Kubernetes clusters documentation

Kubernetes clusters

NetApp
April 16, 2024

Table of Contents

Kubernetes clusters documentation

What’s new with Kubernetes in BlueXP

Learn what’s new with Kubernetes in BlueXP.

02 April 2023

- You can now uninstall Astra Trident that was installed using the Trident operator or BlueXP.
- User interface improvements have been made and screenshots have been updated in the documentation.

05 March 2023

- Kubernetes in BlueXP now supports Astra Trident 23.01.
- User interface improvements have been made and screenshots have been updated in the documentation.

06 November 2022

When defining storage classes, you can now enable storage class economy for block or filesystem storage.

18 September 2022

You can now import self-managed OpenShift clusters into Cloud Manager.

- Requirements for Kubernetes clusters in OpenShift
- Import an OpenShift cluster to Cloud Manager

31 July 2022

- Using the new `– watch` verb in the storage class and backup and restore YAML configurations, Cloud Manager can now monitor Kubernetes clusters for changes made to the cluster backend and automatically enable backup for new persistent volumes if automatic backup was configured on the cluster.

  Requirements for Kubernetes clusters in AWS

  Requirements for Kubernetes clusters in Azure

  Requirements for Kubernetes clusters in Google Cloud

- When defining storage classes, you can now specify a file system type (fstype) for block storage.

3 July 2022

- If Astra Trident was deployed using the Trident operator, you can now upgrade to the latest version of Astra Trident using Cloud Manager.

  Install and manage Astra Trident

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

Add storage class

6 June 2022

Cloud Manager now supports Amazon FSx for ONTAP as backend storage.

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 BlueXP

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

Using BlueXP and a compatible version of Astra Trident deployed using the Trident operator, you can:

- Add and manage Kubernetes clusters
- Install, upgrade, or uninstall Astra Trident
- Add and remove storage classes
- View persistent volumes
- Remove Kubernetes clusters from the workspace
- Activate or view BlueXP backup and recovery

Supported Kubernetes deployments

BlueXP 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 deployed using the Trident operator is required.

ⓘ Astra Trident deployed using `tridentctl` is not supported. If you deployed Astra Trident using `tridentctl`, you cannot use BlueXP to manage your Kubernetes clusters. You must uninstall using `tridentctl` and reinstall using the Trident operator or using BlueXP.

You can install Astra Trident or upgrade to a supported version directly from BlueXP.

Review Astra Trident prerequisites

Supported backend storage

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

Cost

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

Get started with Kubernetes clusters

Using BlueXP you can start managing Kubernetes clusters in just a few steps.

1 **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

2 **Add your Kubernetes clusters to BlueXP**

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

Add an Amazon Kubernetes cluster

Add an Azure Kubernetes cluster

Add a Google Cloud Kubernetes cluster

3 **Start provisioning Persistent Volumes**

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

Learn more about provisioning your first volume with Astra Trident.

4 **Manage your clusters using BlueXP**

After adding Kubernetes clusters to BlueXP, you can manage the clusters from the BlueXP 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 BlueXP. Before you can add the clusters to BlueXP, 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 or upgrade Astra Trident directly from BlueXP. You should review the prerequisites prior to installing Astra Trident.

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.

BlueXP 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 BlueXP Connector role must be authorized on each Kubernetes cluster. Learn more below.

Prepare a Connector

A BlueXP 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.

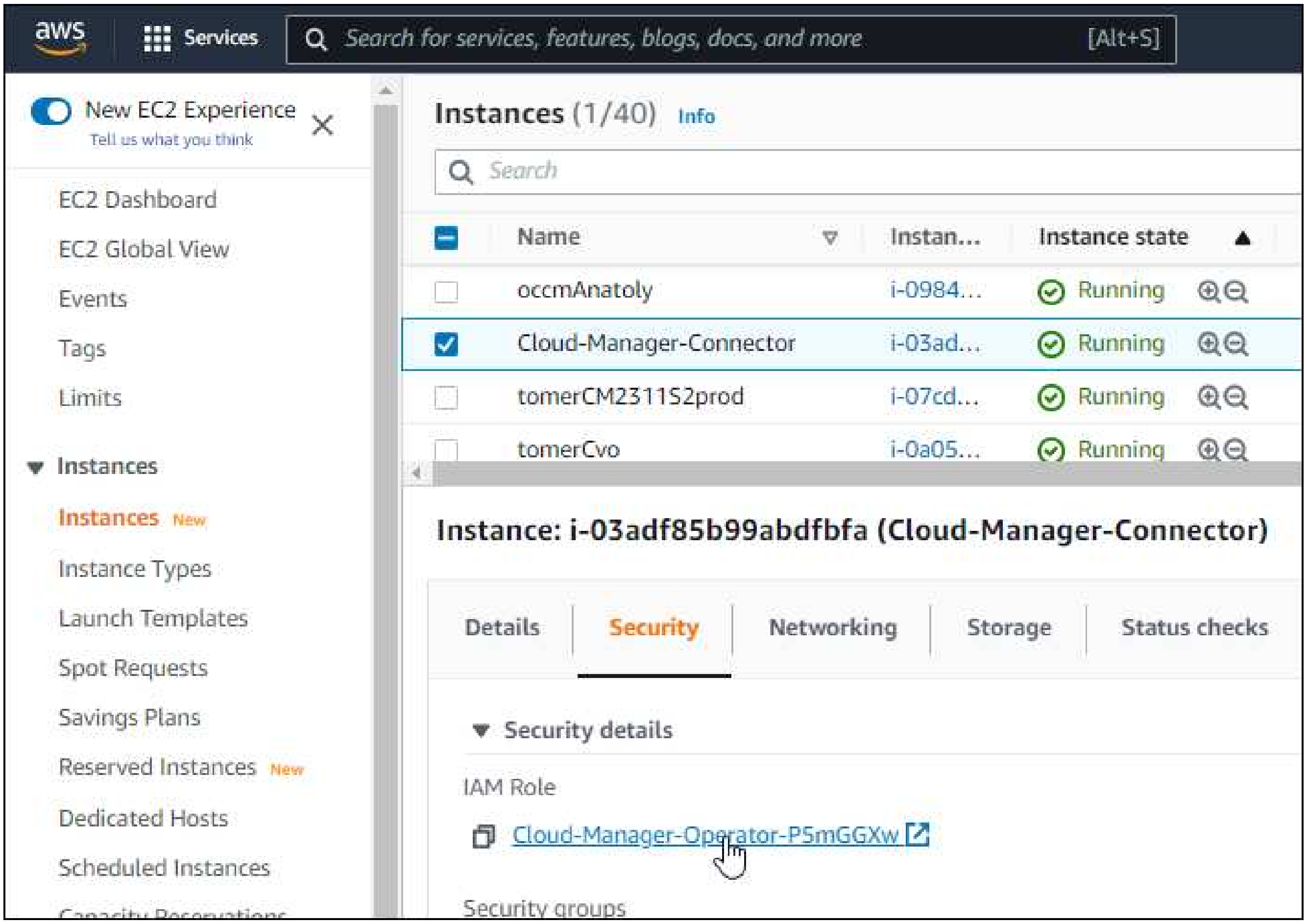
- Create a Connector from BlueXP (recommended)
- Create a Connector from the AWS Marketplace
- Install the Connector on an existing Linux host in AWS

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.



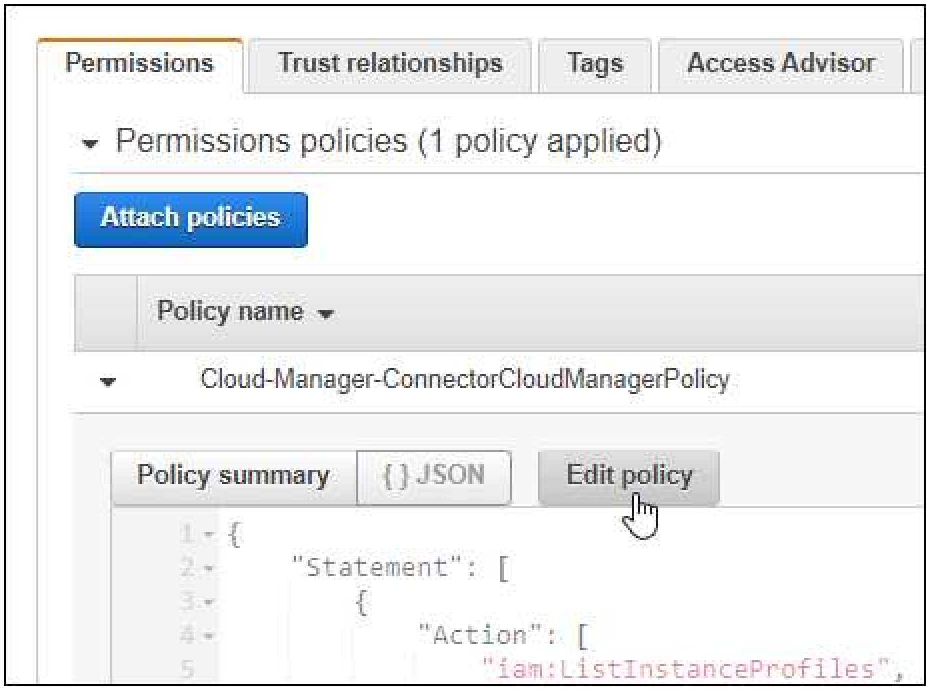
Name	Instan...	Instance state
occmAnatoly	i-0984...	Running
Cloud-Manager-Connector	i-03ad...	Running
tomerCM2311S2prod	i-07cd...	Running
tomerCvo	i-0a05...	Running

Instance: i-03adf85b99abdfbfa (Cloud-Manager-Connector)

IAM Role

Cloud-Manager-Operator-PSmGGXw

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



```
{
    "Statement": [
        {
            "Action": [
                "iam:ListInstanceProfiles",
```

4. Click **JSON** and add the following permissions under the first set of actions:
    - ec2:DescribeRegions
    - eks:ListClusters
    - eks:DescribeCluster
    - iam:GetInstanceProfile

    View the full JSON format for the policy

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

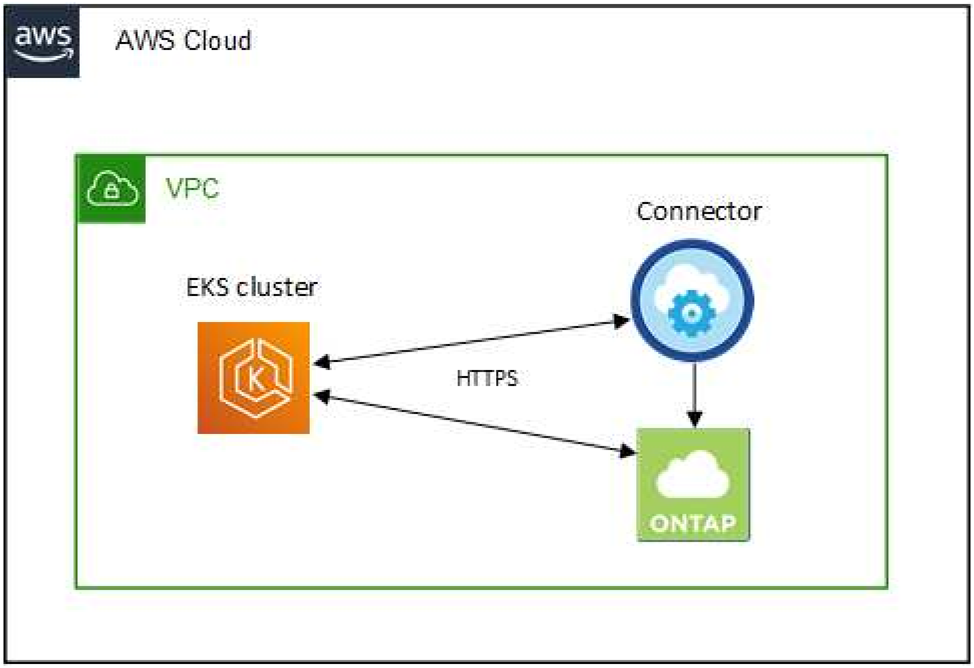
Review networking requirements

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.

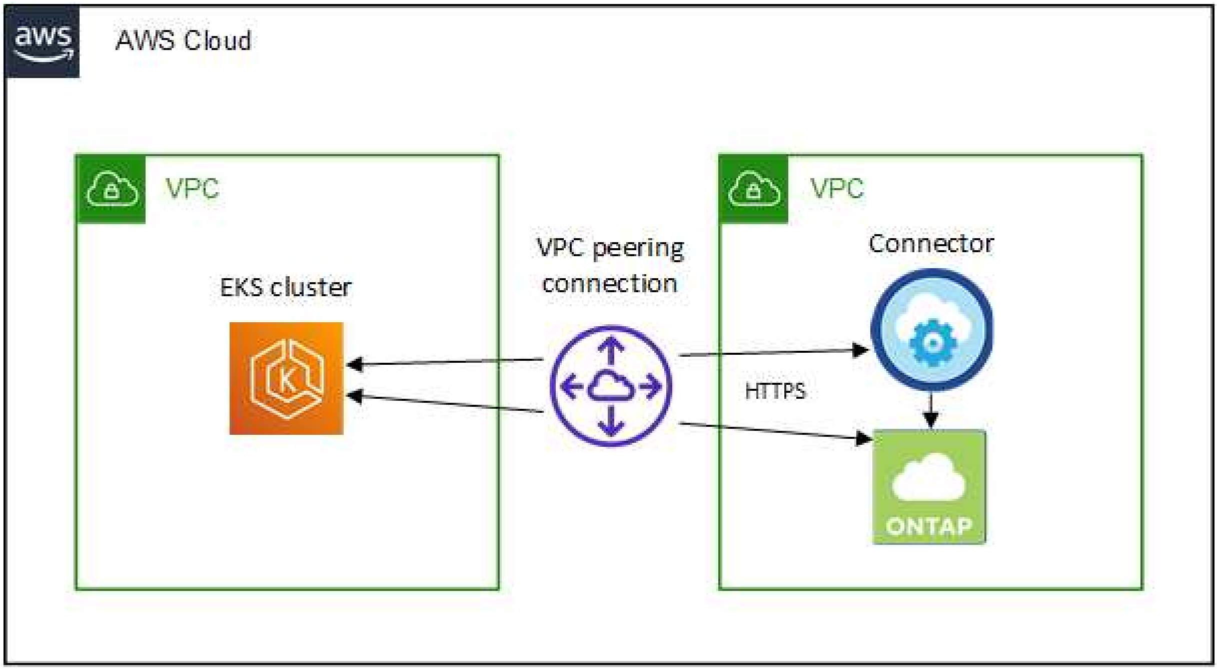
- Each Kubernetes cluster must have an inbound connection from the Connector
- The Connector must have an outbound connection to each Kubernetes cluster over port 443

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 BlueXP and monitor the cluster for changes to the backend.

Install Astra trident

You need to provide full authorization for BlueXP to install Astra Trident.

> ⓘ When installing Astra Trident, BlueXP 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. You can customize authorization based on your 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
          - watch
    - apiGroups:
          - ''
      resources:
          - persistentvolumes
      verbs:
          - list
          - watch
    - apiGroups:
          - ''
      resources:
          - pods
          - pods/exec
      verbs:
          - get
          - list
          - watch
    - apiGroups:
          - ''
      resources:
          - persistentvolumeclaims
      verbs:
          - list
          - create
          - watch
    - apiGroups:
          - storage.k8s.io
      resources:
          - storageclasses
      verbs:
          - list
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentbackends
      verbs:
          - list
          - watch
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentorchestrators
      verbs:
          - get
          - watch
---
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 BlueXP.

```
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
          - watch
          - create
          - delete
          - watch
    - apiGroups:
          - storage.k8s.io
      resources:
          - storageclasses
      verbs:
          - get
          - create
          - list
          - watch
          - delete
          - patch
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentbackends
          - tridentorchestrators
          - tridentbackendconfigs
      verbs:
          - get
          - list
          - watch
          - create
          - delete
          - watch
---
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
```

Trident installation

Use the command line to provide full authorization and enable BlueXP 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 BlueXP 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 BlueXP 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 BlueXP. Before you can add the clusters to BlueXP, 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 or upgrade Astra Trident directly from BlueXP. You should review the prerequisites prior to installing Astra Trident.

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.

BlueXP 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

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

Prepare a Connector

A BlueXP 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 BlueXP (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**.

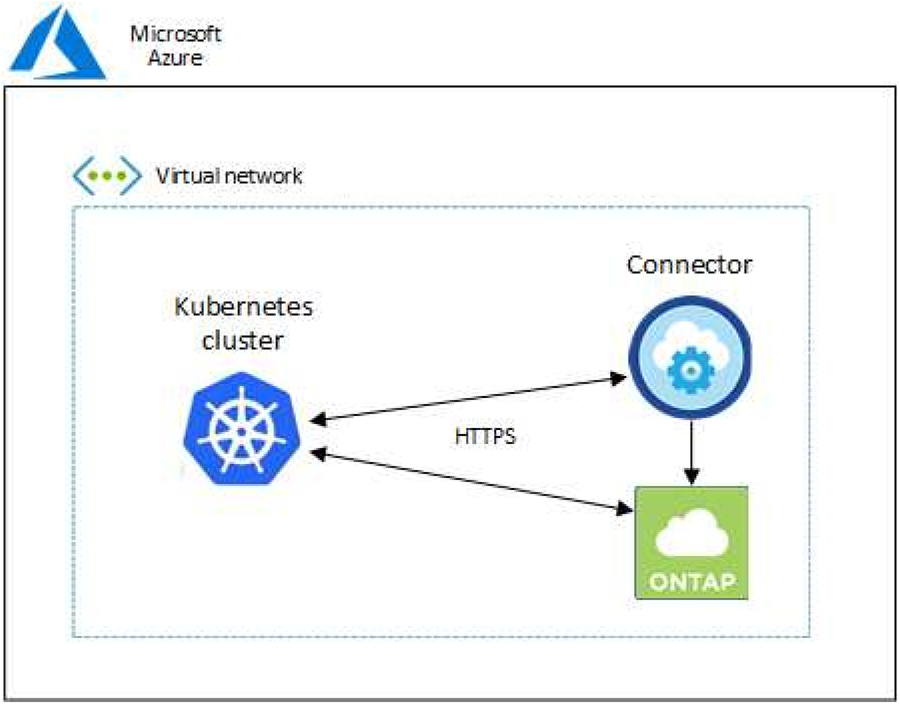
Review networking requirements

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.

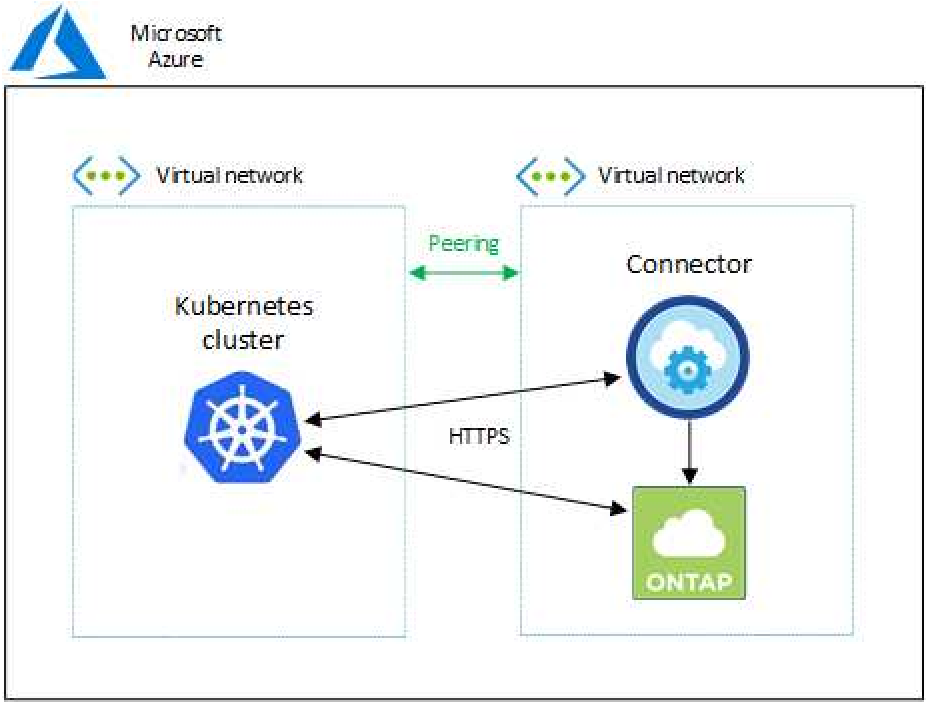
- Each Kubernetes cluster must have an inbound connection from the Connector
- The Connector must have an outbound connection to each Kubernetes cluster over port 443

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 BlueXP and monitor the cluster for changes to the backend.

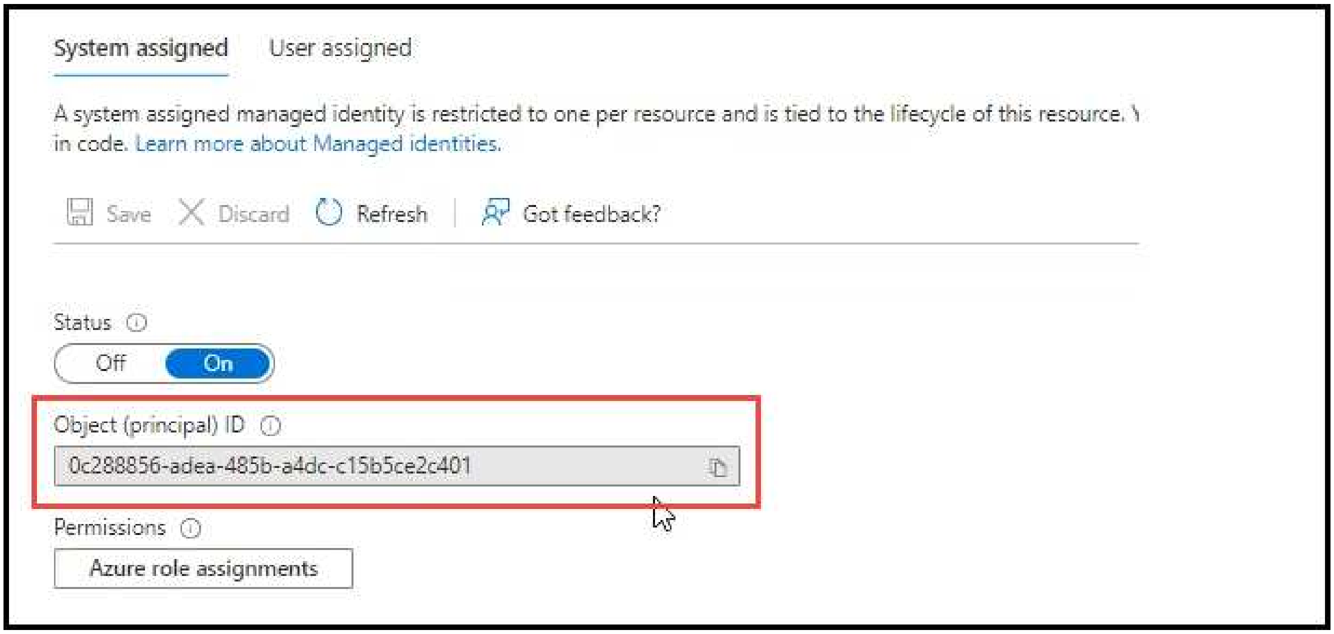
Install Astra trident
: You need to provide full authorization for BlueXP to install Astra Trident.

> ⓘ When installing Astra Trident, BlueXP 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.



System assigned   User assigned

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. Y in code. Learn more about Managed identities.

Status: Off [✓ On]

Object (principal) ID: 0c288856-adea-485b-a4dc-c15b5ce2c401

- 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. You can customize authorization based on your requirements.

Backup/restore

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

Replace the `subjects: kind:` variable with your username and `subjects: name:` with either the Object ID for the system-assigned managed identity or username of any authorized user as described above.

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

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.

```
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
          - watch
          - create
          - delete
          - watch
    - apiGroups:
          - storage.k8s.io
      resources:
          - storageclasses
      verbs:
          - get
          - create
          - list
          - watch
          - delete
          - patch
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentbackends
          - tridentorchestrators
          - tridentbackendconfigs
      verbs:
          - get
          - list
          - watch
          - create
          - delete
          - watch
---
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
```

Trident installation

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

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

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 BlueXP. Before you can add the clusters to BlueXP, 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 or upgrade Astra Trident directly from BlueXP. You should review the prerequisites prior to installing Astra Trident

Cloud Volumes ONTAP

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

BlueXP 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

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

Prepare a Connector

A BlueXP 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 BlueXP (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.

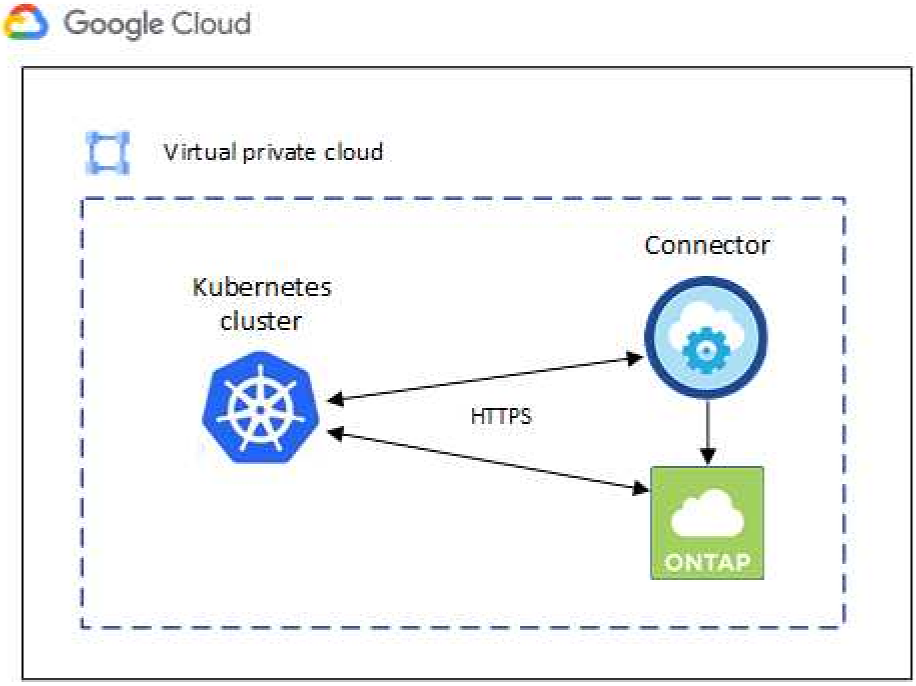
Review networking requirements

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 BlueXP and monitor the cluster for changes to the backend.

Install Astra trident

You need to provide full authorization for BlueXP to install Astra Trident.

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

Before you begin

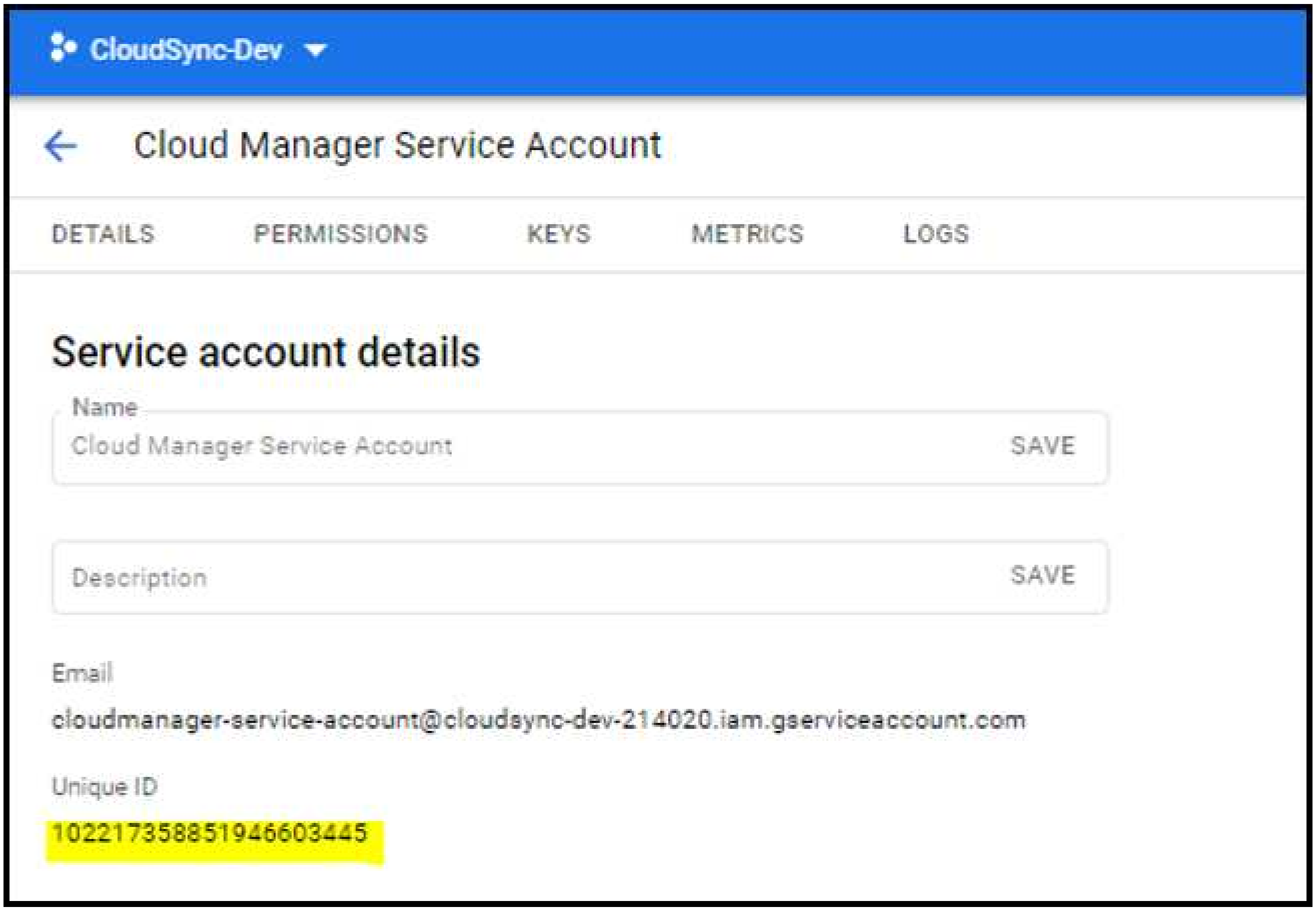
To configure `subjects: name:` in the YAML file, you need to know the BlueXP Unique ID.

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.



Name
Cloud Manager Service Account

Description

Email
cloudmanager-service-account@cloudsync-dev-214020.iam.gserviceaccount.com

Unique ID
102217358851946603445

Steps

Create a cluster role and role binding.

1. You can customize authorization based on your requirements.

Backup/restore

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

Replace the `subjects: kind:` variable with your username and `subjects: name:` with the unique ID for the authorized service account.

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

Replace the `subjects: kind:` variable with your username and `subjects: user:` with the unique ID for the authorized service account.

```
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
          - watch
          - create
          - delete
          - watch
    - apiGroups:
          - storage.k8s.io
      resources:
          - storageclasses
      verbs:
          - get
          - create
          - list
          - watch
          - delete
          - patch
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentbackends
          - tridentorchestrators
          - tridentbackendconfigs
      verbs:
          - get
          - list
          - watch
          - create
          - delete
          - watch
---
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
```

Trident installation

Use the command line to provide full authorization and enable BlueXP 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>
```

Requirements for Kubernetes clusters in OpenShift

You can add and manage self-managed OpenShift Kubernetes clusters using BlueXP. Before you can add the clusters to BlueXP, ensure the following requirements are met.

Requirements

Astra Trident

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

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.

BlueXP Connector

A BlueXP Connector is required to import and manage Kubernetes clusters. You'll need to create a new Connector or use an existing Connector that has the required permissions for your Cloud provider:

- AWS Connector
- Azure Connector
- Google Cloud Connector

Network connectivity

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

Kubernetes configuration file (kubeconfig) with RBAC authorization

To import OpenShift clusters, you need a kubeconfig file with the RBAC authorization required to enable different functionality. Create a kubeconfig file.

- Backup and restore: Backup and restore requires only basic authorization.
- Add storage classes: Expanded authorization is required to add storage classes using BlueXP and monitor the cluster for changes to the backend.
- Install Astra Trident: You need to provide full authorization for BlueXP to install Astra Trident.

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

Create a kubeconfig file

Using the OpenShift CLI, create a kubeconfig file to import to BlueXP.

Steps

1. Log in to the OpenShift CLI using `oc login` on a public URL with an administrative user.
2. Create a service account as follows:
   a. Create a service account file called `oc-service-account.yaml`.

      Adjust the name and namespace as needed. If changes are made here, you should apply the same changes in the following steps.

      ```
      oc-service-account.yaml
      ```

      ```
      apiVersion: v1
      kind: ServiceAccount
      metadata:
        name: oc-service-account
        namespace: default
      ```

   b. Apply the service account:

      ```
      kubectl apply -f oc-service-account.yaml
      ```

3. Create a custom role binding based on your authorization requirements.
   a. Create a `ClusterRoleBinding` file called `oc-clusterrolebinding.yaml`.

      ```
      oc-clusterrolebinding.yaml
      ```

   b. Configure RBAC authorization as needed for your cluster.

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
          - watch
    - apiGroups:
          - ''
      resources:
          - persistentvolumes
      verbs:
          - list
          - watch
    - apiGroups:
          - ''
      resources:
          - pods
          - pods/exec
      verbs:
          - get
          - list
          - watch
    - apiGroups:
          - ''
      resources:
          - persistentvolumeclaims
      verbs:
          - list
          - create
          - watch
    - apiGroups:
          - storage.k8s.io
      resources:
          - storageclasses
      verbs:
          - list
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentbackends
      verbs:
          - list
          - watch
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentorchestrators
      verbs:
          - get
          - watch
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
subjects:
    - kind: ServiceAccount
      name: oc-service-account
      namespace: default
```

Storage classes

Add expanded authorization to add storage classes using BlueXP.

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

Trident installation

Grant full admin authorization and enable BlueXP to install Astra Trident.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cloudmanager-access-clusterrole
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: oc-service-account
  namespace: default
```

c. Apply the cluster role binding:

```
kubectl apply -f oc-clusterrolebinding.yaml
```

4. List the service account secrets, replacing `<context>` with the correct context for your installation:

```
kubectl get serviceaccount oc-service-account --context <context>
--namespace default -o json
```

The end of the output should look similar to the following:

```
"secrets": [
{ "name": "oc-service-account-dockercfg-vhz87"},
{ "name": "oc-service-account-token-r59kr"}
]
```

The indices for each element in the `secrets` array begin with 0. In the above example, the index for `oc-service-account-dockercfg-vhz87` would be 0 and the index for `oc-service-account-token-r59kr` would be 1. In your output, make note of the index for the service account name that has the word "token" in it.

5. Generate the kubeconfig as follows:

a. Create a `create-kubeconfig.sh` file. Replace `TOKEN_INDEX` in the beginning of the following script with the correct value.

```
create-kubeconfig.sh
```

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=oc-service-account
NAMESPACE=default
NEW_CONTEXT=oc
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-context
${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

# Set context to use token user
```

```
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp
```

b. Source the commands to apply them to your Kubernetes cluster.

```
source create-kubeconfig.sh
```

Result

You will use the resulting `kubeconfig-sa` file to add an OpenShift cluster to BlueXP.

Add Kubernetes clusters

Add an Amazon Kubernetes cluster to BlueXP

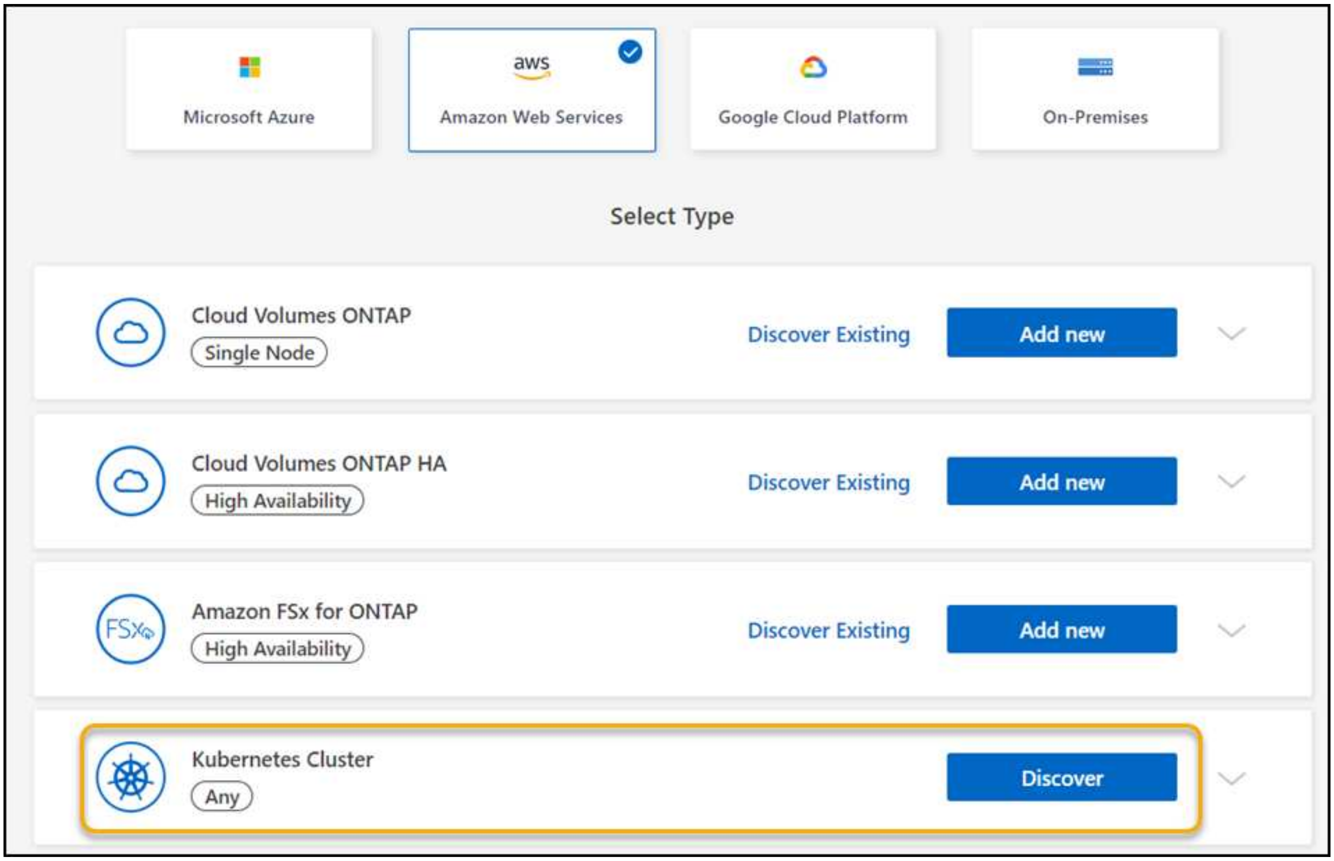
You can discover or import Kubernetes clusters to BlueXP so you can back up persistent volumes to Amazon S3.

Discover a cluster

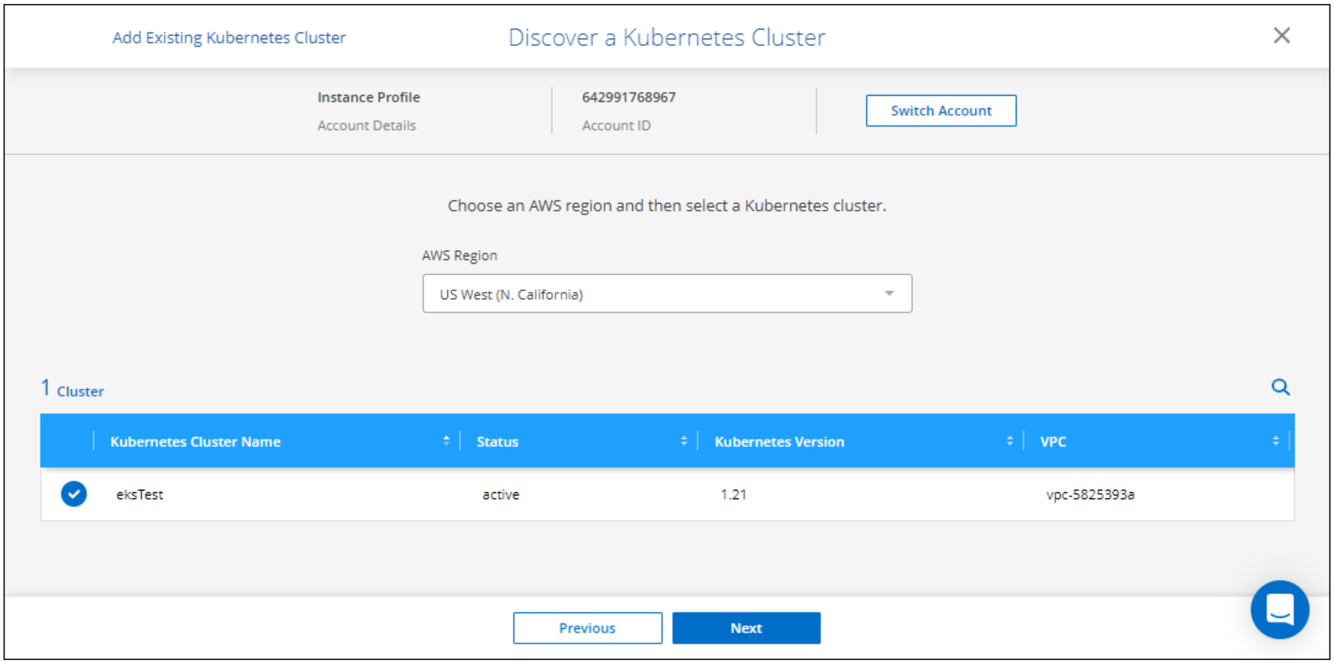
You can discover a fully-managed or self-managed Kubernetes cluster. Managed clusters must be discovered; they cannot be imported.

Steps

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



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



Discover a Kubernetes Cluster

Instance Profile
Account Details

642991768967
Account ID

Choose an AWS region and then select a Kubernetes cluster.

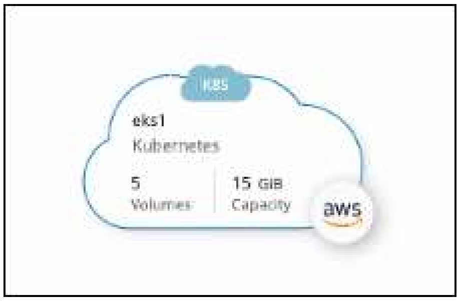
AWS Region: US West (N. California)

1 Cluster

	Kubernetes Cluster Name	Status	Kubernetes Version	VPC
✓	eksTest	active	1.21	vpc-5825393a

Result

BlueXP adds the Kubernetes cluster to the Canvas.

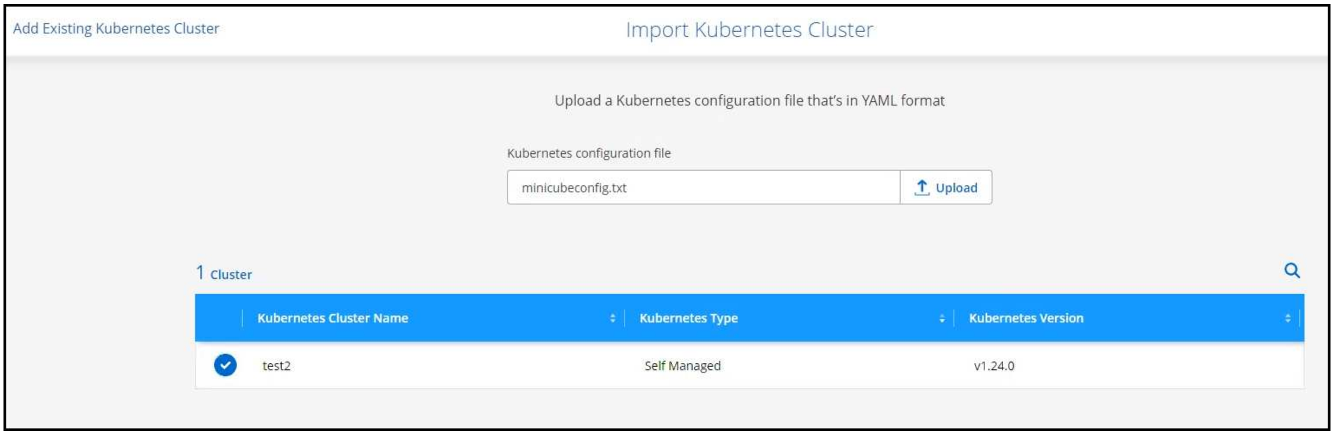


Import a Cluster

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** > **Discover**.
3. Select **Import Cluster** and click **Next**.
4. Upload a Kubernetes configuration file in YAML format.



Upload a Kubernetes configuration file that's in YAML format

Kubernetes configuration file: minicubeconfig.txt

1 Cluster

	Kubernetes Cluster Name	Kubernetes Type	Kubernetes Version
✓	test2	Self Managed	v1.24.0

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

Result

BlueXP adds the Kubernetes cluster to the Canvas.

Add an Azure Kubernetes cluster to BlueXP

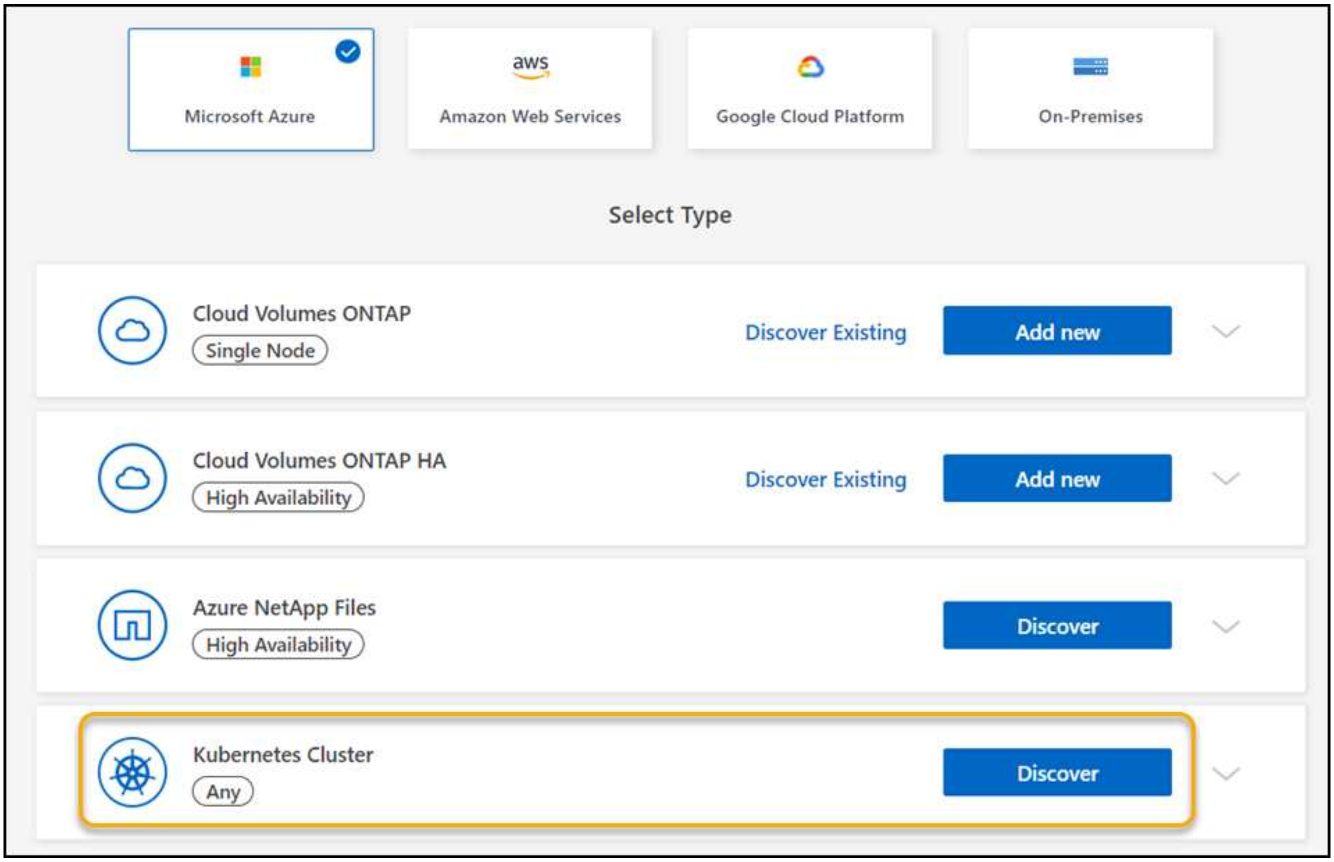
You can discover or import Kubernetes clusters to BlueXP so that you can back up persistent volumes to Azure.

Discover a cluster

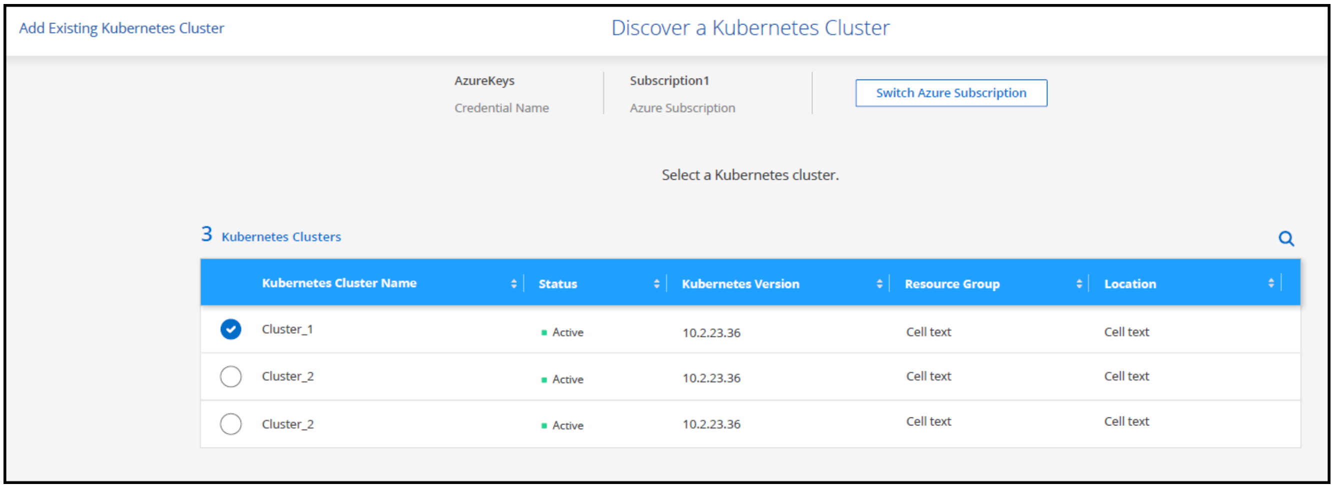
You can discover a fully-managed or self-managed Kubernetes cluster. Managed clusters must be discovered; they cannot be imported.

Steps

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



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


Add Existing Kubernetes Cluster
Discover a Kubernetes Cluster
AzureKeys
Credential Name
Subscription1
Azure Subscription
Switch Azure Subscription

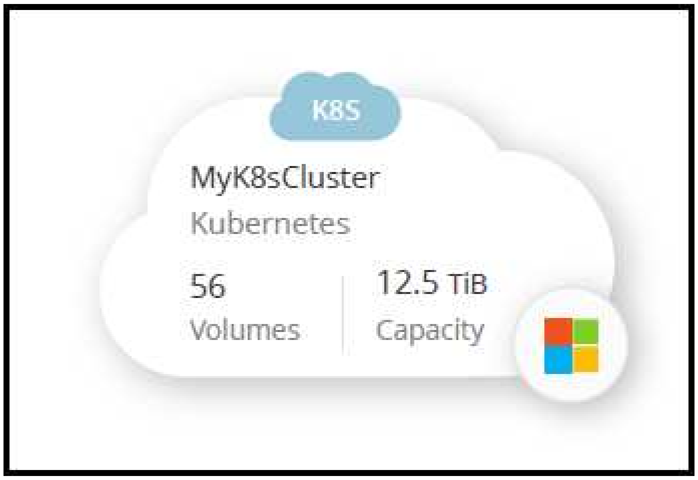
Select a Kubernetes cluster.

3 Kubernetes Clusters

	Kubernetes Cluster Name	Status	Kubernetes Version	Resource Group	Location
●	Cluster_1	Active	10.2.23.36	Cell text	Cell text
○	Cluster_2	Active	10.2.23.36	Cell text	Cell text
○	Cluster_2	Active	10.2.23.36	Cell text	Cell text

Result

BlueXP adds the Kubernetes cluster to the Canvas.



Import a Cluster

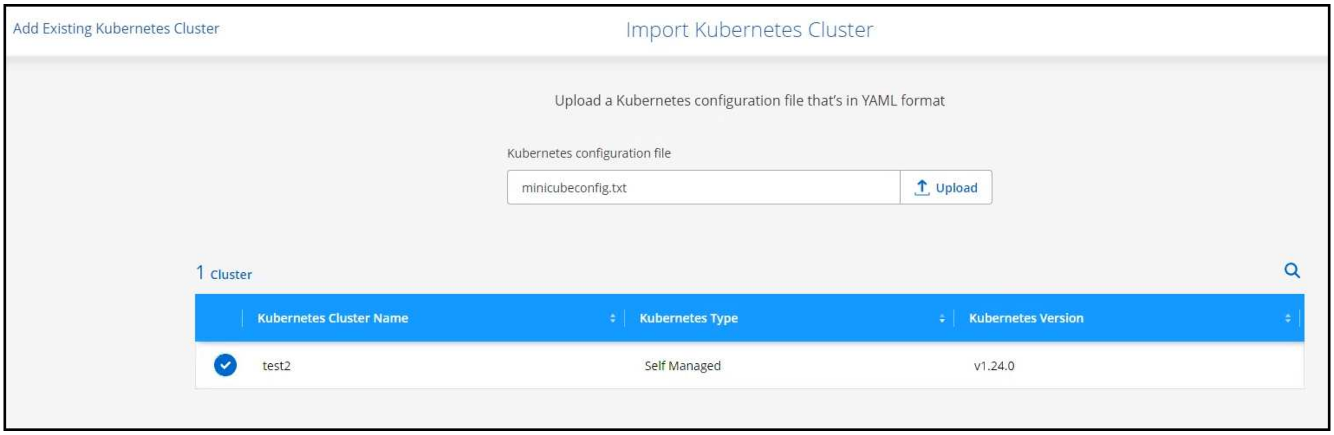
You can import a self-managed Kubernetes cluster using a Kubernetes configuration file.

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** > **Discover**.
3. Select **Import Cluster** and click **Next**.
4. Upload a Kubernetes configuration file in YAML format.



Upload a Kubernetes configuration file that's in YAML format

Kubernetes configuration file: minicubeconfig.txt

1 Cluster

	Kubernetes Cluster Name	Kubernetes Type	Kubernetes Version
✓	test2	Self Managed	v1.24.0

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

Result

BlueXP adds the Kubernetes cluster to the Canvas.

Add a Google Cloud Kubernetes cluster to BlueXP

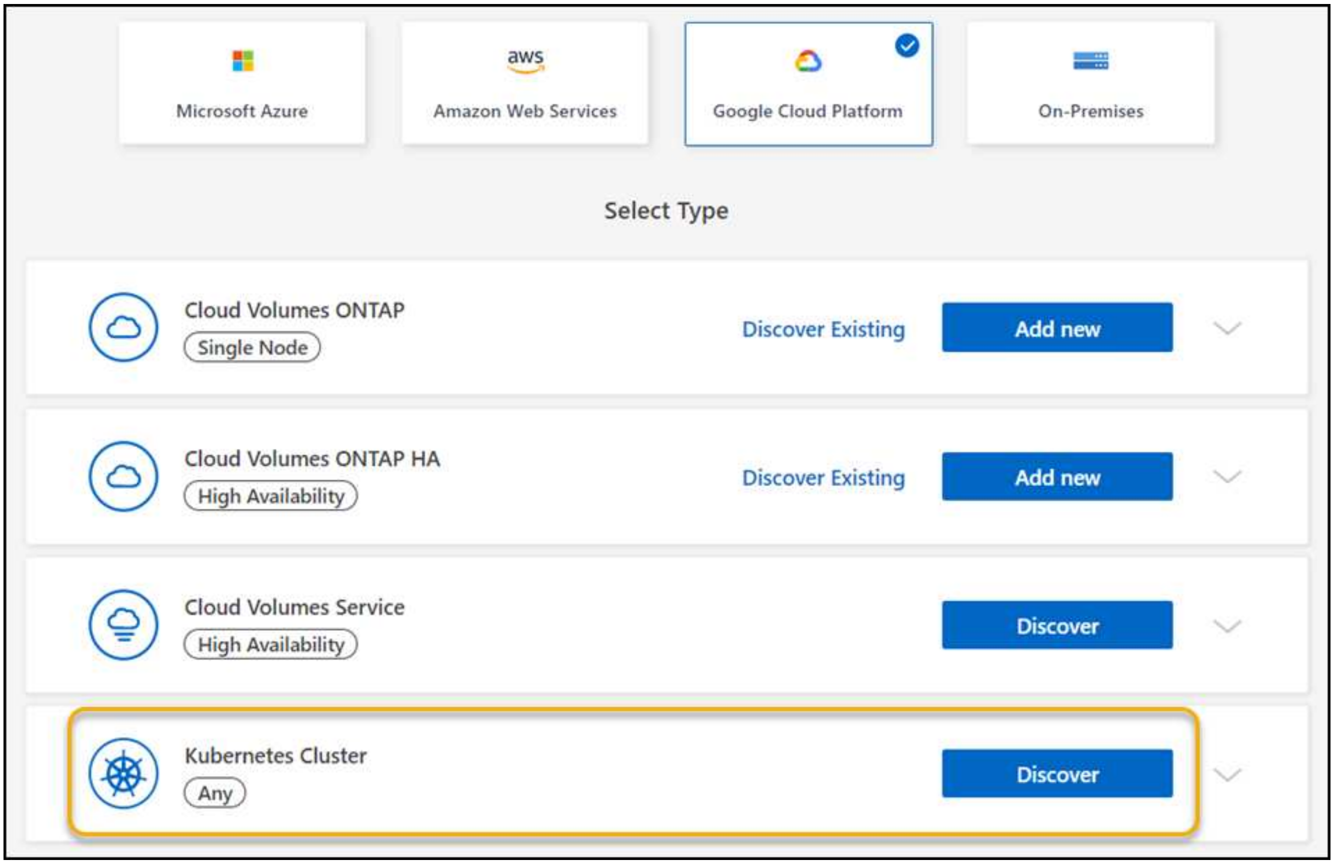
You can discover or import Kubernetes clusters to BlueXP so that you can back up persistent volumes to Google Cloud.

Discover a cluster

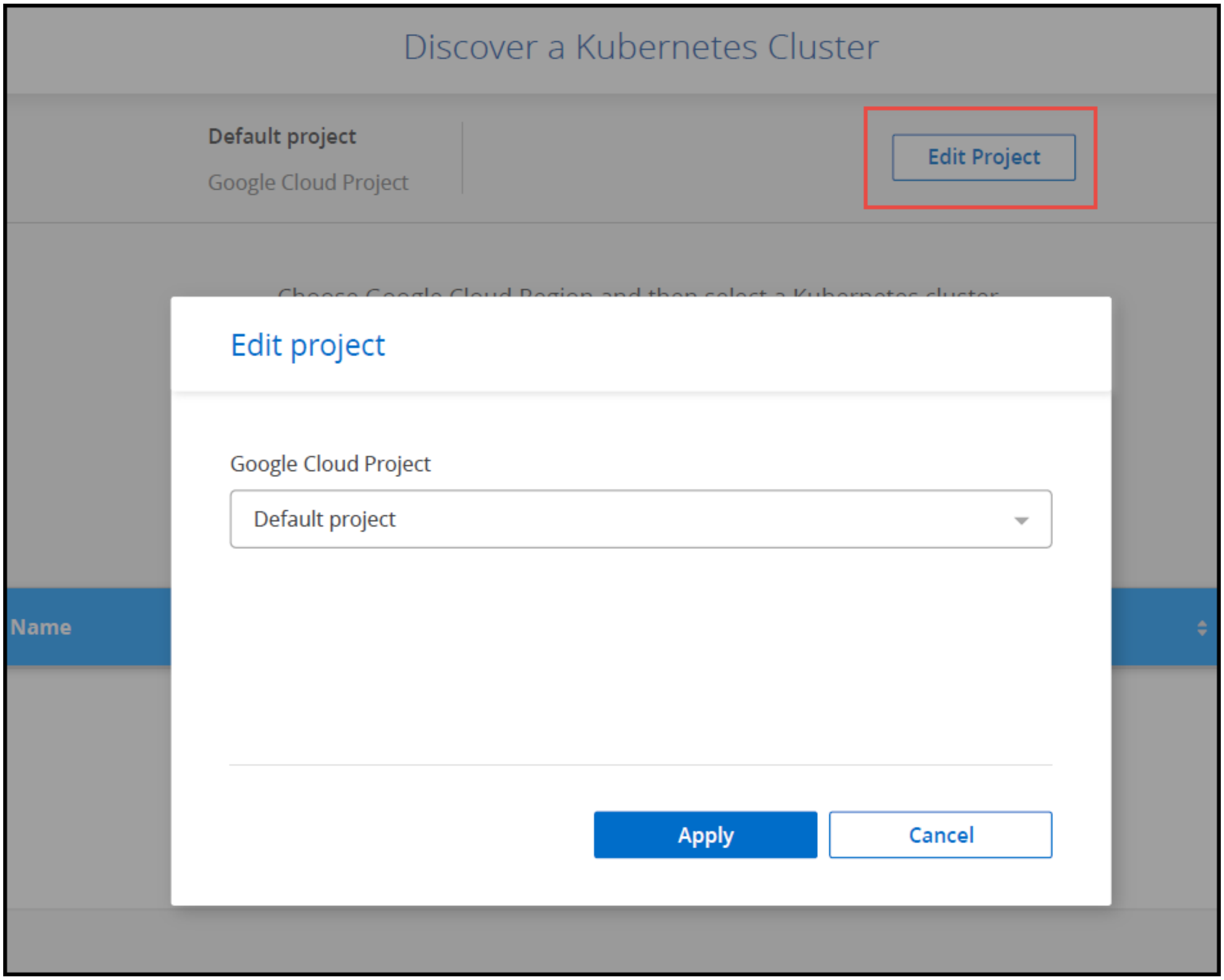
You can discover a fully-managed or self-managed Kubernetes cluster. Managed clusters must be discovered; they cannot be imported.

Steps

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



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.



Discover a Kubernetes Cluster

Default project

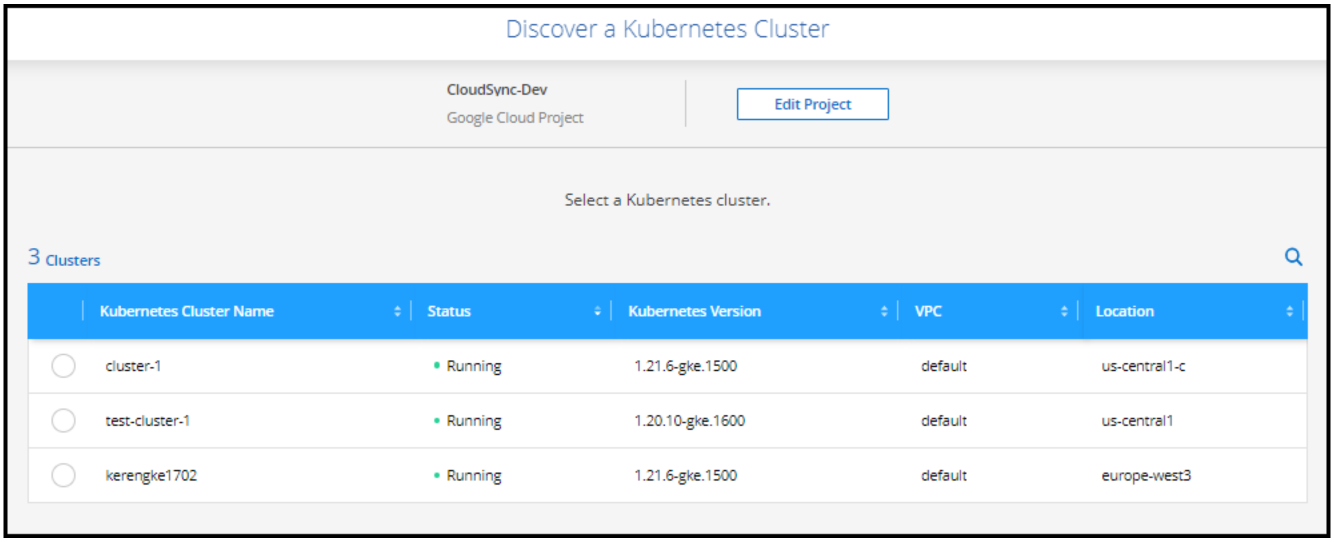
Google Cloud Project

Edit Project
Choose Google Cloud Region and then select a Kubernetes cluster
Name

Edit project

Google Cloud Project: Default project

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



Discover a Kubernetes Cluster

CloudSync-Dev

Google Cloud Project

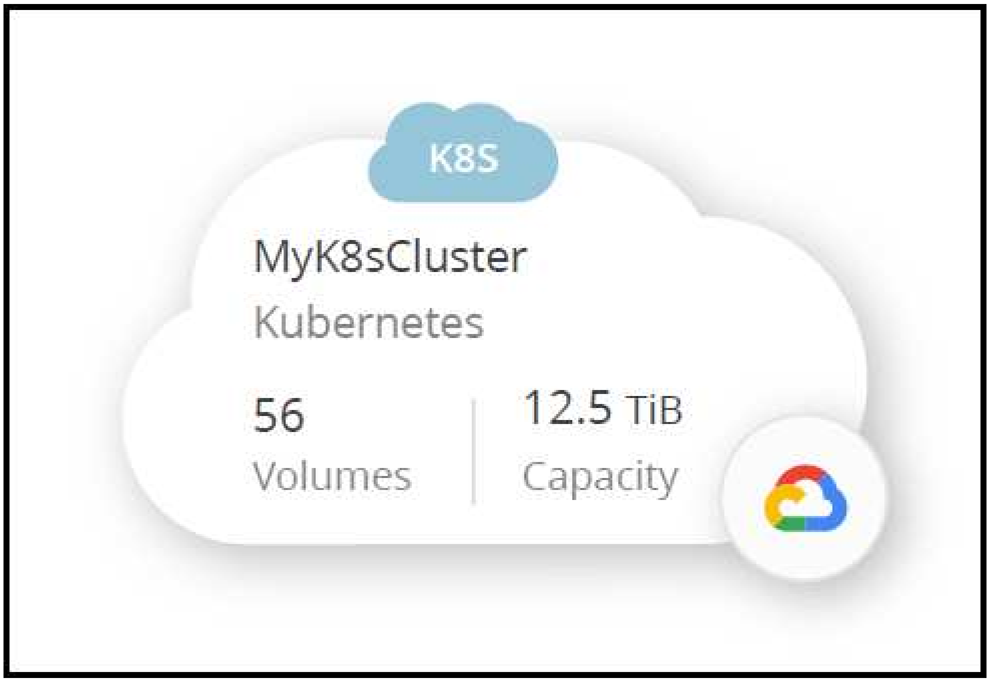
Select a Kubernetes cluster.

3 Clusters

	Kubernetes Cluster Name	Status	Kubernetes Version	VPC	Location
○	cluster-1	• Running	1.21.6-gke.1500	default	us-central1-c
○	test-cluster-1	• Running	1.20.10-gke.1600	default	us-central1
○	kerengke1702	• Running	1.21.6-gke.1500	default	europe-west3

Result

BlueXP adds the Kubernetes cluster to the Canvas.



Import a Cluster

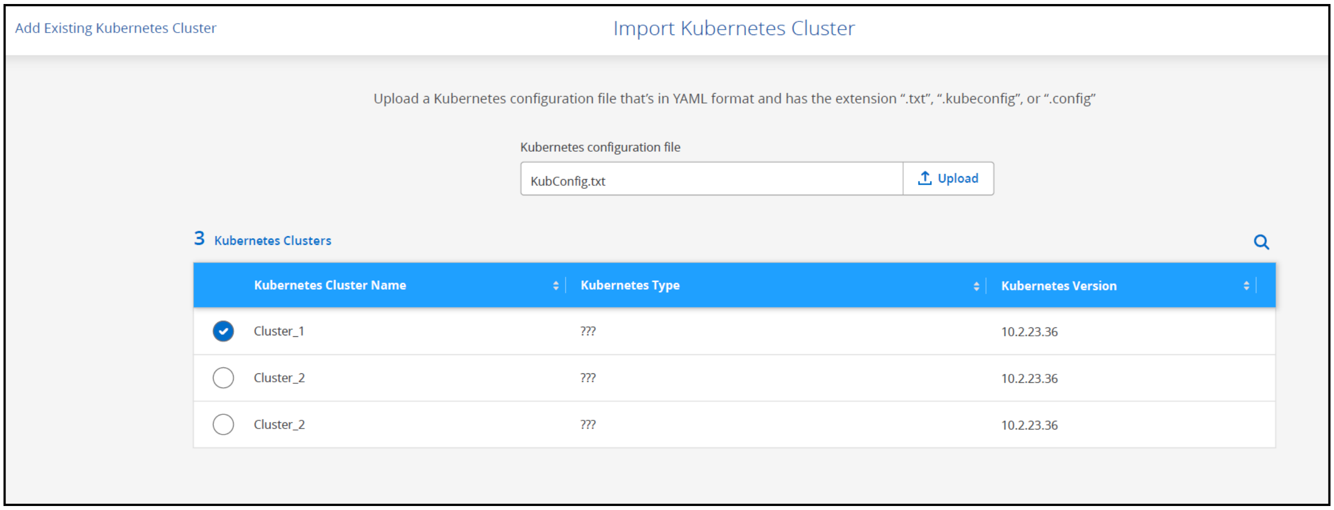
You can import a self-managed Kubernetes cluster using a Kubernetes configuration file.

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** > **Discover**.
3. Select **Import Cluster** and click **Next**.
4. Upload a Kubernetes configuration file in YAML format.



Import Kubernetes Cluster

Upload a Kubernetes configuration file that's in YAML format and has the extension ".txt", ".kubeconfig", or ".config"

Kubernetes configuration file: KubConfig.txt

3 Kubernetes Clusters

	Kubernetes Cluster Name	Kubernetes Type	Kubernetes Version
●	Cluster_1	???	10.2.23.36
○	Cluster_2	???	10.2.23.36
○	Cluster_2	???	10.2.23.36

Result

BlueXP adds the Kubernetes cluster to the Canvas.

Import an OpenShift cluster to BlueXP

Import a self-managed OpenShift cluster to BlueXP so you can start backing up persistent volumes to your Cloud provider.

Import a Cluster

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

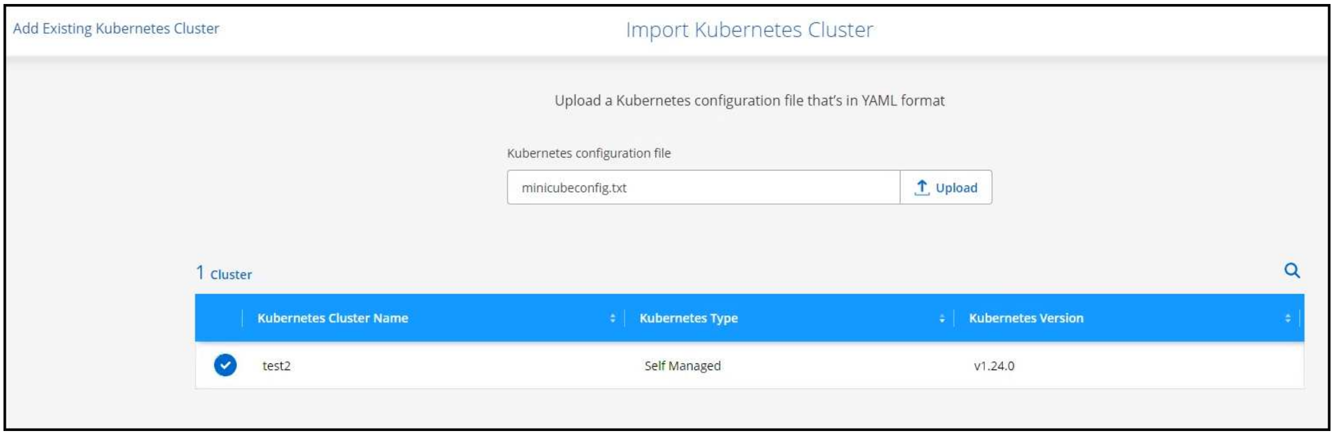
Before you begin

Before importing an OpenShift cluster, you need:

- The `kubeconfig-sa`file you created in create a kubeconfig file.
- The public Certificate Authority (for example, ca.crt), Client Key (for example, tls.key), and Client Certification (for example, tls.crt) files for the cluster.

Steps

1. On the **Canvas**, select **Add Working Environment**.
2. Select your Cloud provider and select **Kubernetes Cluster** > **Discover**.
3. Select **Import Cluster** then **Next**.
4. Upload the `kubeconfig-sa` file you created in create a kubeconfig file. Select the Kubernetes cluster and select **Next**.



Import Kubernetes Cluster

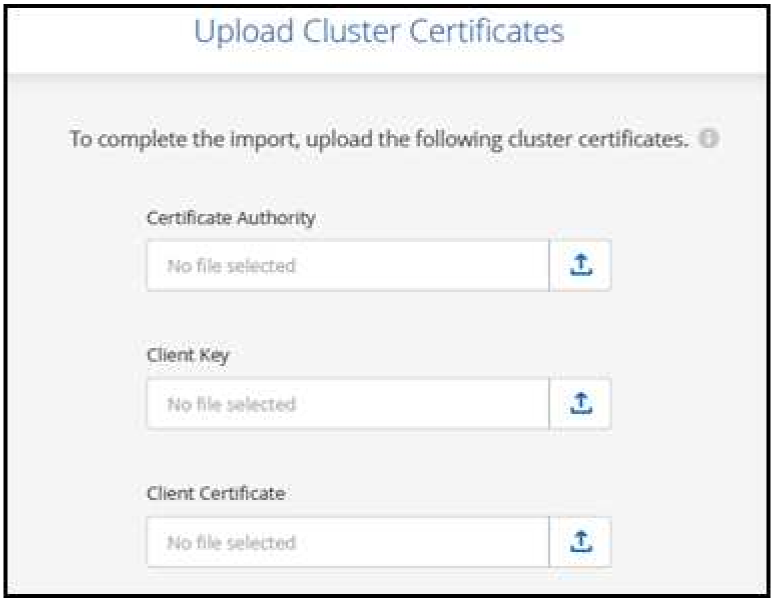
Upload a Kubernetes configuration file that's in YAML format

Kubernetes configuration file: minicubeconfig.txt

1 Cluster

	Kubernetes Cluster Name	Kubernetes Type	Kubernetes Version
✓	test2	Self Managed	v1.24.0

5. Upload the cluster certificates.



Upload Cluster Certificates

To complete the import, upload the following cluster certificates.

Certificate Authority

No file selected

Client Key

No file selected

Client Certificate

No file selected

Result

BlueXP adds the Kubernetes cluster to the Canvas.

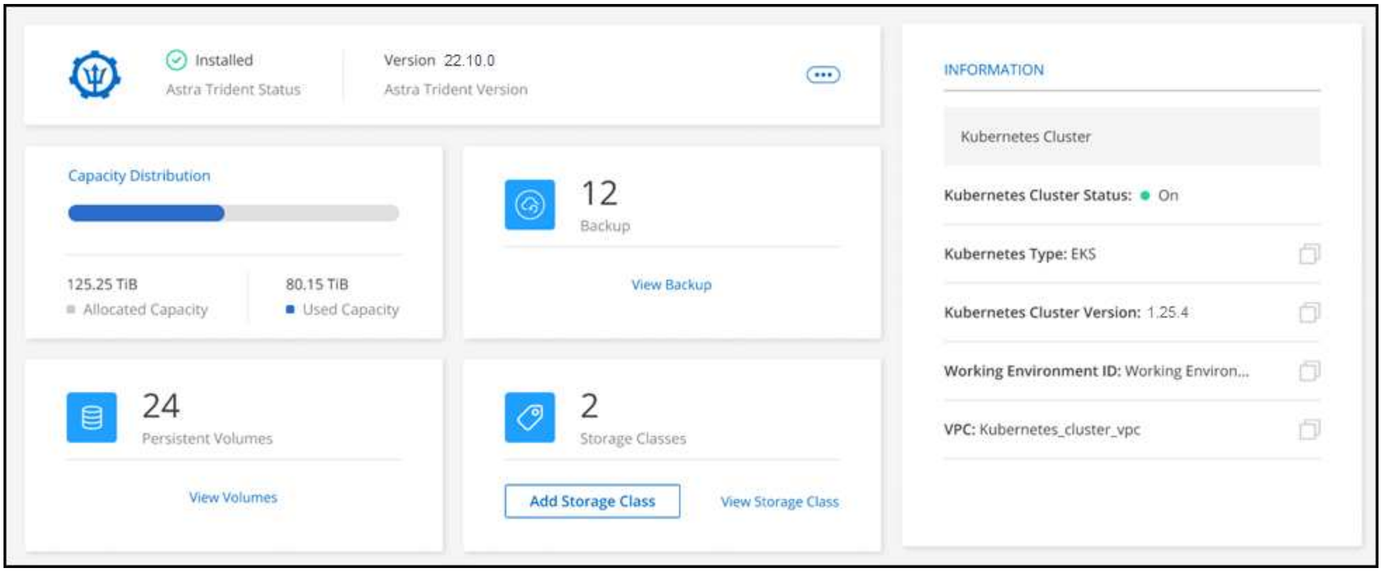
Manage Kubernetes clusters

Manage Astra Trident

After you add a managed Kubernetes cluster to the Canvas, you can use BlueXP to confirm a compatible Astra Trident installation, install or upgrade Astra Trident to the latest version, or uninstall Astra Trident.

Astra Trident in BlueXP

After adding Kubernetes clusters to BlueXP, you can manage Astra Trident and your Kubernetes clusters from the overview page. To open the overview page, double-click the Kubernetes working environment on the Canvas.



Installed
Astra Trident Status
Version 22.10.0
Astra Trident Version

Capacity Distribution
125.25 TiB Allocated Capacity
80.15 TiB Used Capacity

12 Backup

24 Persistent Volumes

2 Storage Classes

INFORMATION
Kubernetes Cluster
Kubernetes Cluster Status: ● On
Kubernetes Type: EKS
Kubernetes Cluster Version: 1.25.4
Working Environment ID: Working Environ...
VPC: Kubernetes_cluster_vpc

Supported Astra Trident versions

One of the four most recent versions of Astra Trident deployed using the Trident operator—either manually or using Helm chart—is required. If Astra Trident is not installed, or an incompatible version of Astra Trident is installed, the cluster will show there is an action required.

> Astra Trident deployed using `tridentctl` is not supported. If you deployed Astra Trident using `tridentctl`, you cannot use BlueXP to manage your Kubernetes clusters or uninstall Astra Trident. You must uninstall using `tridentctl` and reinstall Astra Trident either manually using the Trident operator or in BlueXP using Install or upgrade Astra Trident.

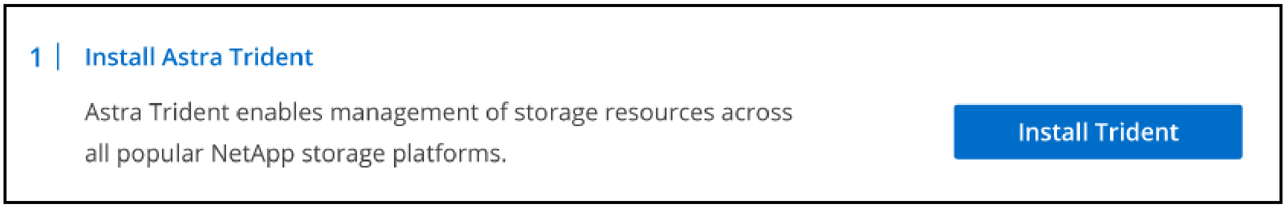
To learn more about Astra Trident, see Astra Trident documentation.

Install or upgrade Astra Trident

You can review your Astra Trident installation status and version on the overview page. If Astra Trident is not already installed, or an incompatible version is installed, you can manage that using BlueXP.

Steps

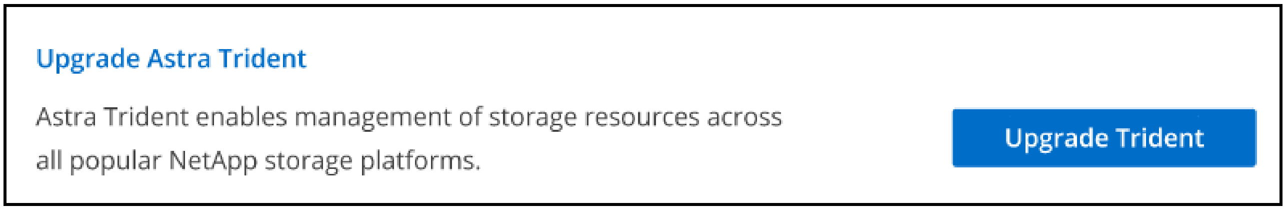
1. Double-click the Kubernetes working environment on the Canvas or click **Enter Working Environment**.
   a. If Astra Trident is not installed, click **Install Trident**.



1 | Install Astra Trident

Astra Trident enables management of storage resources across all popular NetApp storage platforms.

   b. If an unsupported version of Astra Trident is installed, click **Upgrade Trident**.



Upgrade Astra Trident

Astra Trident enables management of storage resources across all popular NetApp storage platforms.

> You cannot use BlueXP to upgrade from Astra Trident versions earlier than 21.01. To upgrade from an earlier version, refer to Upgrade with the operator.

Results

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

Uninstall Astra Trident

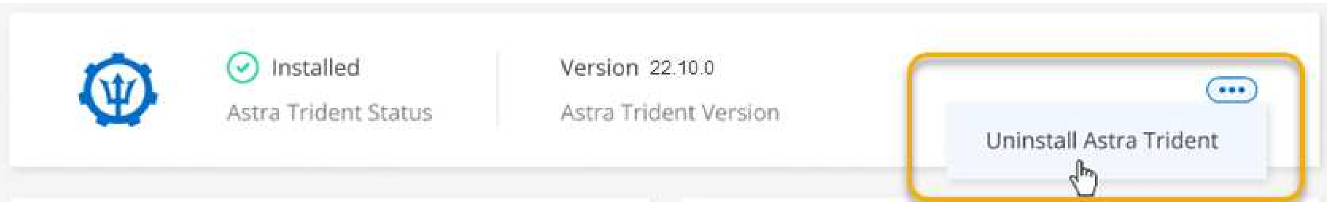
If you installed Astra Trident using BlueXP or using the Trident operator (either Helm or manually), you can uninstall it using BlueXP.

> - After uninstalling Astra Trident you cannot create new persistent volumes, but existing volumes are still available.
> - While Astra Trident is uninstalled, backup is unavailable.
> - You can reinstall Astra Trident to the working environment at any time to continue managing clusters.

Uninstalling Astra Trident using BlueXP does not remove all Astra Trident services applied during installation. To completely remove Astra Trident, including all custom resource definitions (CRDs) it creates, refer to uninstall using the Trident operator

Steps

1. From the overview page, select the ellipses and **Uninstall Astra Trident**.



2. Select **Uninstall** to confirm and uninstall Astra Trident.

Results

Astra Trident is now uninstalled from the working environment. You can reinstall Astra Trident at any time.

Manage storage classes

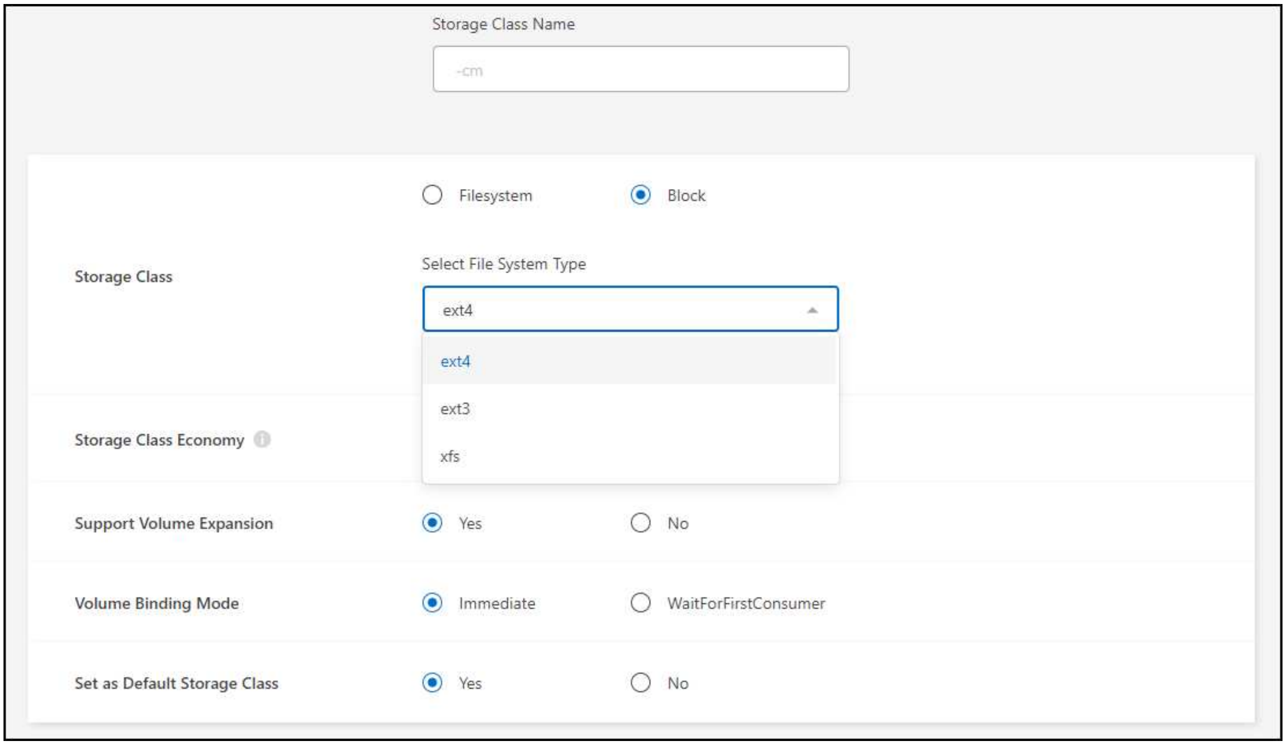
After you add a managed Kubernetes cluster to the Canvas, you can use BlueXP to manage storage classes.

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

Add storage class

Steps

1. From the Canvas, drag and drop the Kubernetes working environment on to the Cloud Volumes ONTAP or Amazon FSx for ONTAP working environment to open the storage class wizard.
2. Provide a name for the storage class.
3. Select **Filesystem** or **Block** storage.
    a. For **Block** storage, select a File System Type (fstype)



Storage Class Name: -cm

Storage Class: ○ Filesystem ● Block

Select File System Type: ext4

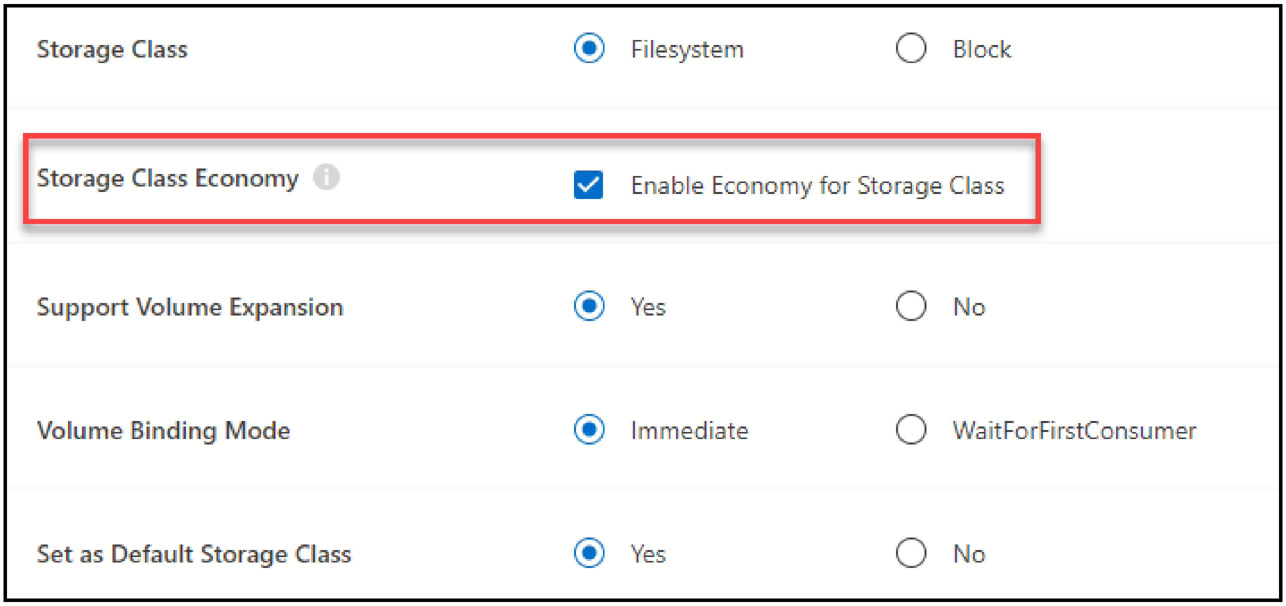
Storage Class Economy

Support Volume Expansion: ● Yes ○ No

Volume Binding Mode: ● Immediate ○ WaitForFirstConsumer

Set as Default Storage Class: ● Yes ○ No

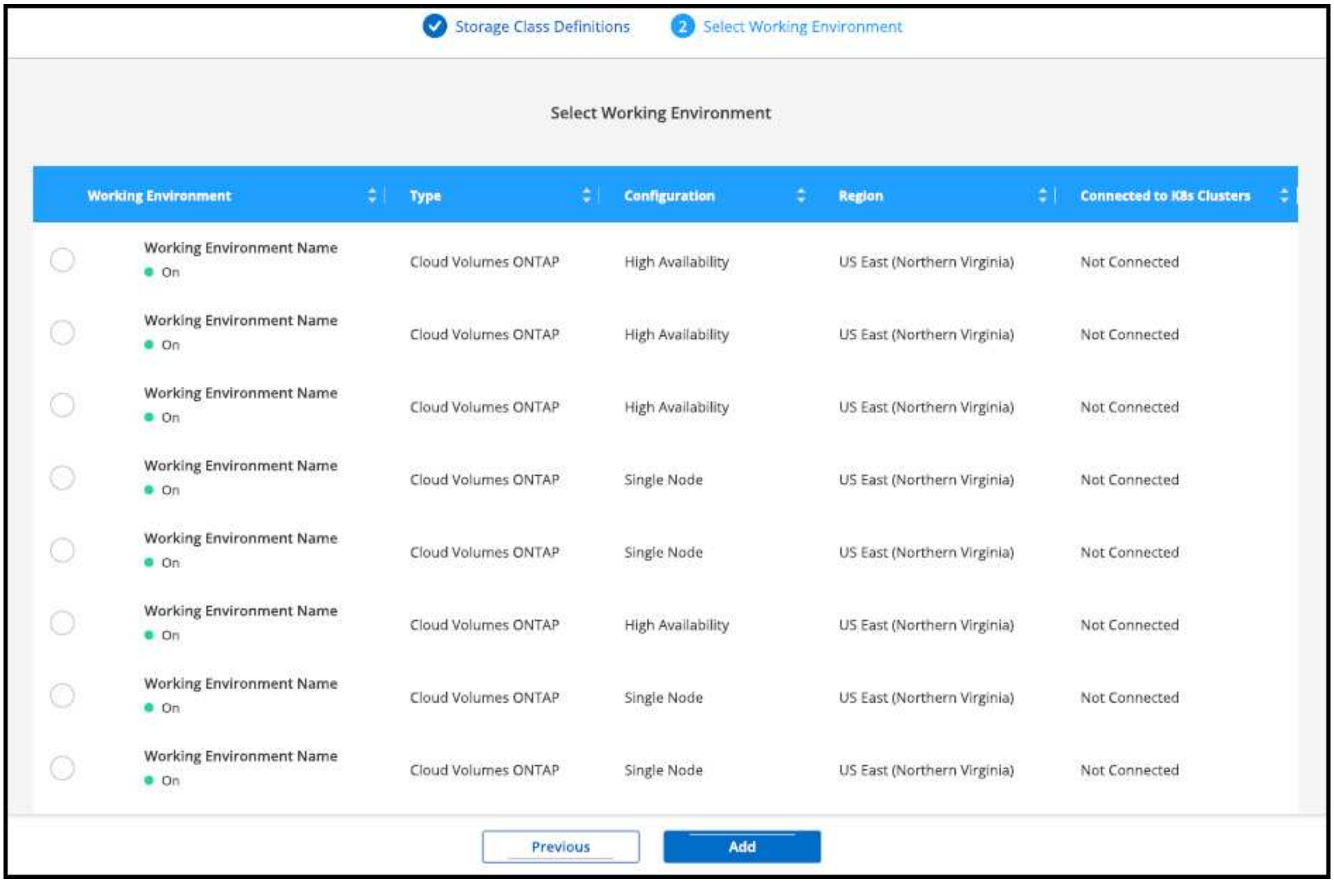
    b. For **Block** or **Filesystem** storage, you can select to enable storage class economy.



Storage Class	● Filesystem	○ Block
Storage Class Economy	☑ Enable Economy for Storage Class	
Support Volume Expansion	● Yes	○ No
Volume Binding Mode	● Immediate	○ WaitForFirstConsumer
Set as Default Storage Class	● Yes	○ No

Backup and restore are not supported when using storage class economy.

4. Select options for volume expansion, volume binding, and default storage class. Click **Next**.
5. Select a working environment to connect to the cluster. Click **Add**.

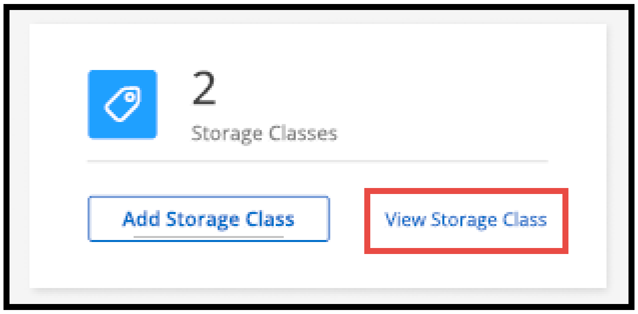


Select Working Environment

	Working Environment	Type	Configuration	Region	Connected to K8s Clusters
○	Working Environment Name ● On	Cloud Volumes ONTAP	High Availability	US East (Northern Virginia)	Not Connected
○	Working Environment Name ● On	Cloud Volumes ONTAP	High Availability	US East (Northern Virginia)	Not Connected
○	Working Environment Name ● On	Cloud Volumes ONTAP	High Availability	US East (Northern Virginia)	Not Connected
○	Working Environment Name ● On	Cloud Volumes ONTAP	Single Node	US East (Northern Virginia)	Not Connected
○	Working Environment Name ● On	Cloud Volumes ONTAP	Single Node	US East (Northern Virginia)	Not Connected
○	Working Environment Name ● On	Cloud Volumes ONTAP	High Availability	US East (Northern Virginia)	Not Connected
○	Working Environment Name ● On	Cloud Volumes ONTAP	Single Node	US East (Northern Virginia)	Not Connected
○	Working Environment Name ● On	Cloud Volumes ONTAP	Single Node	US East (Northern Virginia)	Not Connected

Results

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



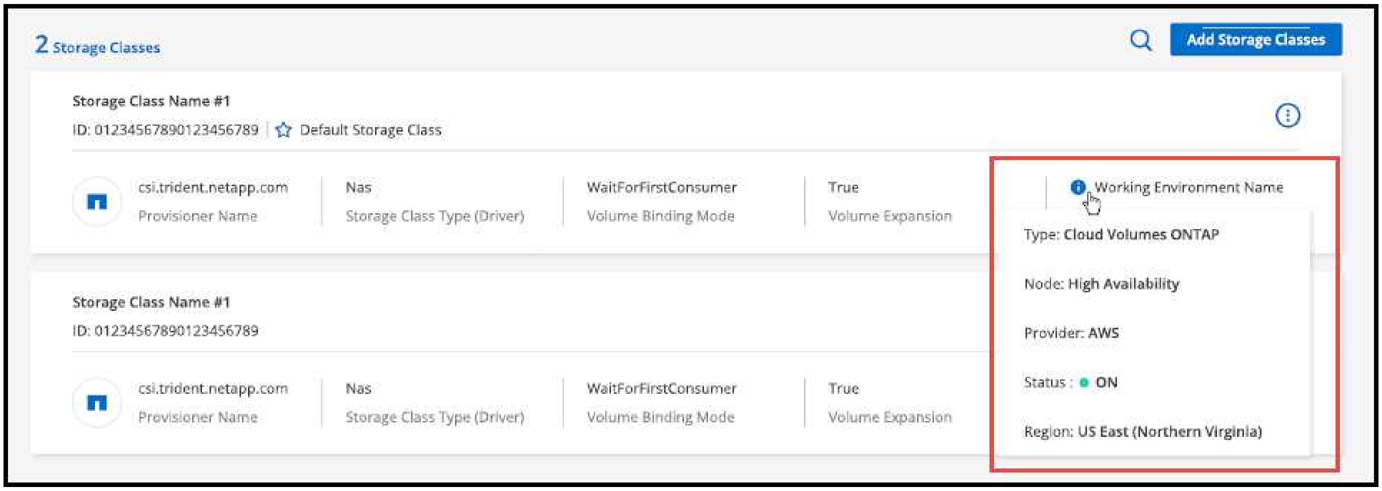
View working environment details

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.



Storage Class Name #1
ID: 01234567890123456789 | ☆ Default Storage Class

csi.trident.netapp.com
Provisioner Name

Nas
Storage Class Type (Driver)

WaitForFirstConsumer
Volume Binding Mode

True
Volume Expansion

Working Environment Name

Type: Cloud Volumes ONTAP

Node: High Availability

Provider: AWS

Status : ● ON

Region: US East (Northern Virginia)

Storage Class Name #1
ID: 01234567890123456789

csi.trident.netapp.com
Provisioner Name

Nas
Storage Class Type (Driver)

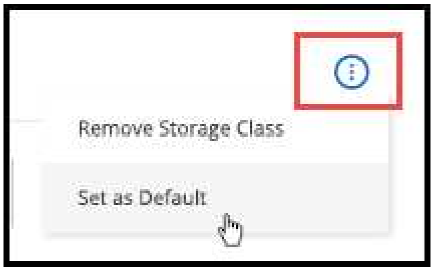
WaitForFirstConsumer
Volume Binding Mode

True
Volume Expansion

Set default storage class

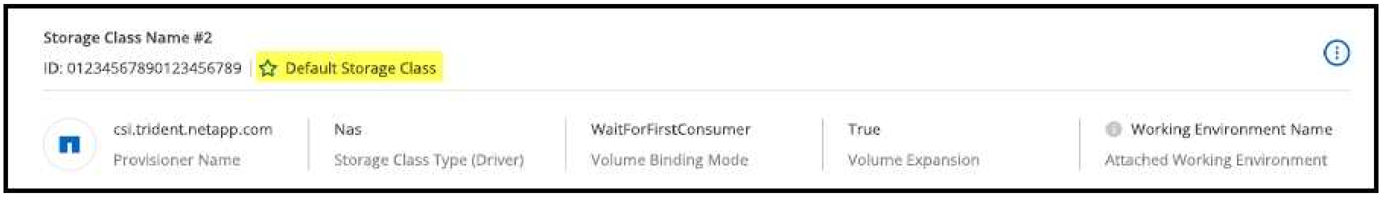
Steps

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.



Storage Class Name #2

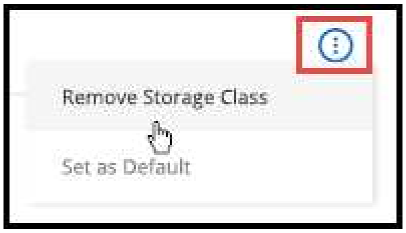
ID: 01234567890123456789 | ☆ Default Storage Class

csi.trident.netapp.com	Nas	WaitForFirstConsumer	True	Working Environment Name
Provisioner Name	Storage Class Type (Driver)	Volume Binding Mode	Volume Expansion	Attached Working Environment

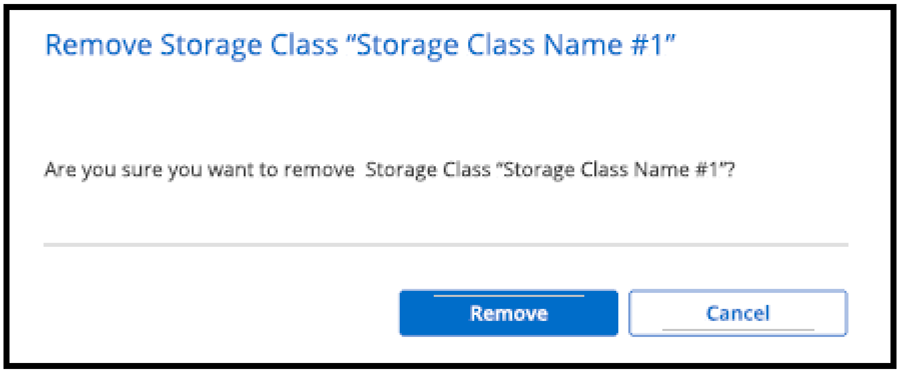
Remove storage class

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.



Remove Storage Class “Storage Class Name #1”

Are you sure you want to remove Storage Class “Storage Class Name #1”?

Results

The selected storage class is removed.

View persistent volumes

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

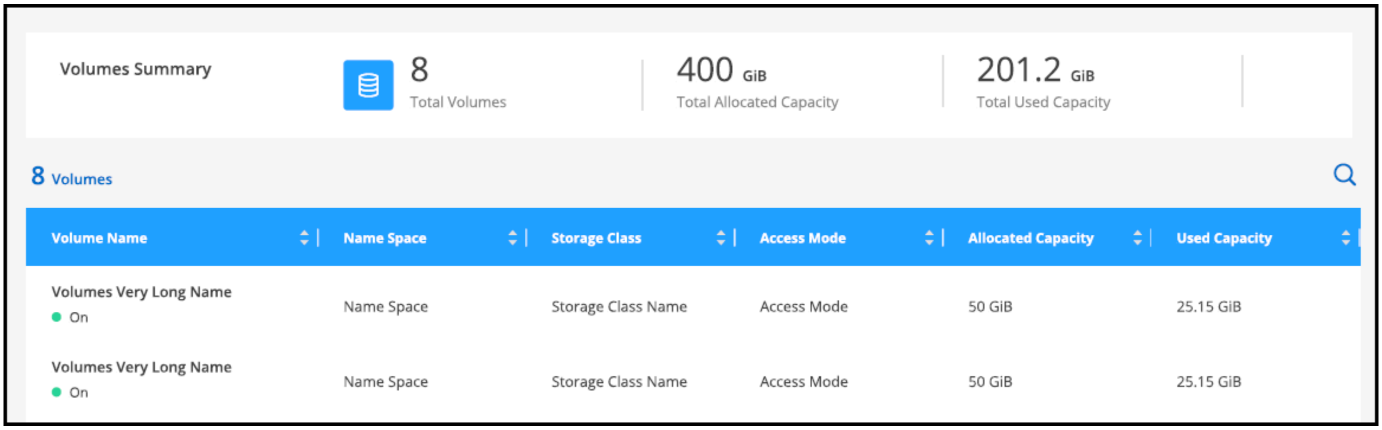
> BlueXP monitors the Kubernetes cluster for changes to the backend and updates the persistent volume table when new volumes are added. If automatic backup was configured on the cluster, backup is automatically enabled on the new persistent volumes.

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.



Volumes Summary

8 Total Volumes

400 GiB Total Allocated Capacity

201.2 GiB Total Used Capacity

8 Volumes

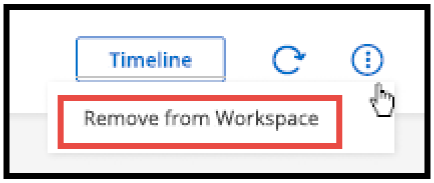
Volume Name	Name Space	Storage Class	Access Mode	Allocated Capacity	Used Capacity
Volumes Very Long Name ● On	Name Space	Storage Class Name	Access Mode	50 GiB	25.15 GiB
Volumes Very Long Name ● On	Name Space	Storage Class Name	Access Mode	50 GiB	25.15 GiB

Remove Kubernetes clusters from the workspace

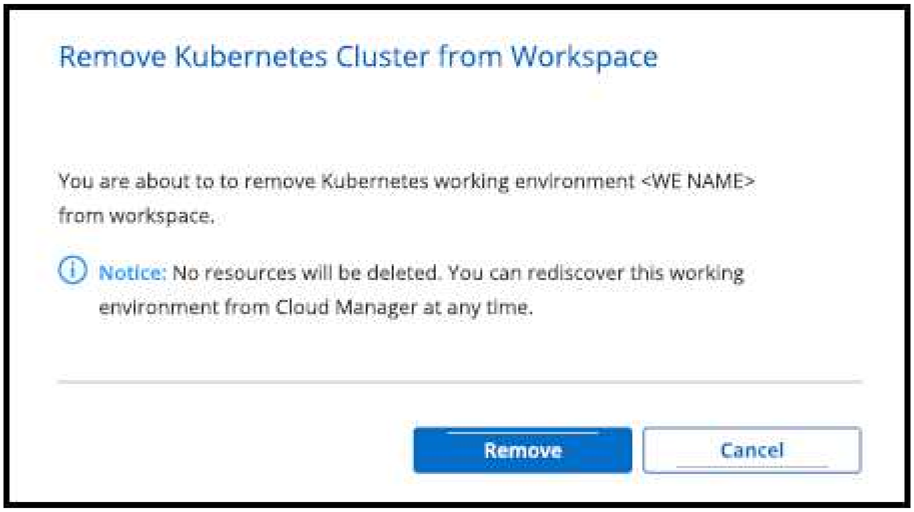
After you add a managed Kubernetes cluster to the Canvas, you can use BlueXP to remove clusters from the workspace.

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.



Remove Kubernetes Cluster from Workspace

You are about to to remove Kubernetes working environment <WE NAME> from workspace.

ⓘ Notice: No resources will be deleted. You can rediscover this working environment from Cloud Manager at any time.

Results

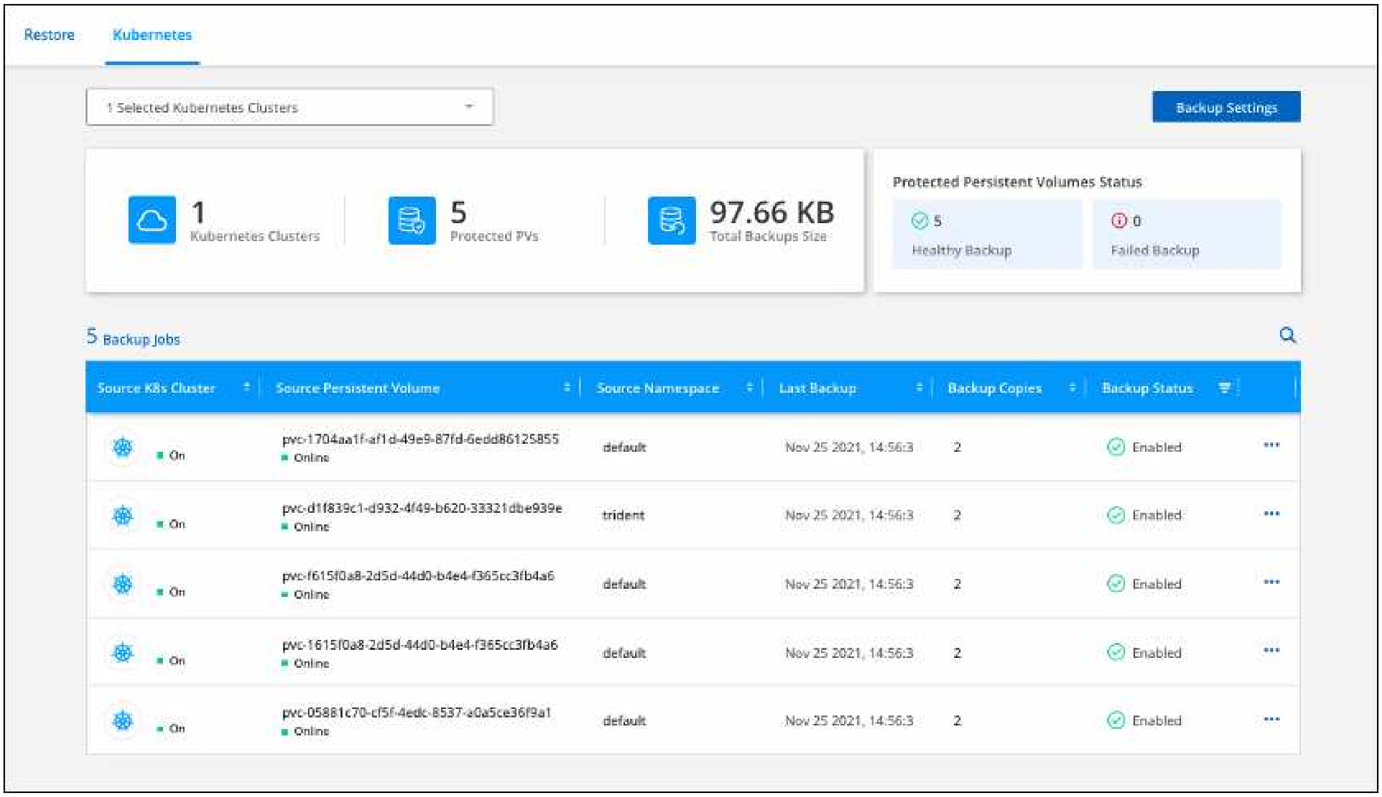
The Kubernetes cluster is removed from the workspace and is no longer visible on the Canvas.

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.

You can use BlueXP backup and recovery to back up persistent volumes to object storage.

Learn how to protect your Kubernetes cluster data using BlueXP backup and recovery.



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

Support registration is required to receive technical support specific to BlueXP and its storage solutions and services. Support registration is also required to enable key workflows for Cloud Volumes ONTAP systems.

Registering for support does not enable NetApp support for a cloud provider file service. For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Cloud Volumes Service for Google Cloud

Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your BlueXP account ID support subscription (your 20 digit 960xxxxxxxxx serial number located on the Support Resources page in BlueXP).

  This serves as your single support subscription ID for any service within BlueXP. Each BlueXP account-level support subscription must be registered.

- Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider's marketplace (these are 20 digit 909201xxxxxxxx serial numbers).

  These serial numbers are commonly referred to as *PAYGO serial numbers* and get generated by BlueXP at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets and automatic case generation. Registration is completed by adding NetApp Support Site (NSS) accounts to BlueXP as described below.

Register your BlueXP account for NetApp support

To register for support and activate support entitlement, one user in your BlueXP account must associate a NetApp Support Site account with their BlueXP login. How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

Existing customer with an NSS account

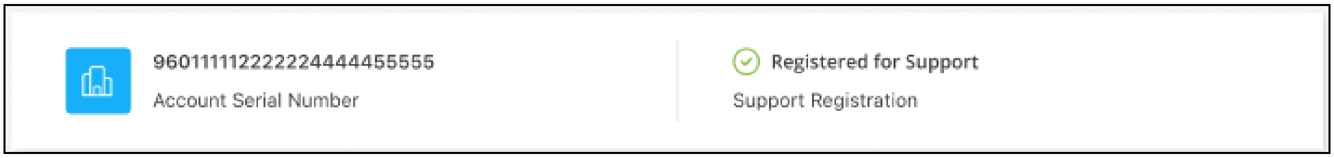
If you're a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select **User Credentials**.

3. Select **Add NSS credentials** and follow the NetApp Support Site (NSS) Authentication prompt.
4. To confirm that the registration process was successful, select the Help icon, and select **Support**.

   The **Resources** page should show that your account is registered for support.

   960111112222224444455555
   Account Serial Number

   Registered for Support
   Support Registration

   Note that other BlueXP users will not see this same support registration status if they have not associated a NetApp Support Site account with their BlueXP login. However, that doesn't mean that your BlueXP account is not registered for support. As long as one user in the account has followed these steps, then your account has been registered.

Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you need to create an NSS account and associate it with your BlueXP login.

Steps

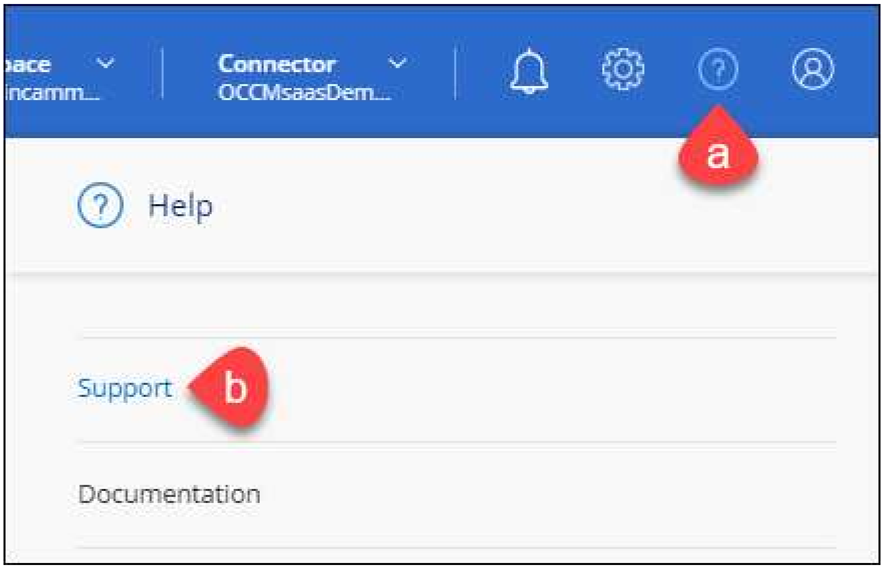
1. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.
2. Associate your new NSS account with your BlueXP login by completing the steps under Existing customer with an NSS account.

Brand new to NetApp

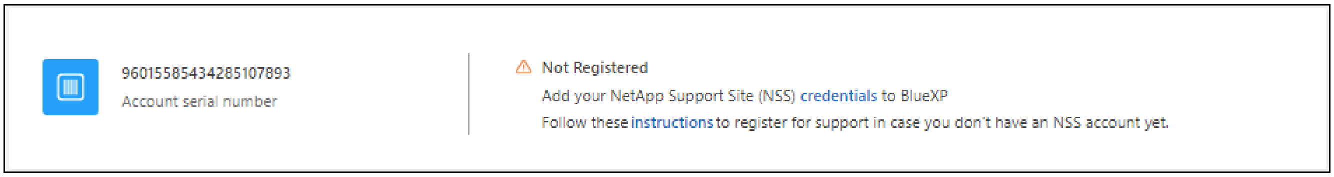
If you are brand new to NetApp and you don't have an NSS account, follow each step below.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.

2. Locate your account ID serial number from the Support Registration page.



96015585434285107893
Account serial number

⚠ Not Registered
Add your NetApp Support Site (NSS) credentials to BlueXP
Follow these instructions to register for support in case you don't have an NSS account yet.

3. Navigate to NetApp's support registration site and select **I am not a registered NetApp Customer**.
4. Fill out the mandatory fields (those with red asterisks).
5. In the **Product Line** field, select **Cloud Manager** and then select your applicable billing provider.
6. Copy your account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

   An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn't arrive in few minutes.

7. Confirm the action from within the email.

   Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, associate the account with your BlueXP login by completing the steps under Existing customer with an NSS account.

Associate NSS credentials for Cloud Volumes ONTAP support

Associating NetApp Support Site credentials with your BlueXP account is required to enable the following key workflows for Cloud Volumes ONTAP:

- Registering pay-as-you-go Cloud Volumes ONTAP systems for support

  Providing your NSS account is required to activate support for your system and to gain access to NetApp technical support resources.

- Deploying Cloud Volumes ONTAP when you bring your own license (BYOL)

  Providing your NSS account is required so that BlueXP can upload your license key and to enable the subscription for the term that you purchased. This includes automatic updates for term renewals.

- Upgrading Cloud Volumes ONTAP software to the latest release

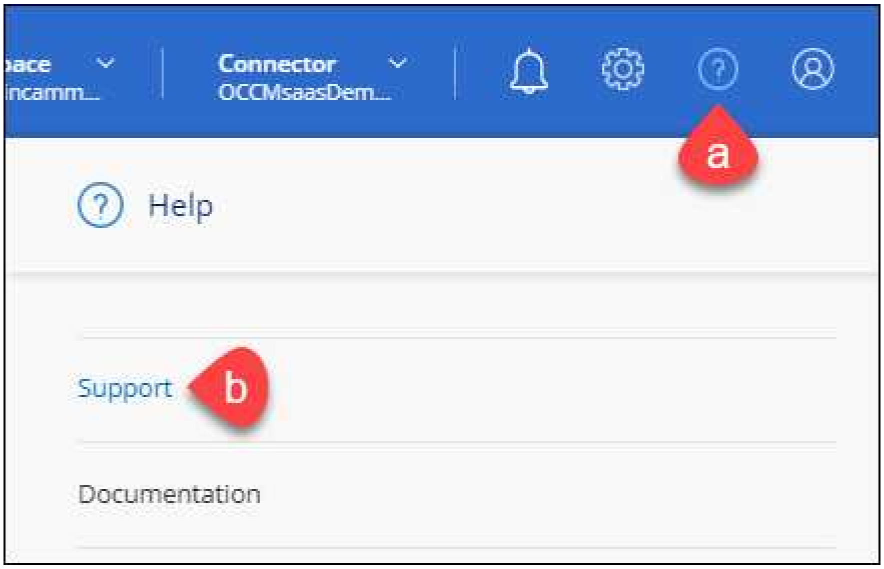
Associating NSS credentials with your BlueXP account is different than the NSS account that is associated with a BlueXP user login.

These NSS credentials are associated with your specific BlueXP account ID. Users who belong to the BlueXP account can access these credentials from **Support > NSS Management**.

- If you have a customer-level account, you can add one or more NSS accounts.
- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added alongside customer-level accounts.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.

2. Select **NSS Management > Add NSS Account**.
3. When you're prompted, select **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Entra ID as the identity provider for authentication services specific to support and licensing.

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

   These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

   Note the following:

   - The NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
   - There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

     "The NSS customer type is not allowed for this account as there are already NSS Users of different type."

     The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level account.

   - Upon successful login, NetApp will store the NSS user name.

    This is a system-generated ID that maps to your email. On the **NSS Management** page, you can display your email from the ••• menu.

  - If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the ••• menu.

    Using this option prompts you to log in again. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

Get help

NetApp provides support for BlueXP 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.

Get support for a cloud provider file service

For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Cloud Volumes Service for Google Cloud

To receive technical support specific to BlueXP and its storage solutions and services, use the support options described below.

Use self-support options

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

- Documentation

  The BlueXP documentation that you’re currently viewing.

- Knowledge base

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

- Communities

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

Create a case with NetApp support

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

Before you get started

- To use the **Create a Case** capability, you must first associate your NetApp Support Site credentials with your BlueXP login. Learn how to manage credentials associated with your BlueXP login.
- If you're opening a case for an ONTAP system that has a serial number, then your NSS account must be associated with the serial number for that system.

Steps

1. In BlueXP, select **Help > Support**.
2. On the **Resources** page, choose one of the available options under Technical Support:

   a. Select **Call Us** if you'd like to speak with someone on the phone. You'll be directed to a page on netapp.com that lists the phone numbers that you can call.

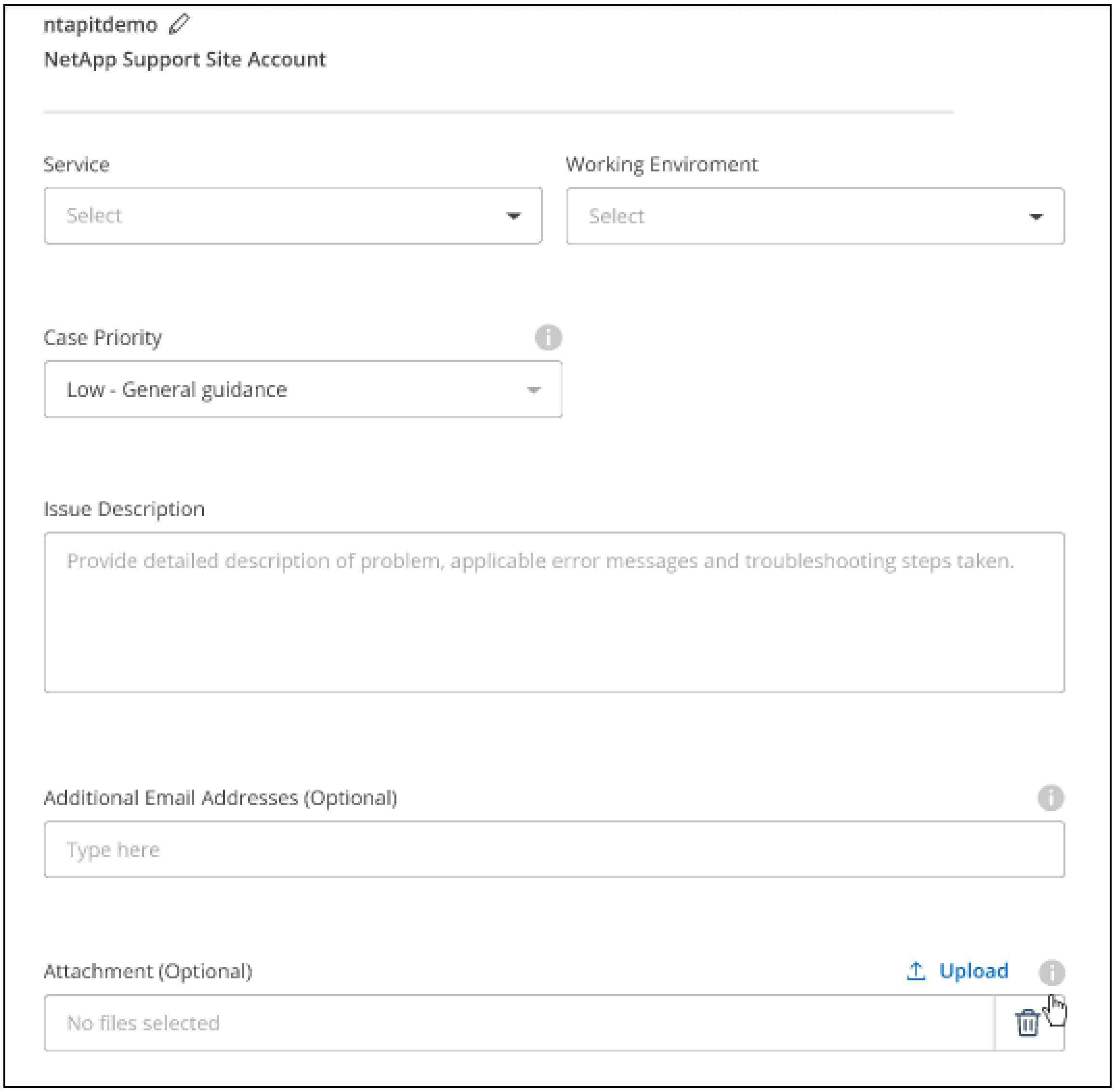
   b. Select **Create a Case** to open a ticket with a NetApp Support specialist:

      - **Service**: Select the service that the issue is associated with. For example, BlueXP when specific to a technical support issue with workflows or functionality within the service.
      - **Working Environment**: If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.

        The list of working environments are within scope of the BlueXP account, workspace, and Connector you have selected in the top banner of the service.
      - **Case Priority**: Choose the priority for the case, which can be Low, Medium, High, or Critical.

        To learn more details about these priorities, hover your mouse over the information icon next to the field name.
      - **Issue Description**: Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.
      - **Additional Email Addresses**: Enter additional email addresses if you'd like to make someone else aware of this issue.
      - **Attachment (Optional)**: Upload up to five attachments, one at a time.

        Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.



ntapitdemo

NetApp Support Site Account

Service: Select

Working Enviroment: Select

Case Priority: Low - General guidance

Issue Description: Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional): Type here

Attachment (Optional): No files selected

After you finish

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.

For a history of your support cases, you can select **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It’s possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it’s associated with is not the same company of record for the BlueXP account serial number (ie. 960xxxx) or the working environment serial number. You can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at https://mysupport.netapp.com/site/help

Manage your support cases (Preview)

You can view and manage active and resolved support cases directly from BlueXP. You can manage the cases associated with your NSS account and with your company.

Case management is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Note the following:

- The case management dashboard at the top of the page offers two views:
  - The view on the left shows the total cases opened in the past 3 months by the user NSS account you provided.
  - The view on the right shows the total cases opened in the past 3 months at your company level based on your user NSS account.

  The results in the table reflect the cases related to the view that you selected.

- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

  View the steps below for more details.

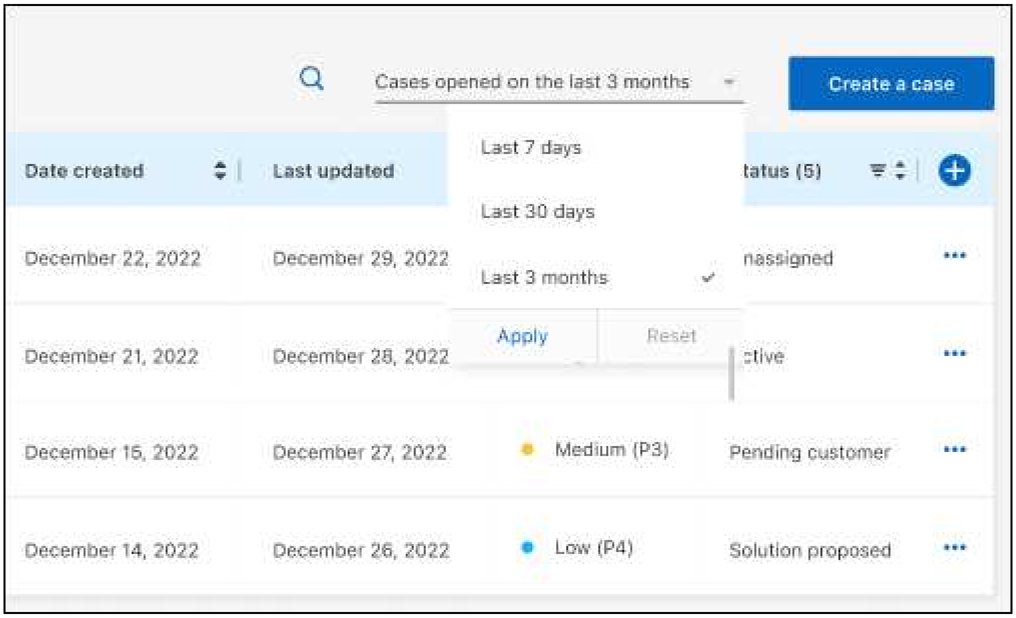
- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

Steps

1. In BlueXP, select **Help > Support**.
2. Select **Case Management** and if you’re prompted, add your NSS account to BlueXP.

   The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP user account. This is the same NSS account that appears at the top of the **NSS management** page.

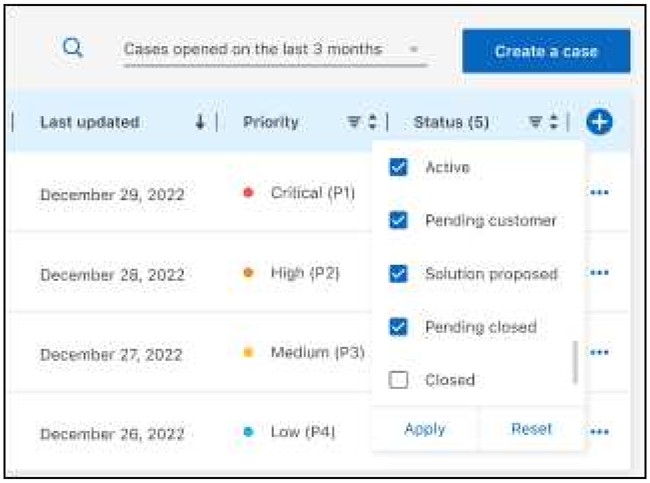
3. Optionally modify the information that displays in the table:
   - Under **Organization’s cases**, select **View** to view all cases associated with your company.
   - Modify the date range by choosing an exact date range or by choosing a different time frame.


Cases opened on the last 3 months

- Last 7 days
- Last 30 days
- Last 3 months ✓

Date created	Last updated		tatus (5)
December 22, 2022	December 29, 2022		nassigned
December 21, 2022	December 28, 2022		ctive
December 15, 2022	December 27, 2022	● Medium (P3)	Pending customer
December 14, 2022	December 26, 2022	● Low (P4)	Solution proposed

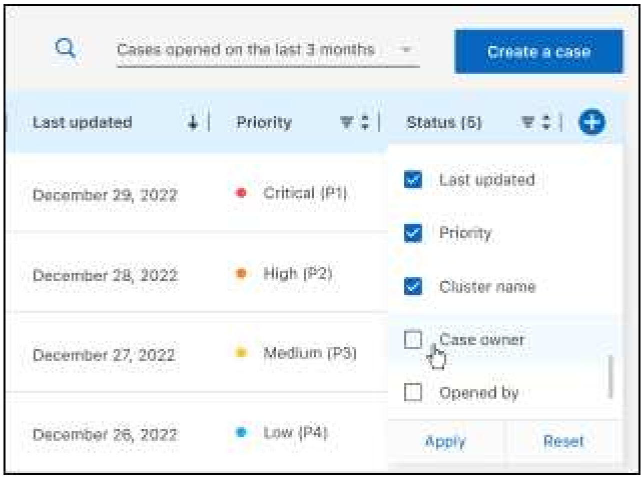
- Filter the contents of the columns.


Cases opened on the last 3 months

Last updated	Priority	Status (5)
December 29, 2022	● Critical (P1)	
December 28, 2022	● High (P2)	
December 27, 2022	● Medium (P3)	
December 26, 2022	● Low (P4)	

☑ Active
☑ Pending customer
☑ Solution proposed
☑ Pending closed
☐ Closed

- Change the columns that appear in the table by selecting ⊕ and then choosing the columns that you'd like to display.


Cases opened on the last 3 months

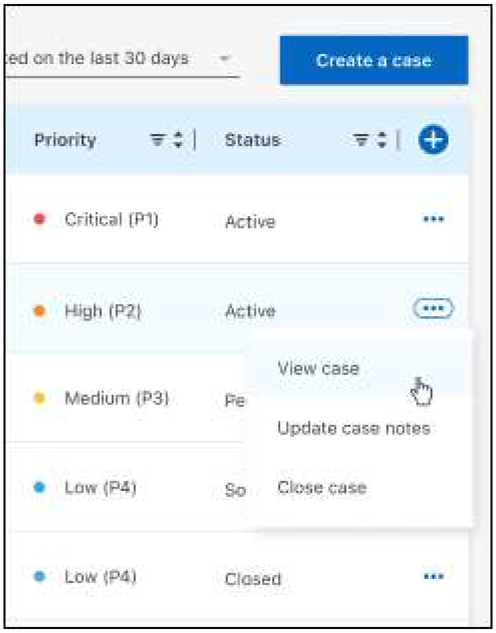
Last updated	Priority	Status (5)
December 29, 2022	● Critical (P1)	
December 28, 2022	● High (P2)	
December 27, 2022	● Medium (P3)	
December 26, 2022	● Low (P4)	

☑ Last updated
☑ Priority
☑ Cluster name
☐ Case owner
☐ Opened by

4. Manage an existing case by selecting ••• and selecting one of the available options:

   - **View case**: View full details about a specific case.
   - **Update case notes**: Provide additional details about your problem or select **Upload files** to attach up to a maximum of five files.

     Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.
   - **Close case**: Provide details about why you’re closing the case and select **Close case**.



Priority	Status
● Critical (P1)	Active
● High (P2)	Active
● Medium (P3)	Pe
● Low (P4)	So
● Low (P4)	Closed

Legal notices

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

Copyright

https://www.netapp.com/company/legal/copyright/

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.

https://www.netapp.com/company/legal/trademarks/

Patents

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

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Privacy policy

https://www.netapp.com/company/legal/privacy-policy/

Open source

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

Notice for BlueXP

Copyright information

Trademark information