outbound connection to each Kubernetes cluster over port 443

The simplest way to provide this connectivity is to deploy the Connector and Cloud Volumes ONTAP in the same VNet as the Kubernetes cluster. Otherwise, you need to set up a peering connection between the different VNets.

Here's an example that shows each component in the same VNet.



And here's another example that shows a Kubernetes cluster running in a different VNet. In this example, peering provides a connection between the VNet for the Kubernetes cluster and the VNet for the Connector and Cloud Volumes ONTAP.



Set up RBAC authorization

RBAC validation occurs only on Kubernetes clusters with Active Directory (AD) enabled. Kubernetes clusters without AD will pass validation automatically.

You need authorize the Connector role on each Kubernetes cluster so the Connector can discover and manage a cluster.

Backup and restore

Backup and restore requires only basic authorization.

Add storage classes

Expanded authorization is required to add storage classes using Cloud Manager.

Install Astra trident

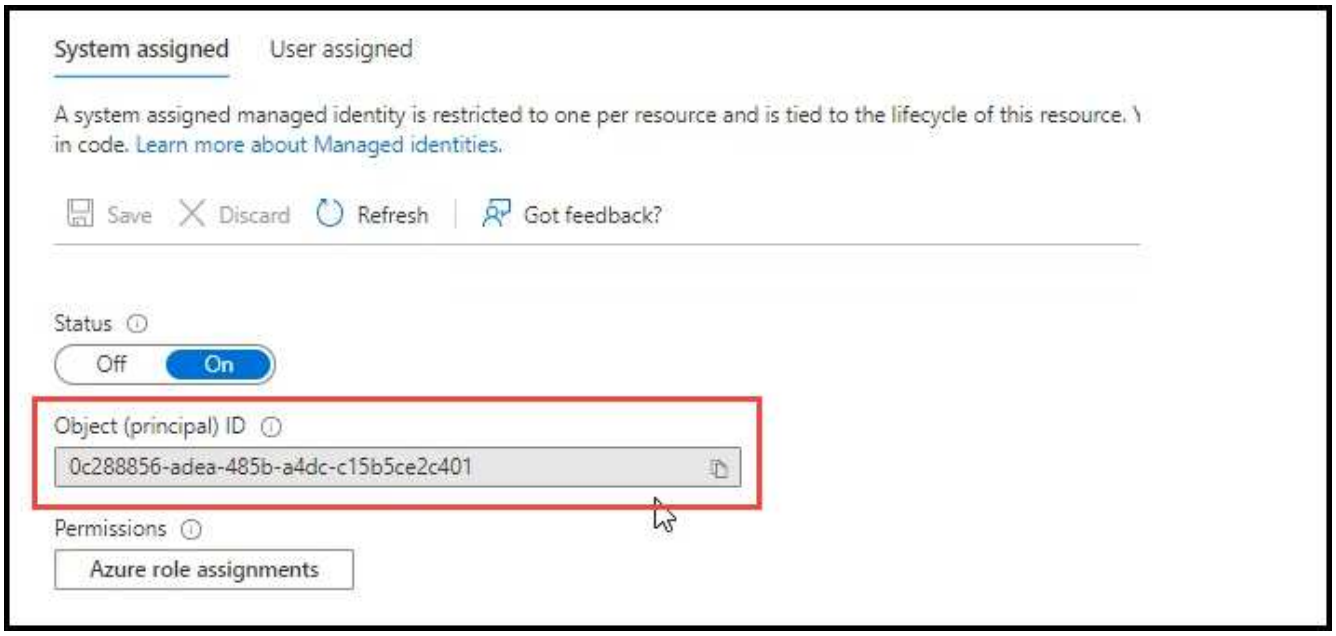
You need to provide full authorization for Cloud Manager to install Astra Trident.

When installing Astra Trident, Cloud Manager installs the Astra Trident backend and Kubernetes secret that contains the credentials Astra Trident needs to communicate with the storage cluster.

Before you begin

Your RBAC `subjects: name:` configuration varies slightly based on your Kubernetes cluster type.

- If you are deploying a **managed AKS cluster**, you need the Object ID for the system-assigned managed identity for the Connector. This ID is available in Azure management portal.



- If you are deploying a **self-managed Kubernetes cluster**, you need the username of any authorized user.

Steps

Create a cluster role and role binding.

1. Create a YAML file that includes the following text based on your authorization requirements. Replace the `subjects: kind:` variable with your username and `subjects: user:` with either the Object ID for the system-assigned managed identity or username of any authorized user as described above.

Backup/restore

Add basic authorization to enable backup and restore for Kubernetes clusters.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
        - ''
      resources:
        - namespaces
      verbs:
        - list
    - apiGroups:
        - ''
      resources:
        - persistentvolumes
      verbs:
        - list
    - apiGroups:
        - ''
      resources:
        - pods
        - pods/exec
      verbs:
        - get
        - list
    - apiGroups:
        - ''
      resources:
        - persistentvolumeclaims
      verbs:
        - list
        - create
    - apiGroups:
        - storage.k8s.io
      resources:
        - storageclasses
      verbs:
        - list
    - apiGroups:
        - trident.netapp.io
      resources:
        - tridentbackends
```

```
      verbs:
          - list
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentorchestrators
      verbs:
          - get
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
subjects:
    - kind: User
      name:
      apiGroup: rbac.authorization.k8s.io
roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
    apiGroup: rbac.authorization.k8s.io
```

Storage classes

Add expanded authorization to add storage classes using Cloud Manager.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
          - ''
      resources:
          - secrets
          - namespaces
          - persistentvolumeclaims
          - persistentvolumes
          - pods
          - pods/exec
      verbs:
          - get
          - list
          - create
          - delete
    - apiGroups:
```

```
            - storage.k8s.io
        resources:
            - storageclasses
        verbs:
            - get
            - create
            - list
            - delete
            - patch
    - apiGroups:
            - trident.netapp.io
        resources:
            - tridentbackends
            - tridentorchestrators
            - tridentbackendconfigs
        verbs:
            - get
            - list
            - create
            - delete
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
subjects:
    - kind: User
      name:
      apiGroup: rbac.authorization.k8s.io
roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
    apiGroup: rbac.authorization.k8s.io
```

Install Trident

Use the command line to provide full authorization and enable Cloud Manager to install Astra Trident.

```
kubectl create clusterrolebinding test --clusterrole cluster-admin
--user <Object (principal) ID>
```

2. Apply the configuration to a cluster.

```
kubectl apply -f <file-name>
```

Requirements for Kubernetes clusters in Google Cloud

You can add and manage managed Google Kubernetes Engine (GKE) clusters and self-managed Kubernetes clusters in Google using Cloud Manager. Before you can add the clusters to Cloud Manager, ensure the following requirements are met.

This topic uses *Kubernetes cluster* where configuration is the same for GKE and self-managed Kubernetes clusters. The cluster type is specified where configuration differs.

Requirements

Astra Trident

One of the four most recent versions of Astra Trident is required. You can install Astra Trident directly from Cloud Manager. You should review the prerequisites prior to installing Astra Trident

To upgrade Astra Trident, upgrade with the operator.

Cloud Volumes ONTAP

Cloud Volumes ONTAP must be in Cloud Manager under the same tenancy account, workspace, and Connector as the Kubernetes cluster. Go to the Astra Trident docs for configuration steps.

Cloud Manager Connector

A Connector must be running in Google with the required permissions. Learn more below.

Network connectivity

Network connectivity is required between the Kubernetes cluster and the Connector and between the Kubernetes cluster and Cloud Volumes ONTAP. Learn more below.

RBAC authorization

Cloud Manager supports RBAC-enabled clusters with and without Active Directory. The Cloud Manager Connector role must be authorized on each GKE cluster. Learn more below.

Prepare a Connector

A Cloud Manager Connector in Google is required to discover and manage Kubernetes clusters. You'll need to create a new Connector or use an existing Connector that has the required permissions.

Create a new Connector

Follow the steps in one of the links below.

- Create a Connector from Cloud Manager (recommended)
- Install the Connector on an existing Linux host

Add the required permissions to an existing Connector (to discover a managed GKE cluster)

If you want to discover a managed GKE cluster, you might need to modify the custom role for the Connector to provide the permissions.

Steps

1. In Cloud Console, go to the **Roles** page.

2. Using the drop-down list at the top of the page, select the project or organization that contains the role that you want to edit.
3. Click a custom role.
4. Click **Edit Role** to update the role's permissions.
5. Click **Add Permissions** to add the following new permissions to the role.

```
container.clusters.get
container.clusters.list
```

6. Click **Update** to save the edited role.

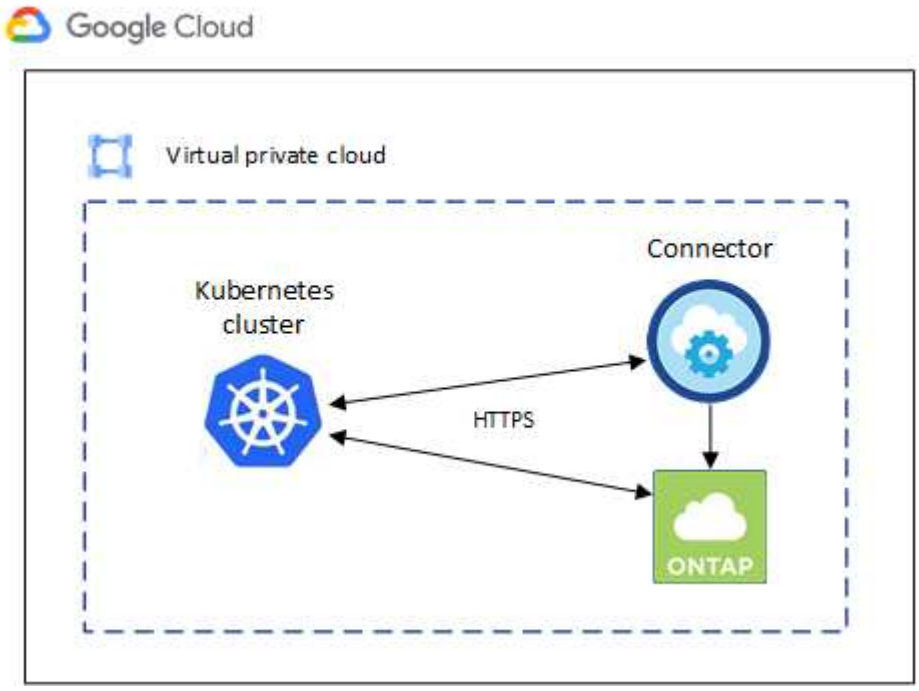
Review networking requirements

You need to provide network connectivity between the Kubernetes cluster and the Connector and between the Kubernetes cluster and the Cloud Volumes ONTAP system that provides backend storage to the cluster.

- Each Kubernetes cluster must have an inbound connection from the Connector
- The Connector must have an outbound connection to each Kubernetes cluster over port 443

The simplest way to provide this connectivity is to deploy the Connector and Cloud Volumes ONTAP in the same VPC as the Kubernetes cluster. Otherwise, you need to set up a peering connection between the different VPC.

Here's an example that shows each component in the same VPC.



Set up RBAC authorization

RBAC validation occurs only on Kubernetes clusters with Active Directory (AD) enabled. Kubernetes clusters without AD will pass validation automatically.

You need authorize the Connector role on each Kubernetes cluster so the Connector can discover and manage a cluster.

Backup and restore

Backup and restore requires only basic authorization.

Add storage classes

Expanded authorization is required to add storage classes using Cloud Manager.

Install Astra trident

You need to provide full authorization for Cloud Manager to install Astra Trident.

When installing Astra Trident, Cloud Manager installs the Astra Trident backend and Kubernetes secret that contains the credentials Astra Trident needs to communicate with the storage cluster.

Before you begin

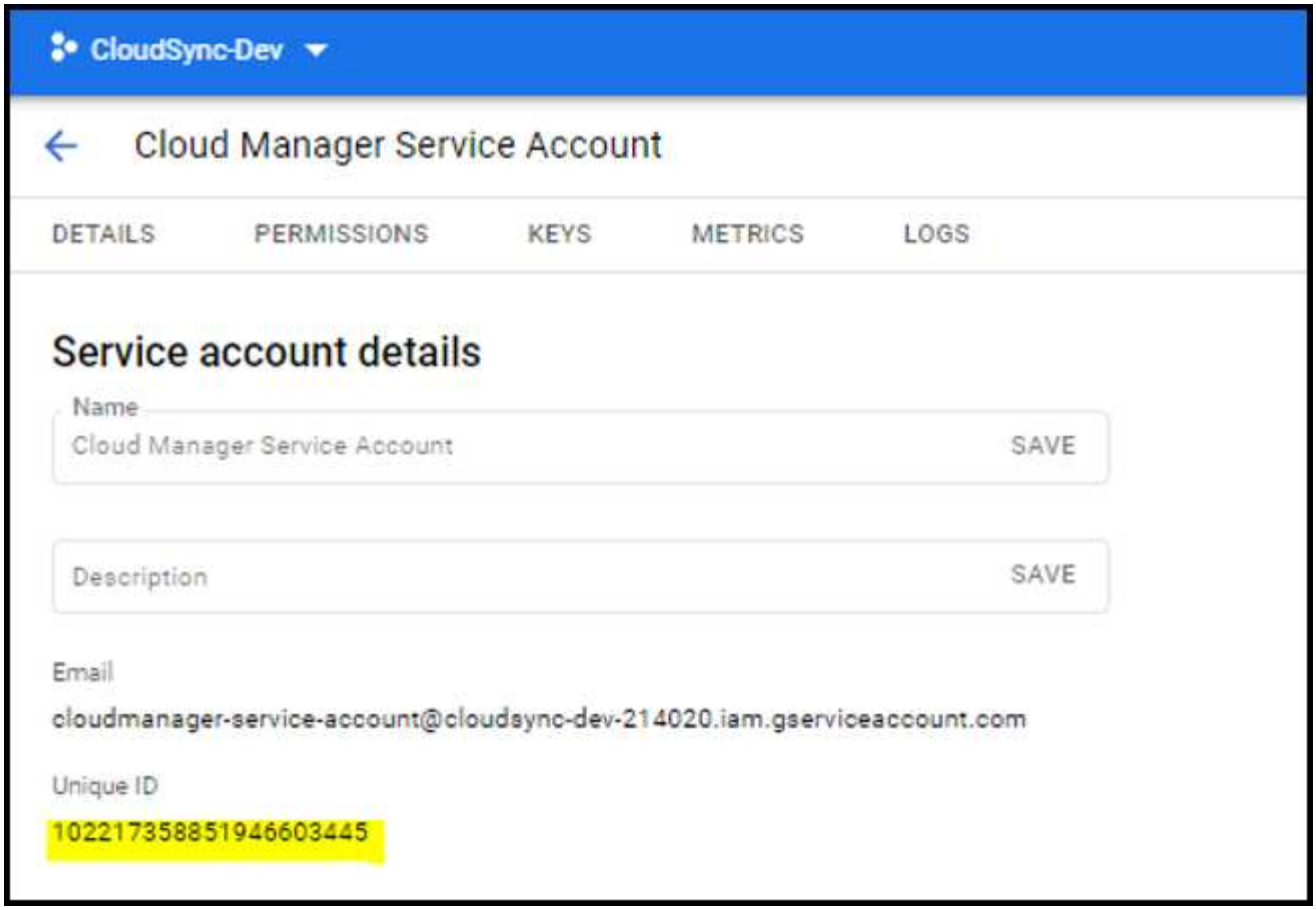
To configure `subjects: name:` in the YAML file, you need to know the Cloud Manager Unique ID.

You can find the unique ID one of two ways:

- Using the command:

```
gcloud iam service-accounts list
gcloud iam service-accounts describe <service-account-email>
```

- In the Service Account Details on the Cloud Console.



Steps

Create a cluster role and role binding.

1. Create a YAML file that includes the following text based on your authorization requirements. Replace the `subjects: kind:` variable with your username and `subjects: user:` with the unique ID for the authorized service account.

Backup/restore

Add basic authorization to enable backup and restore for Kubernetes clusters.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
        - ''
      resources:
        - namespaces
      verbs:
        - list
    - apiGroups:
        - ''
      resources:
        - persistentvolumes
      verbs:
        - list
    - apiGroups:
        - ''
      resources:
        - pods
        - pods/exec
      verbs:
        - get
        - list
    - apiGroups:
        - ''
      resources:
        - persistentvolumeclaims
      verbs:
        - list
        - create
    - apiGroups:
        - storage.k8s.io
      resources:
        - storageclasses
      verbs:
        - list
    - apiGroups:
        - trident.netapp.io
      resources:
        - tridentbackends
```

```
      verbs:
          - list
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentorchestrators
      verbs:
          - get
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
subjects:
    - kind: User
      name:
      apiGroup: rbac.authorization.k8s.io
roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
    apiGroup: rbac.authorization.k8s.io
```

Storage classes

Add expanded authorization to add storage classes using Cloud Manager.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
          - ''
      resources:
          - secrets
          - namespaces
          - persistentvolumeclaims
          - persistentvolumes
          - pods
          - pods/exec
      verbs:
          - get
          - list
          - create
          - delete
    - apiGroups:
```

```
            - storage.k8s.io
        resources:
            - storageclasses
        verbs:
            - get
            - create
            - list
            - delete
            - patch
    - apiGroups:
            - trident.netapp.io
        resources:
            - tridentbackends
            - tridentorchestrators
            - tridentbackendconfigs
        verbs:
            - get
            - list
            - create
            - delete
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
subjects:
    - kind: User
      name:
      apiGroup: rbac.authorization.k8s.io
roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
    apiGroup: rbac.authorization.k8s.io
```

Install Trident

Use the command line to provide full authorization and enable Cloud Manager to install Astra Trident.

```
kubectl create clusterrolebinding test --clusterrole cluster-admin
--user <Unique ID>
```

2. Apply the configuration to a cluster.

```
kubectl apply -f <file-name>
```

Add Kubernetes clusters

Add an Amazon Kubernetes cluster to Cloud Manager

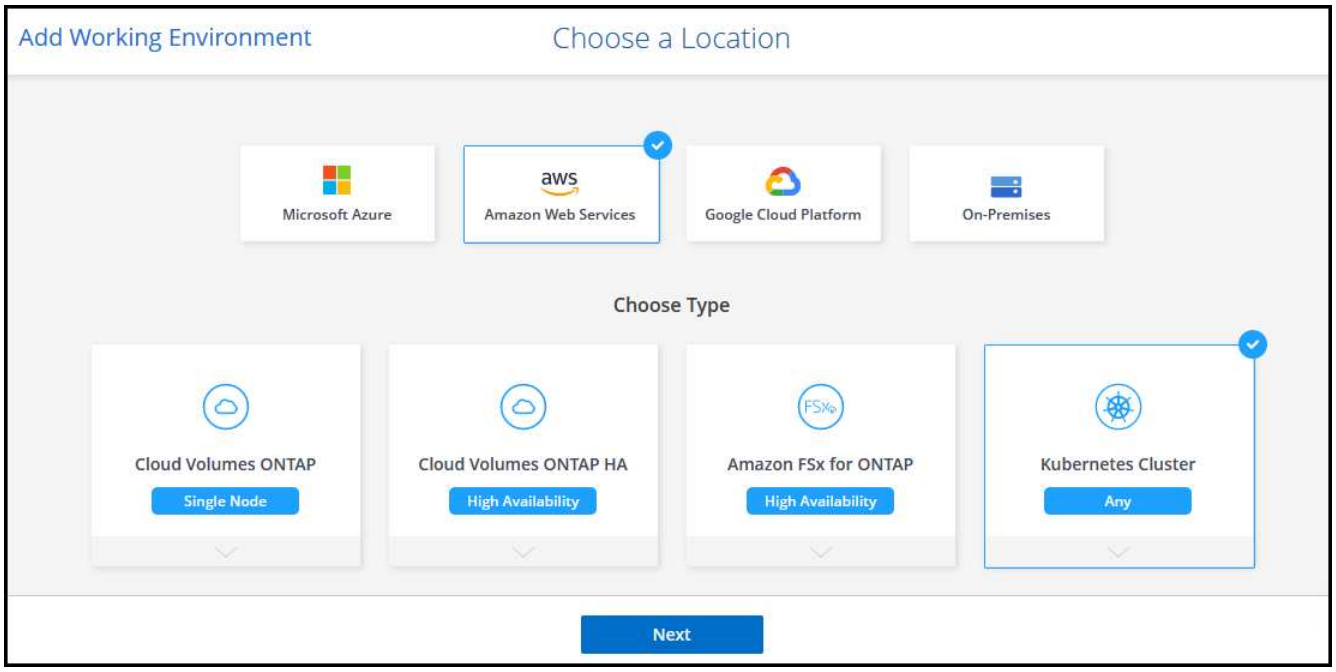
You can discover or import Kubernetes clusters to Cloud Manager so you can back up persistent volumes to Amazon S3.

Discover a cluster

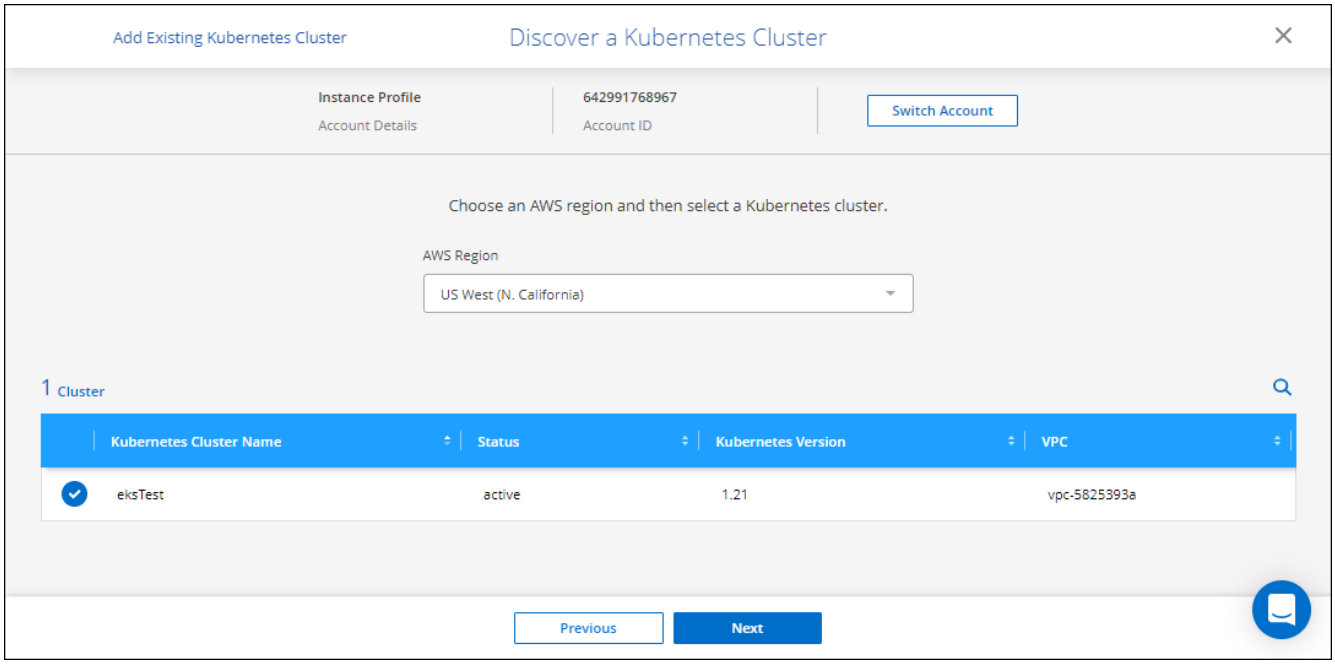
You can discover a fully-managed or self-managed Kubernetes cluster. Managed clusters must be discovered; they cannot be imported.

Steps

1. On the **Canvas**, click **Add Working Environment**.
2. Select **Amazon Web Services** > **Kubernetes Cluster** and click **Next**.

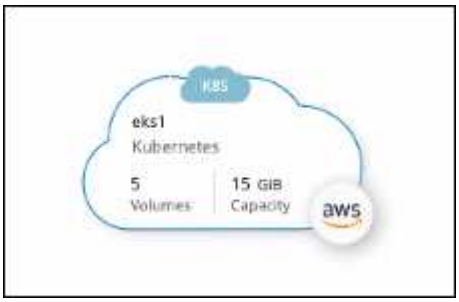


3. Select **Discover Cluster** and click **Next**.
4. Choose an AWS region, select a Kubernetes cluster, and then click **Next**.



Result

Cloud Manager adds the Kubernetes cluster to the Canvas.

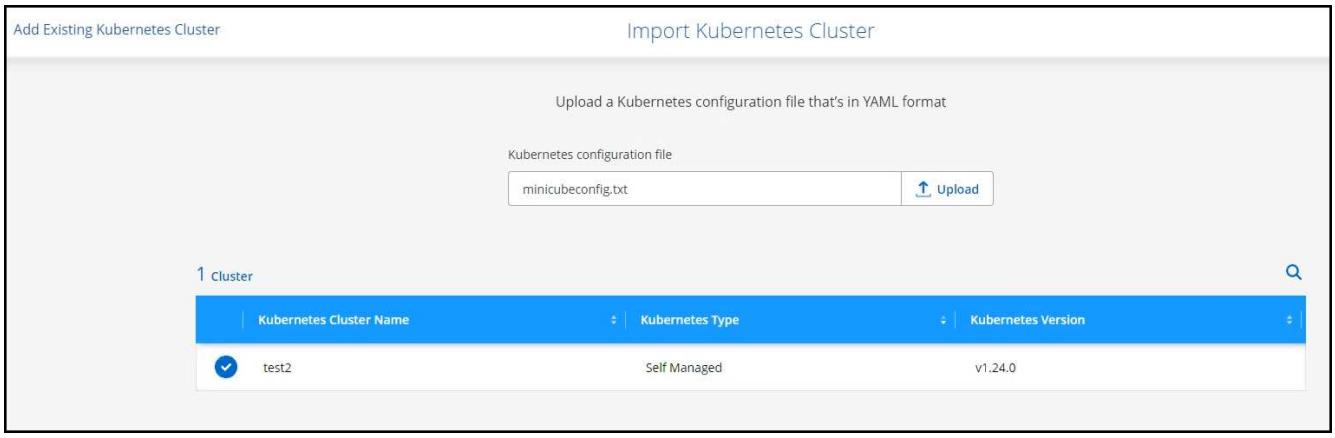


Import a Cluster

You can import a self-managed Kubernetes cluster using a Kubernetes configuration file.

Steps

1. On the **Canvas**, click **Add Working Environment**.
2. Select **Amazon Web Services** > **Kubernetes Cluster** and click **Next**.
3. Select **Import Cluster** and click **Next**.
4. Upload a Kubernetes configuration file in YAML format.



5. Select the Kubernetes cluster and click **Next**.

Result

Cloud Manager adds the Kubernetes cluster to the Canvas.

Add an Azure Kubernetes cluster to Cloud Manager

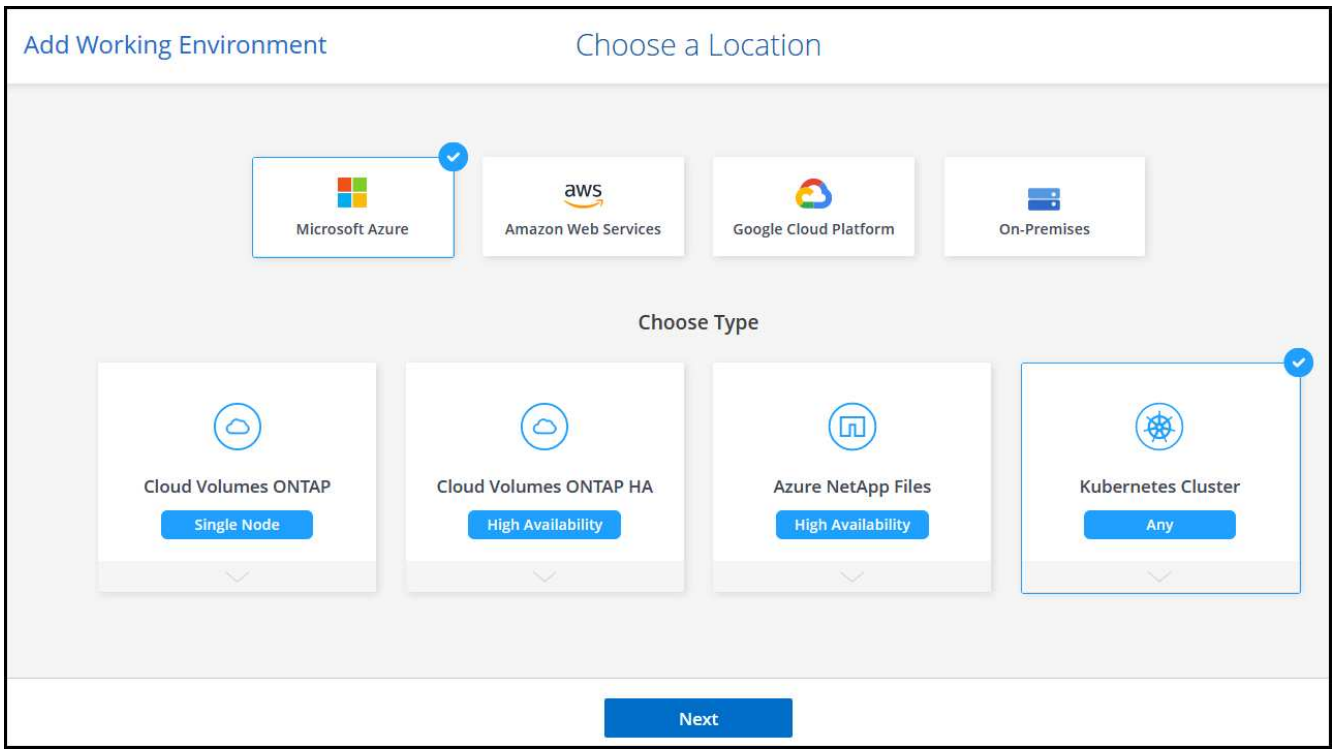
You can discover or import Kubernetes clusters to Cloud Manager so that you can back up persistent volumes to Azure.

Discover a cluster

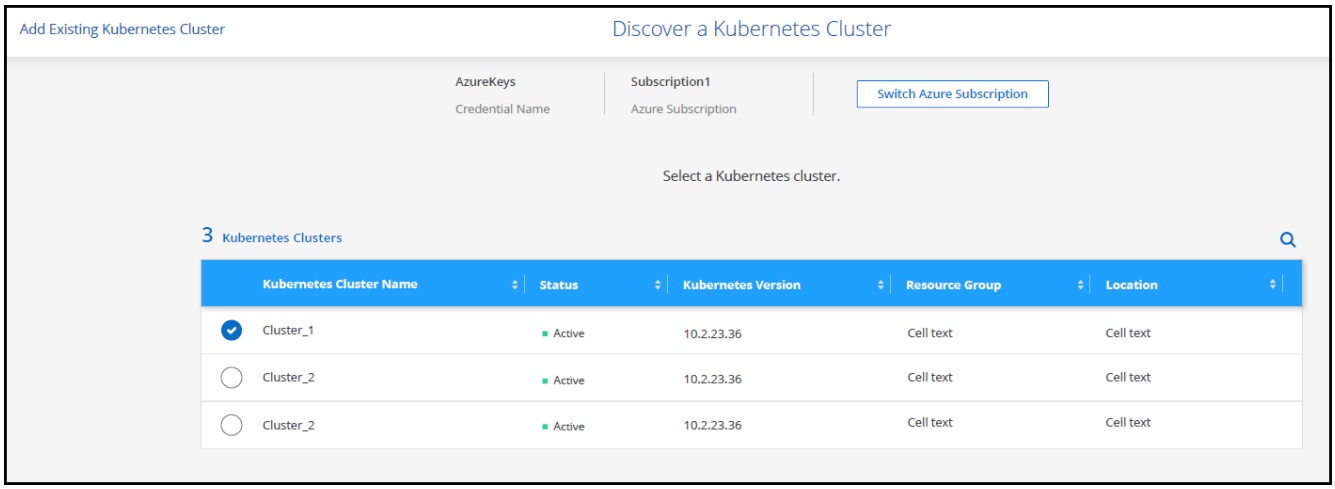
You can discover a fully-managed or self-managed Kubernetes cluster. Managed clusters must be discovered; they cannot be imported.

Steps

1. On the **Canvas**, click **Add Working Environment**.
2. Select **Microsoft Azure** > **Kubernetes Cluster** and click **Next**.

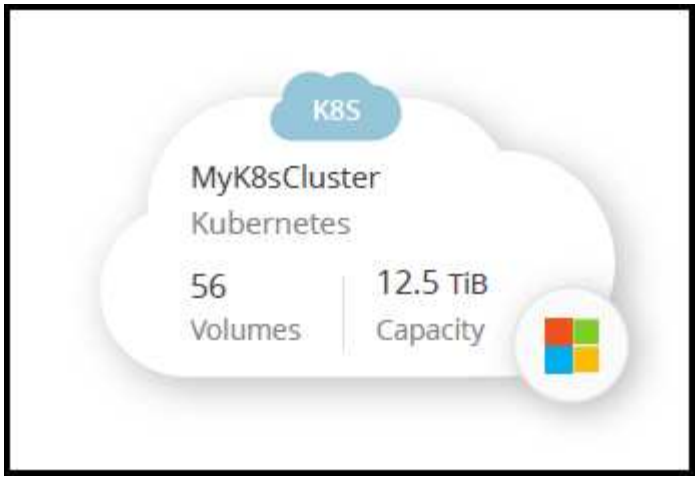


3. Select **Discover Cluster** and click **Next**.
4. Select a Kubernetes cluster and click **Next**.



Result

Cloud Manager adds the Kubernetes cluster to the Canvas.



Import a Cluster

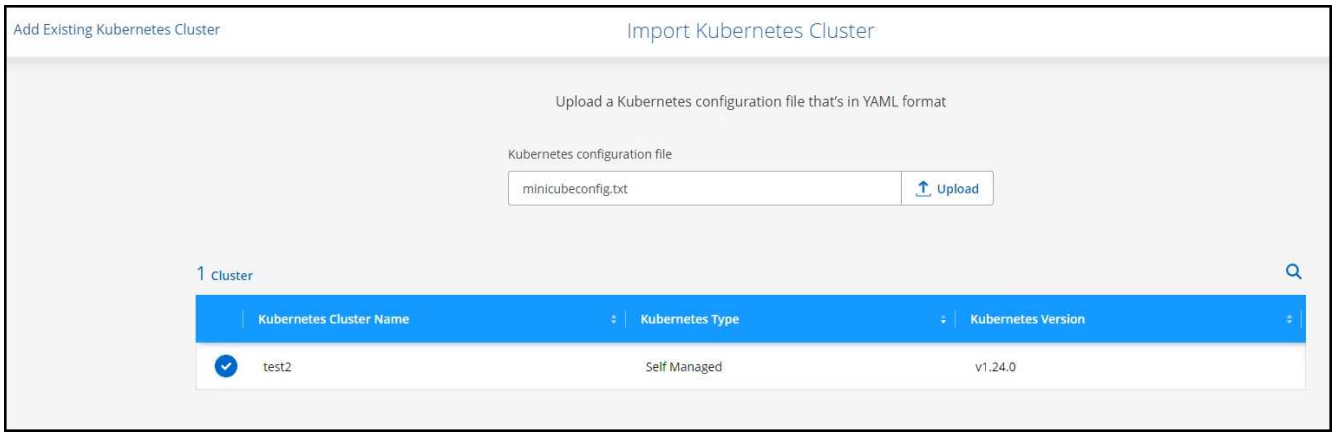
You can import a self-managed Kubernetes cluster using a Kubernetes configuration file.

Before you get started

You will need Certificate Authority, Client Key, and Client Certificate certificates for the user specified in the cluster role YAML file to import Kubernetes clusters. The Kubernetes cluster administrator receives these certifications when creating users on the Kubernetes cluster.

Steps

1. On the **Canvas**, click **Add Working Environment**.
2. Select **Microsoft Azure** > **Kubernetes Cluster** and click **Next**.
3. Select **Import Cluster** and click **Next**.
4. Upload a Kubernetes configuration file in YAML format.



5. Upload the cluster certificates provided by your Kubernetes cluster administrator.

Result

Cloud Manager adds the Kubernetes cluster to the Canvas.

Add a Google Cloud Kubernetes cluster to Cloud Manager

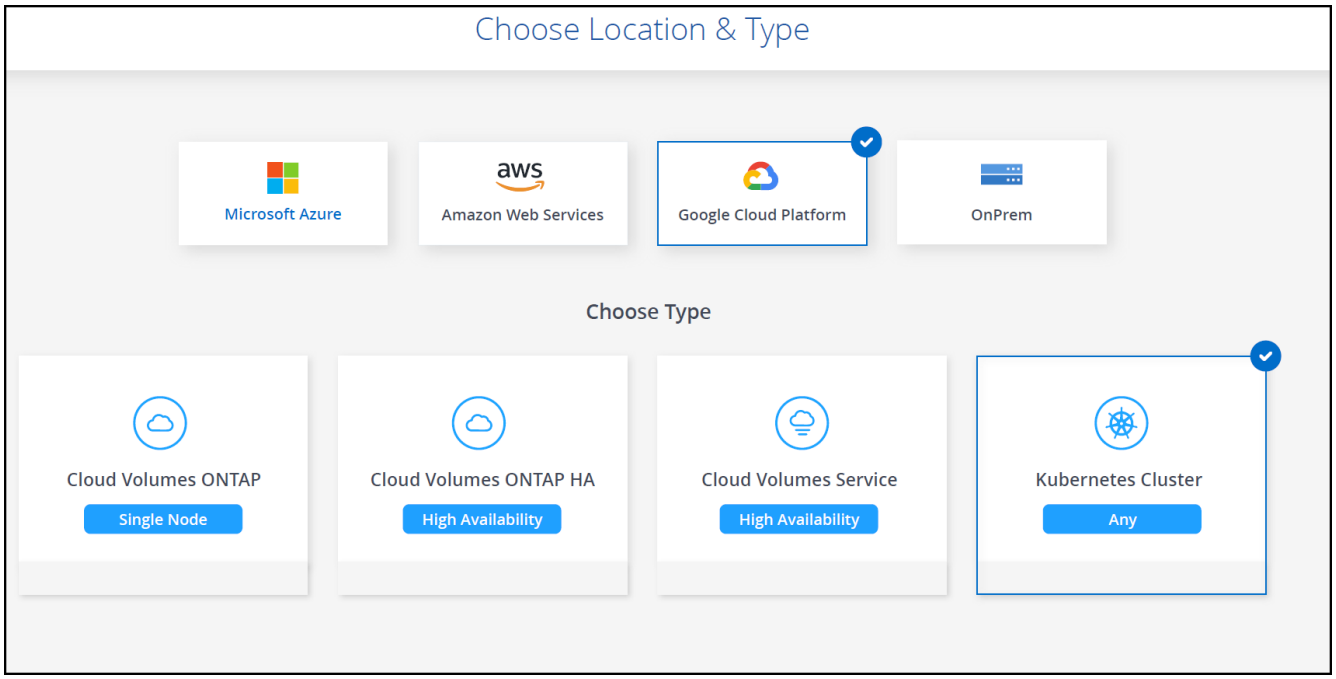
You can discover or import Kubernetes clusters to Cloud Manager so that you can back up persistent volumes to Google Cloud.

Discover a cluster

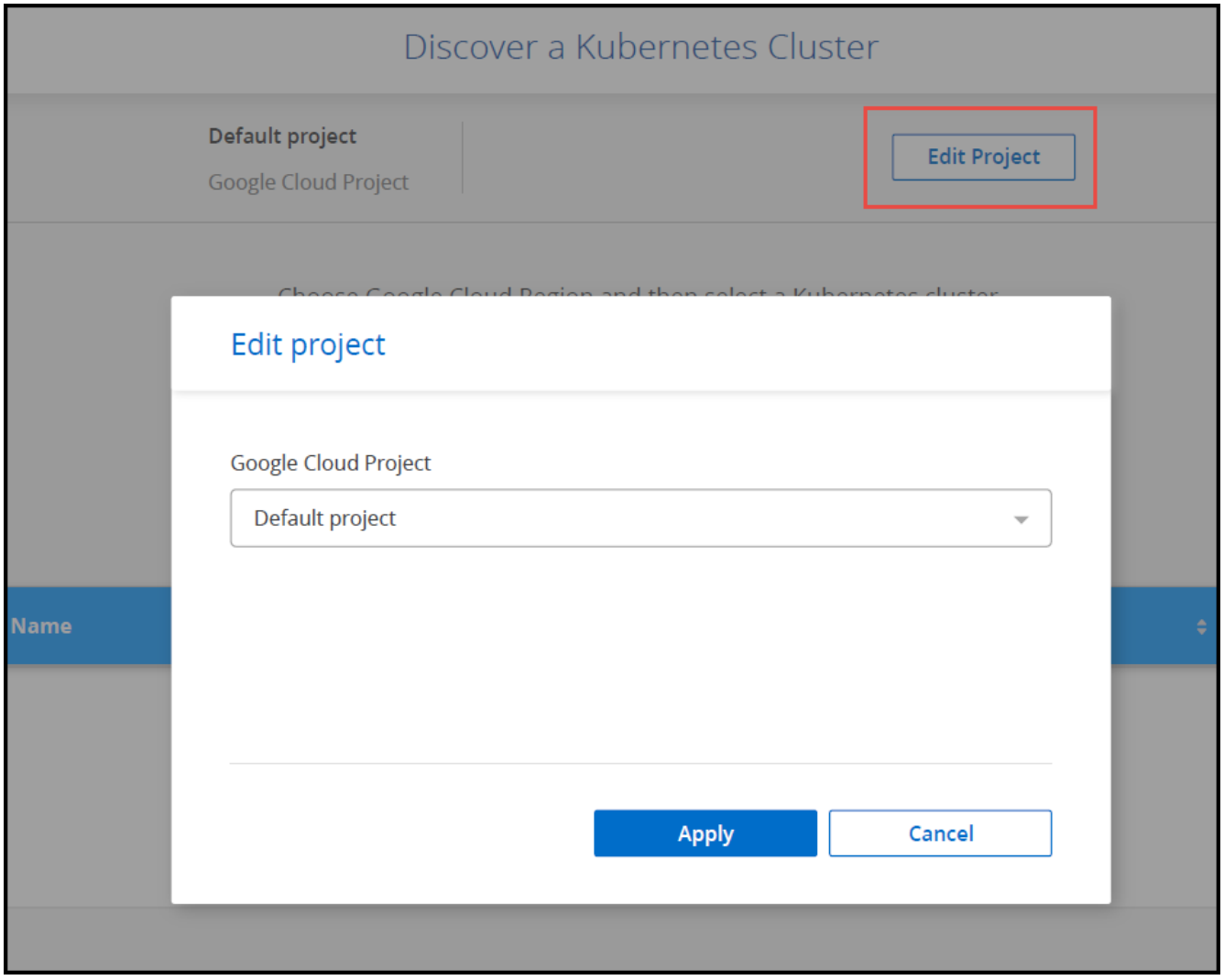
You can discover a fully-managed or self-managed Kubernetes cluster. Managed clusters must be discovered; they cannot be imported.

Steps

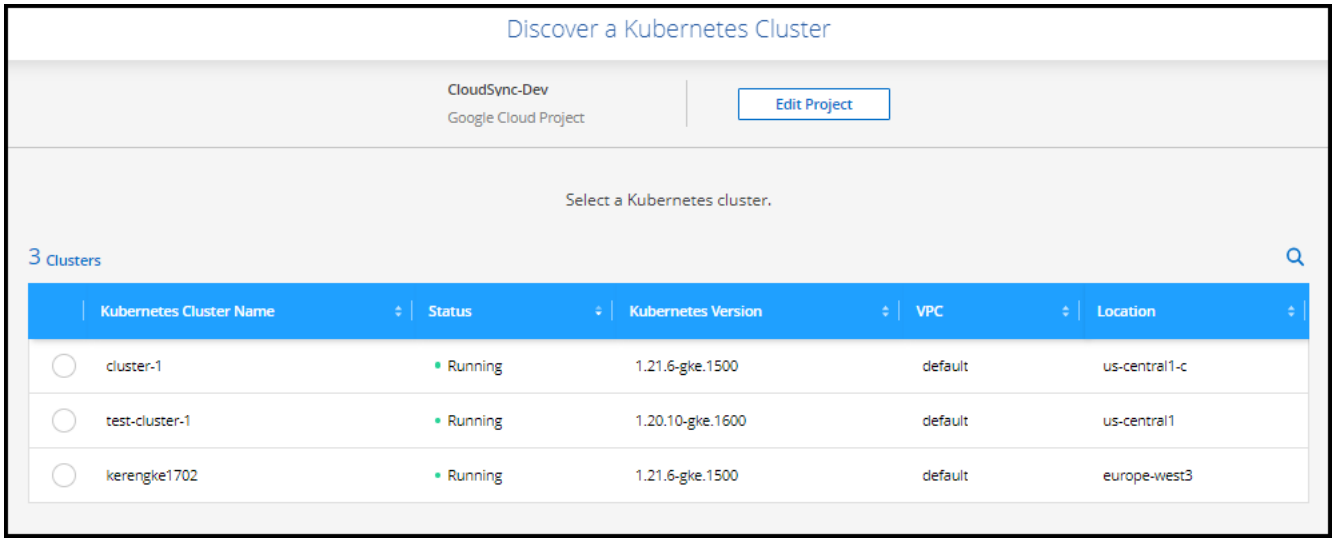
1. On the **Canvas**, click **Add Working Environment**.
2. Select **Google Cloud Platform** > **Kubernetes Cluster** and click **Next**.



3. Select **Discover Cluster** and click **Next**.
4. To select a Kubernetes cluster in a different Google Cloud Project, click **Edit project** and choose an available project.

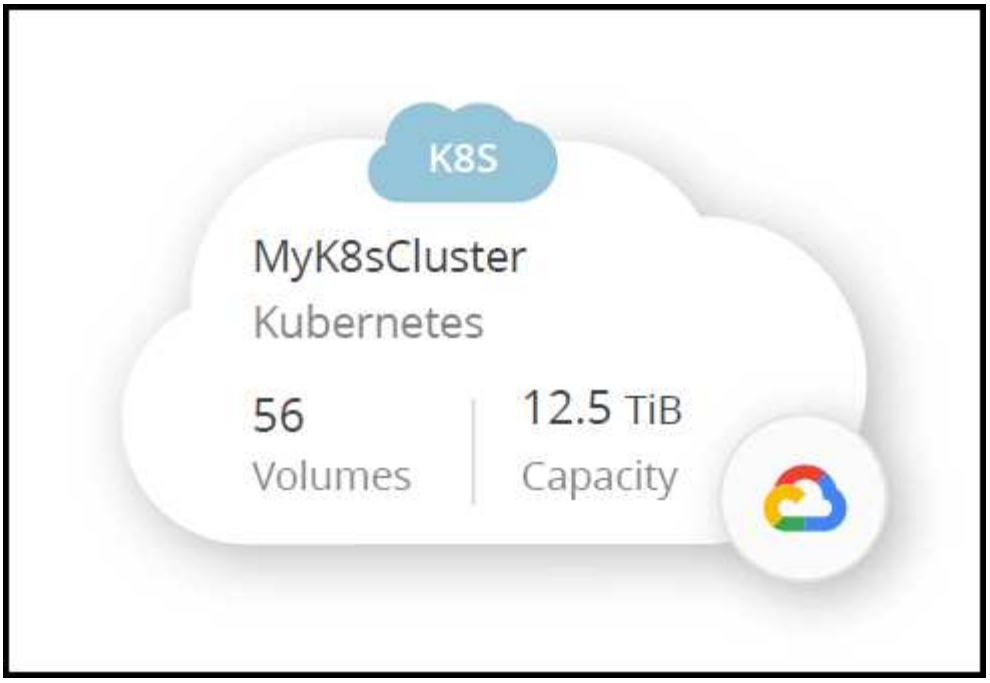


5. Select a Kubernetes cluster and click **Next**.



Result

Cloud Manager adds the Kubernetes cluster to the Canvas.



Import a Cluster

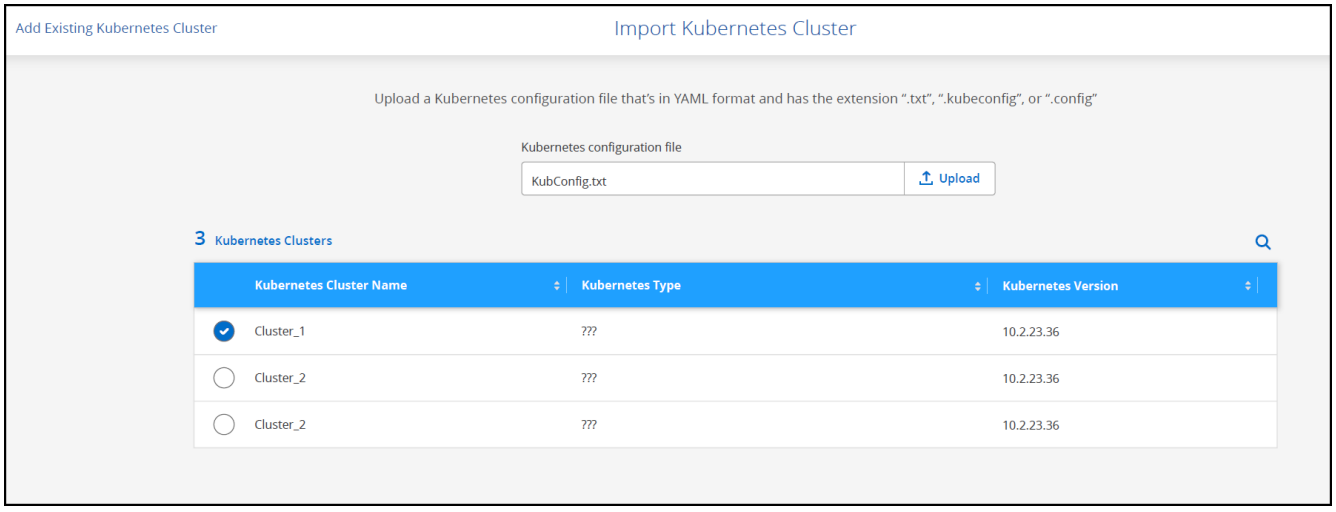
You can import a self-managed Kubernetes cluster using a Kubernetes configuration file.

Before you get started

You will need Certificate Authority, Client Key, and Client Certificate certificates for the user specified in the cluster role YAML file to import Kubernetes clusters. The Kubernetes cluster administrator receives these certifications when creating users on the Kubernetes cluster.

Steps

1. On the **Canvas**, click **Add Working Environment**.
2. Select **Google Cloud Platform** > **Kubernetes Cluster** and click **Next**.
3. Select **Import Cluster** and click **Next**.
4. Upload a Kubernetes configuration file in YAML format.



Result

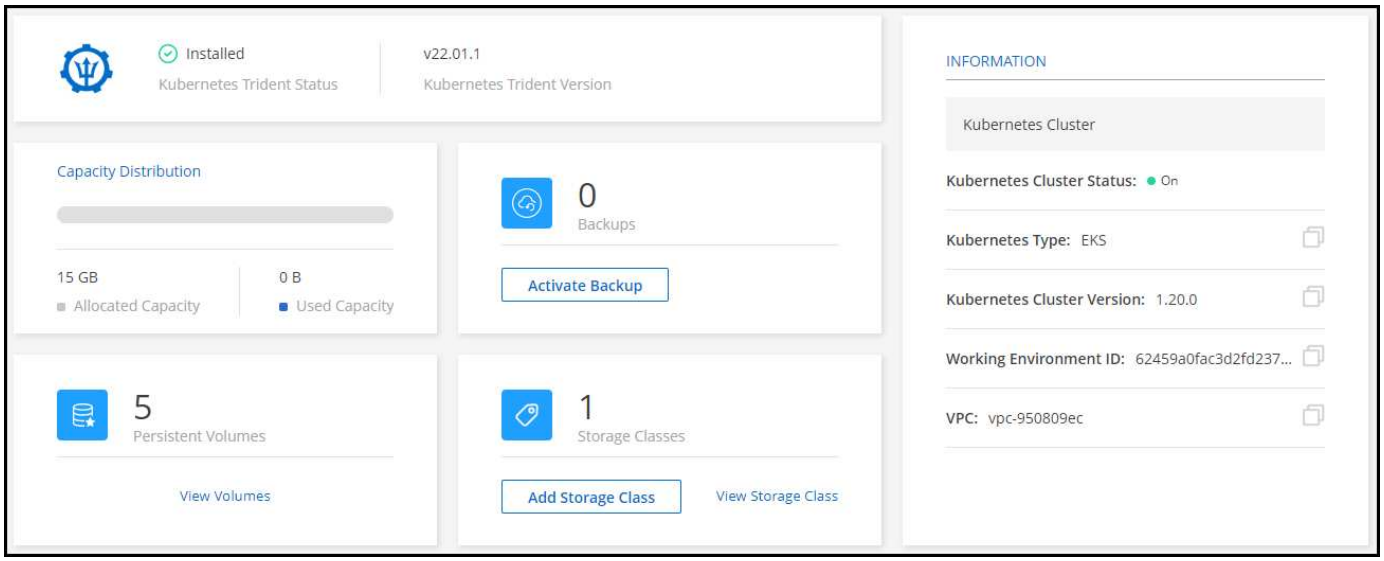
Cloud Manager adds the Kubernetes cluster to the Canvas.

Manage Kubernetes clusters

You can use Cloud Manager to install Astra Trident, configure storage classes, remove clusters, and enable data services.

Features

After adding Kubernetes clusters to Cloud Manager, you can manage the clusters from the resource page. To open the resource page, double-click the Kubernetes working environment on the Canvas.



From the resource page you can:

- View the Kubernetes cluster status.
- Confirm Astra Trident is installed. See Install Astra Trident.
- Add and remove storage classes. See Manage storage classes.
- View persistent volumes. See View persistent volumes.
- Remove Kubernetes clusters from the workspace. See Remove clusters.
- Activate or view Cloud Backup. See Use NetApp cloud data services.

Install Astra Trident

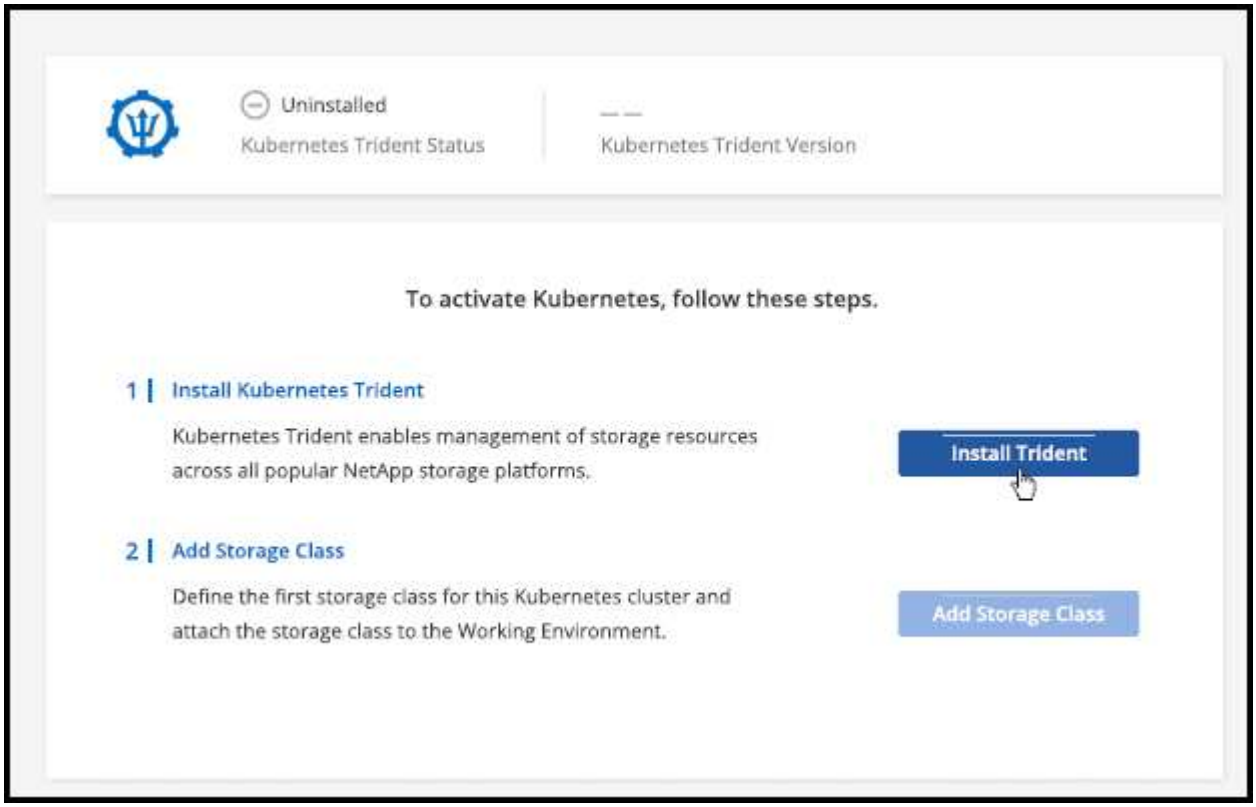
After you add a managed-Kubernetes cluster to the Canvas, you can use Cloud Manager to confirm a compatible Astra Trident installation or install Astra Trident. One of the four most recent versions of Astra Trident is required.

To learn more about Astra Trident, see Astra Trident documentation.

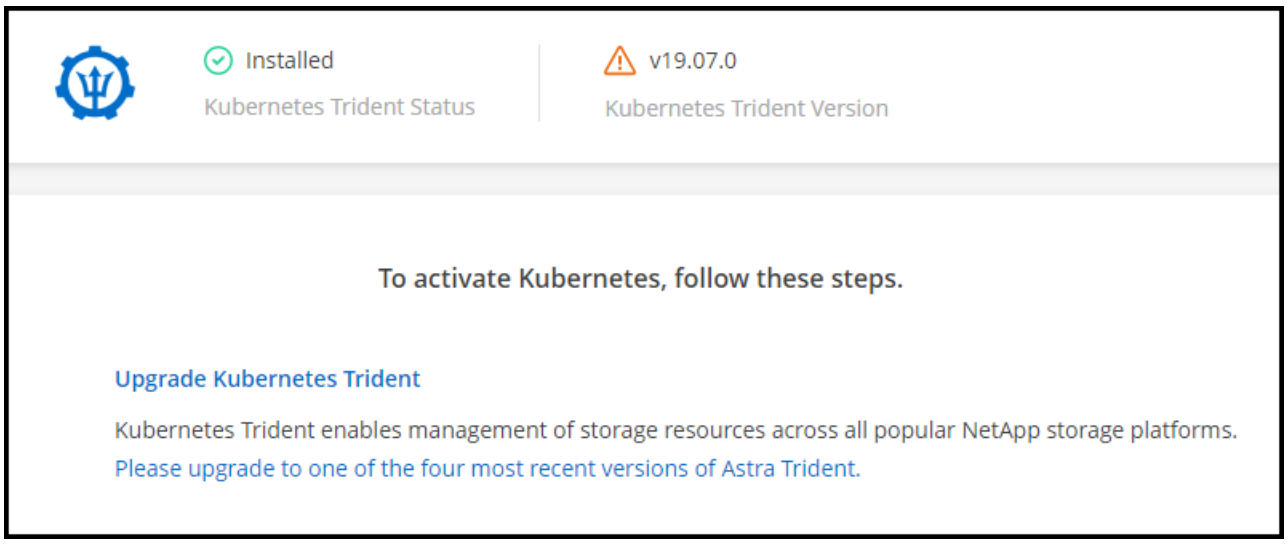
If Astra Trident is not installed, or an incompatible version of Astra Trident is installed, the cluster will show there is an action required.

Steps

1. Double-click the Kubernetes working environment on the Canvas or click **Enter Working Environment**.
   a. If Astra Trident is not installed, click **Install Trident**.



   b. If a back level version of Astra Trident is installed, go to the Astra Trident docs for upgrade steps.



Results

The latest version of Astra Trident is installed. You can now add storage classes.

Manage storage classes

After you add a managed-Kubernetes cluster to the Canvas, you can use Cloud Manager

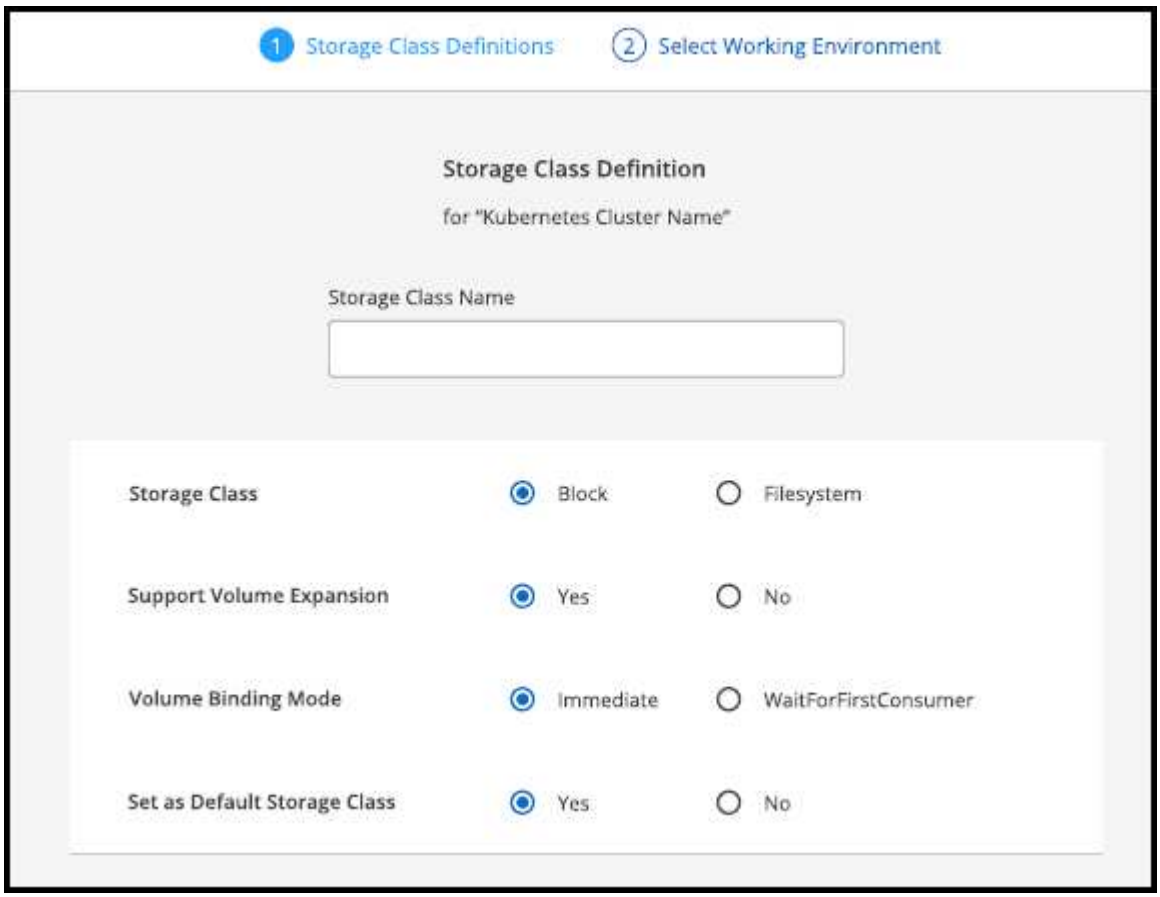
to manage storage classes.

If no storage class is defined, the cluster will show there is an action required. Double-clicking the cluster on the Canvas will open the action page to add a storage class.

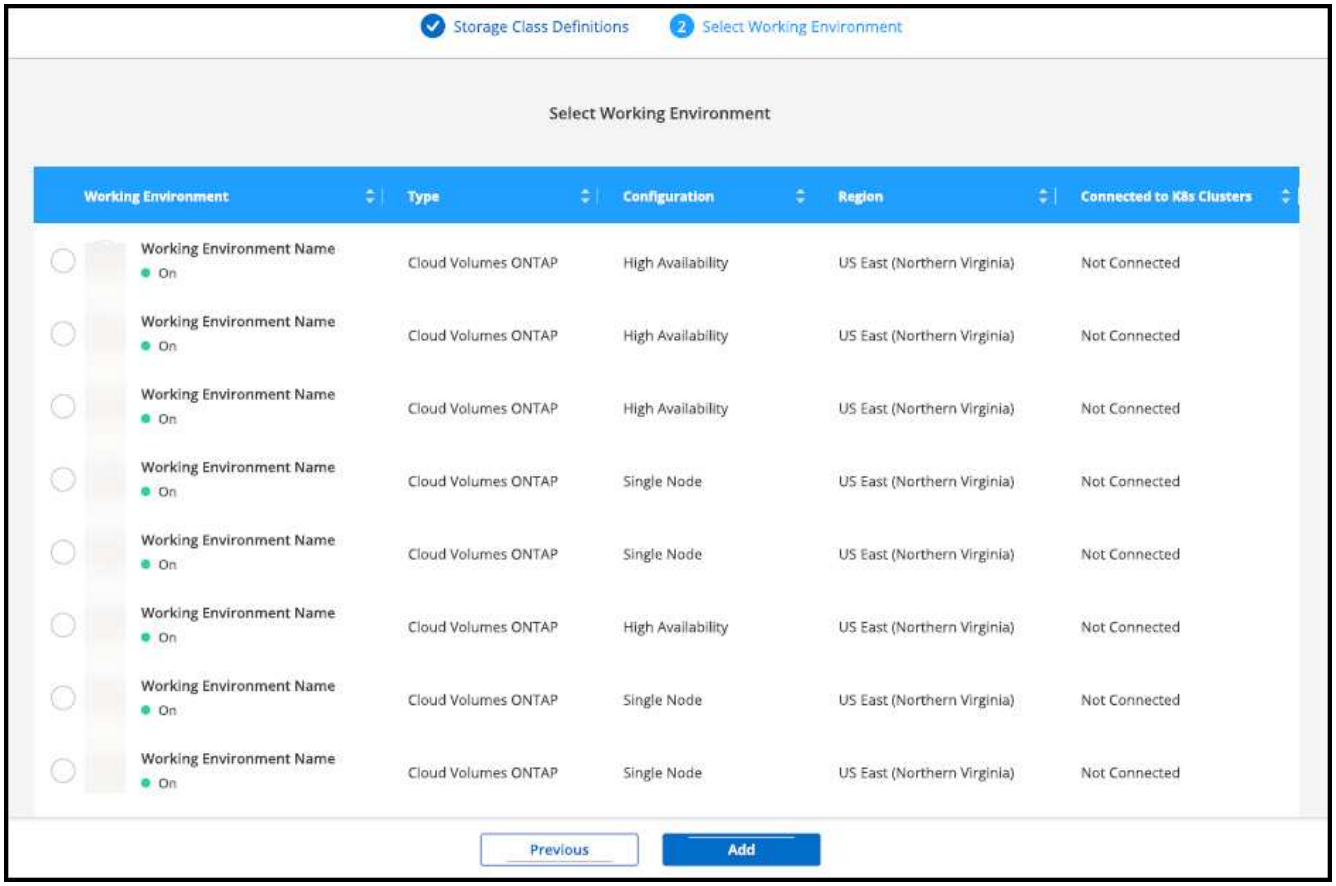
Add storage class

Steps

1. From the Canvas, drag and drop the Kubernetes working environment on the Cloud Volumes ONTAP working environment to open the storage class wizard.
2. Provide a name for the storage class, select definition options, and click **Next**.

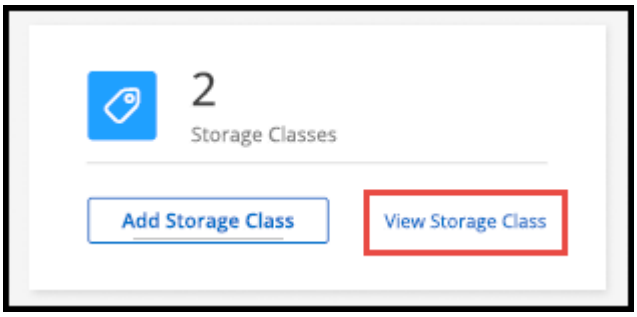


3. Select a working environment to connect to the cluster. Click **Add**.



Results

You can click to view the storage class from the resource page for the Kubernetes cluster.



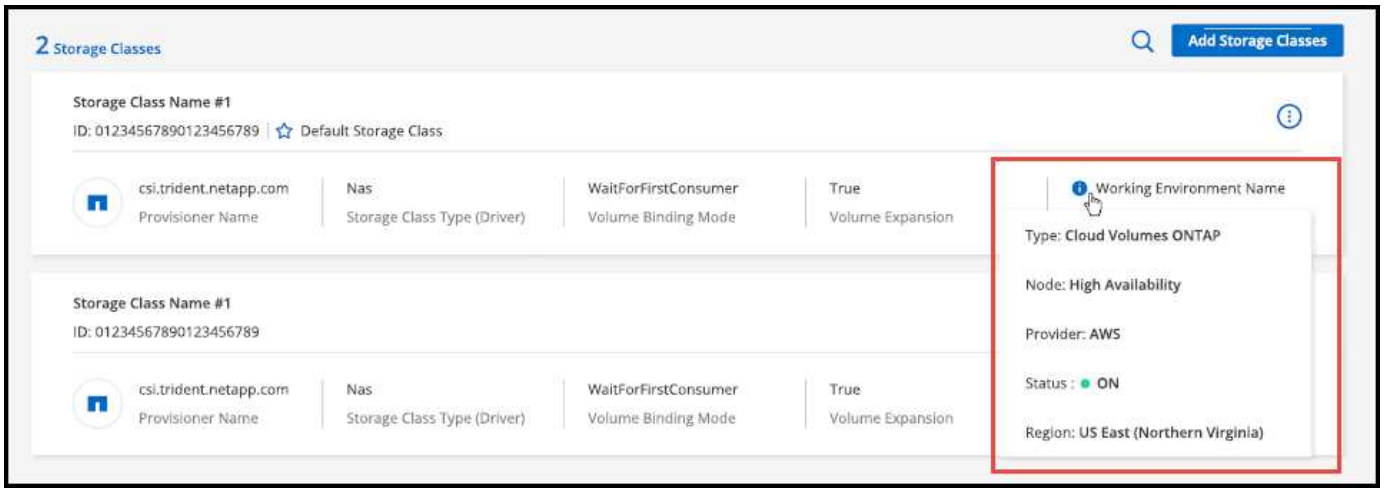
View working environment details

Steps

1. Double-click the Kubernetes working environment on the Canvas or click **Enter Working Environment**.
2. Click the **Storage Classes** tab.
3. Click the information icon to view details for the working environment.

Results

The working environment details panel opens.



Set default storage class

Steps

1. Double-click the Kubernetes working environment on the Canvas or click **Enter Working Environment**.
2. Click the **Storage Classes** tab.
3. Click the action menu for the storage class and click **Set as Default**.

Results

The selected storage class is set as the default.

Remove storage class

Steps

1. Double-click the Kubernetes working environment on the Canvas or click **Enter Working Environment**.
2. Click the **Storage Classes** tab.
3. Click the action menu for the storage class and click **Set as Default**.

4. Click **Remove** to confirm removal of the storage class.

Results

The selected storage class is removed.

View persistent volumes

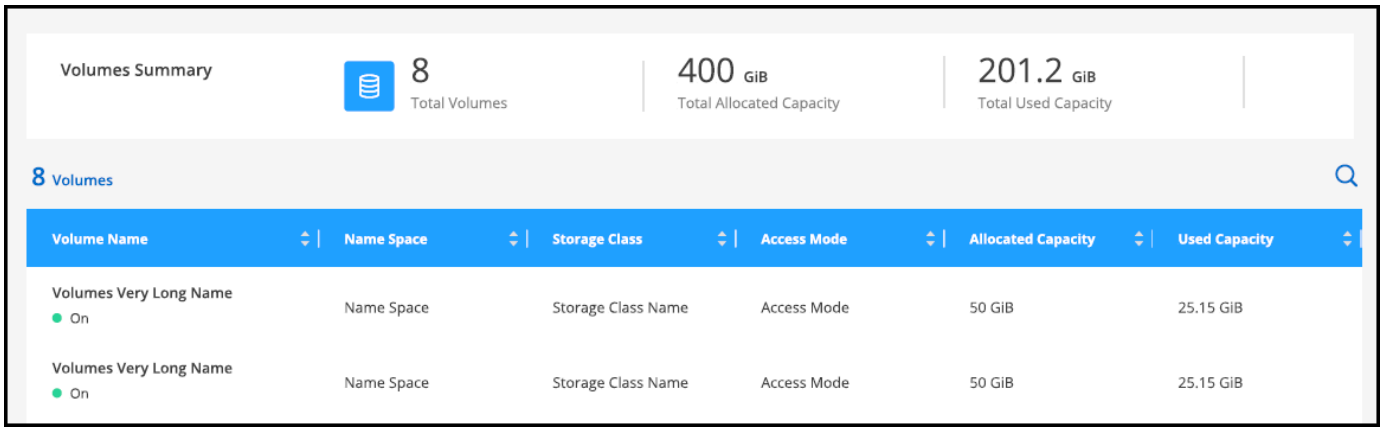
After you add a managed-Kubernetes cluster to the Canvas, you can use Cloud Manager to view persistent volumes.

Steps

1. Double-click the Kubernetes working environment on the Canvas or click **Enter Working Environment**.
2. Click **View Volumes** from the **Overview** tab or click the **Persistent Volumes** tab. If no persistent volumes are configured, see Provisioning for details on provisioning volumes in Astra Trident.

Results

A table of the configured persistent volumes displays.

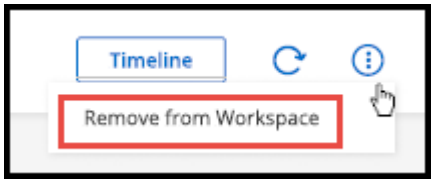


Remove Kubernetes clusters from the workspace

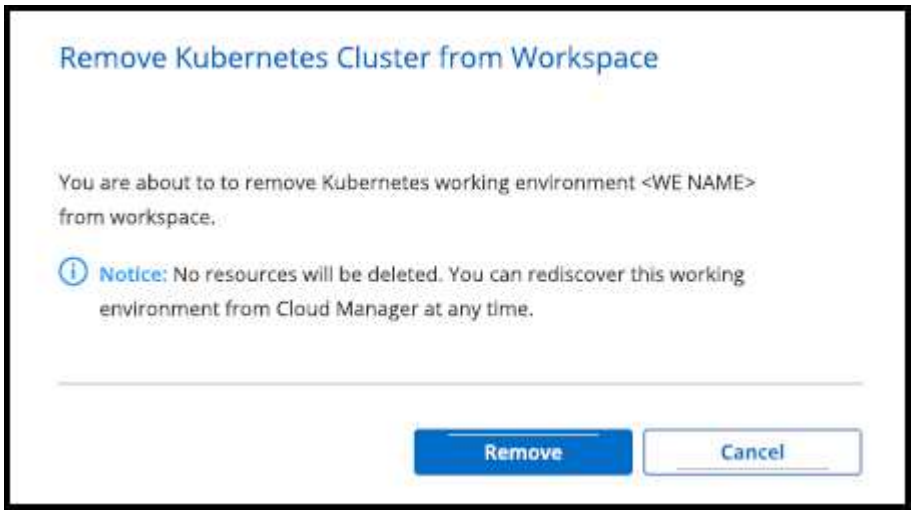
After you add a managed-Kubernetes cluster to the Canvas, you can use Cloud Manager to remove clusters from the workspace.

Steps

1. Double-click the Kubernetes working environment on the Canvas or click **Enter Working Environment**.
2. At the top right of the page, select the actions menu and click **Remove from Workspace**.



3. Click **Remove** to confirm removal of the cluster from the workspace. You can rediscover this cluster at any time.



Results

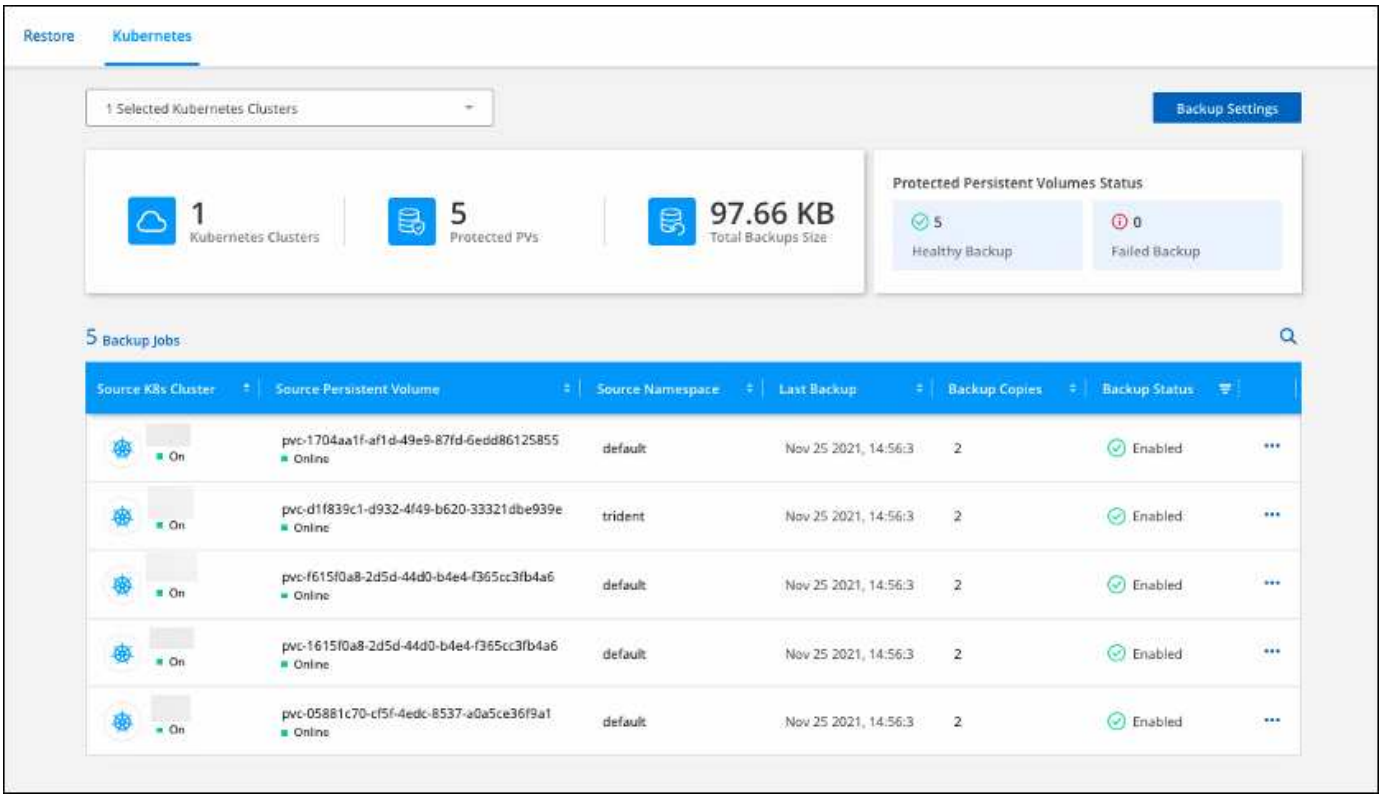
The Kubernetes cluster is removed from the workspace and is no longer visible on the Canvas.

Use NetApp cloud data services with Kubernetes clusters

After you add a managed-Kubernetes cluster to the Canvas, you can use NetApp cloud data services for advanced data management.

At this time, Cloud Backup is supported with Kubernetes clusters. You can use Cloud Backup to back up persistent volumes to object storage.

Learn how to protect your Kubernetes cluster data using Cloud Backup.


Restore
Kubernetes
1 Selected Kubernetes Clusters
Backup Settings
1
Kubernetes Clusters
5
Protected PVs
97.66 KB
Total Backups Size
Protected Persistent Volumes Status
5
Healthy Backup
0
Failed Backup
5 Backup Jobs
Source K8s Cluster
Source Persistent Volume
Source Namespace
Last Backup
Backup Copies
Backup Status
On
pvc-1704aa1f-af1d-49e9-87fd-6edd86125855
Online
default
Nov 25 2021, 14:56:3
2
Enabled
On
pvc-d1f839c1-d932-4f49-b620-33321dbe939e
Online
trident
Nov 25 2021, 14:56:3
2
Enabled
On
pvc-f615f0a8-2d5d-44d0-b4e4-f365cc3fb4a6
Online
default
Nov 25 2021, 14:56:3
2
Enabled
On
pvc-1615f0a8-2d5d-44d0-b4e4-f365cc3fb4a6
Online
default
Nov 25 2021, 14:56:3
2
Enabled
On
pvc-05881c70-cf5f-4edc-8537-a0a5ce36f9a1
Online
default
Nov 25 2021, 14:56:3
2
Enabled

Knowledge and support

Register for support

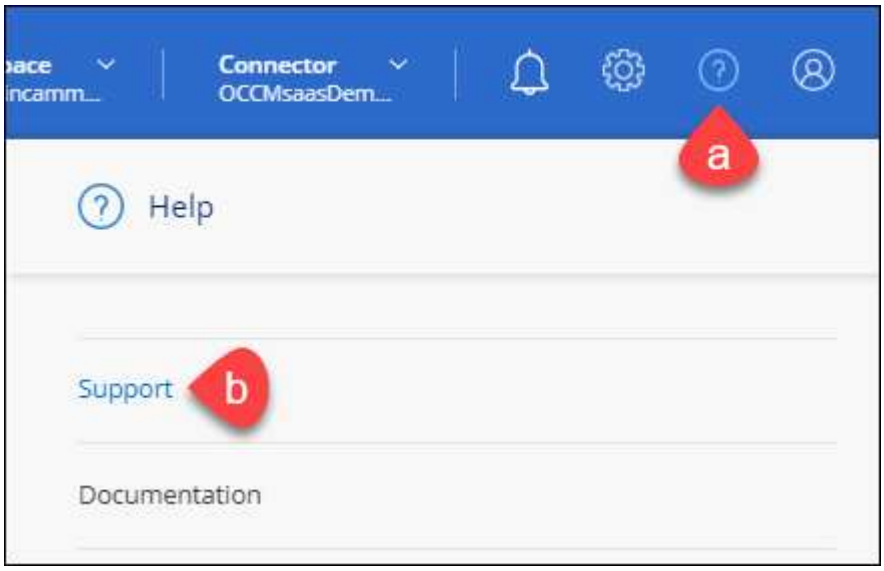
Before you can open a support case with NetApp technical support, you need to add a NetApp Support Site account to Cloud Manager and then register for support.

Add an NSS account

The Support Dashboard enables you to add and manage all of your NetApp Support Site accounts from a single location.

Steps

1. If you don't have a NetApp Support Site account yet, register for one.
2. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.



3. Click **NSS Management > Add NSS Account**.
4. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

5. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

   This action enables Cloud Manager to use your NSS account.

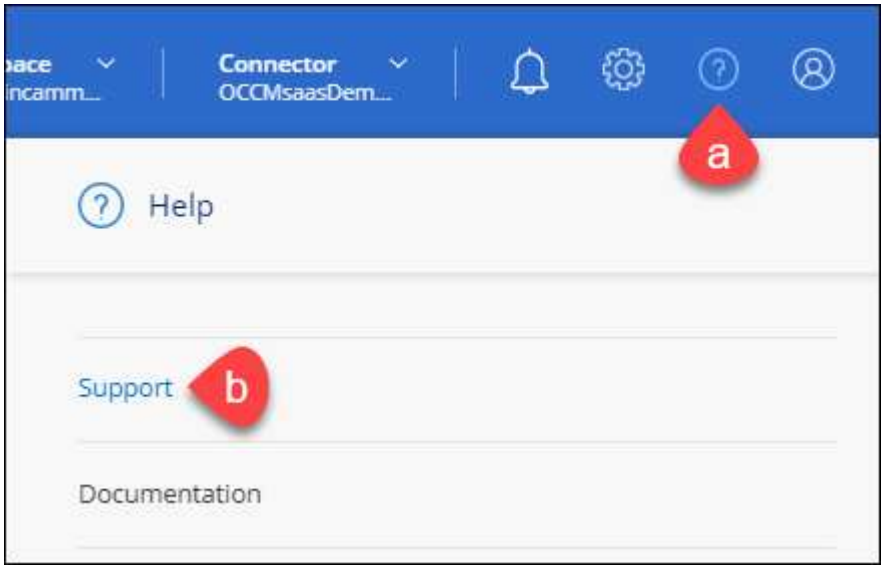
   Note the account must be a customer-level account (not a guest or temp account).

Register your account for support

Support registration is available from Cloud Manager in the Support Dashboard.

Steps

1. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.



2. In the **Resources** tab, click **Register for Support**.
3. Select the NSS credentials that you want to register and then click **Register**.

Get help

NetApp provides support for Cloud Manager and its cloud services in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Self support

These options are available for free, 24 hours a day, 7 days a week:

- Knowledge base

  Search through the Cloud Manager knowledge base to find helpful articles to troubleshoot issues.

- Communities

  Join the Cloud Manager community to follow ongoing discussions or create new ones.

- Documentation

  The Cloud Manager documentation that you're currently viewing.

- Feedback email

  We value your input. Submit feedback to help us improve Cloud Manager.

NetApp support

In addition to the self-support options above, you can work with a NetApp Support Engineer to resolve any issues after you activate support.

Steps

1. In Cloud Manager, click **Help > Support**.
2. Choose one of the available options under Technical Support:
   a. Click **Call Us** to find phone numbers for NetApp technical support.
   b. Click **Open an Issue**, select one the options, and then click **Send**.

      A NetApp representative will review your case and get back to you soon.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- Notice for Cloud Manager 3.9
- Notice for the Cloud Backup

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.