Get started

Astra Control Service

NetApp
November 09, 2021

Table of Contents

Get started

Intro to Astra Control

Astra Control is a Kubernetes application data lifecycle management solution that simplifies operations for stateful applications. Easily protect, back up, and migrate Kubernetes workloads, and instantly create working application clones.

Features

Astra Control offers critical capabilities for Kubernetes application data lifecycle management:

- Automatically manage persistent storage
- Create application-aware, on-demand snapshots and backups
- Automate policy-driven snapshot and backup operations
- Migrate applications and data from one Kubernetes cluster to another
- Easily clone an application from production to staging
- Visualize application health and protection status
- Use a user interface or an API to implement your backup and migration workflows

Astra Control continually watches your compute for state changes, so it's aware of any new apps that you add along the way.

Deployment models

Astra Control is available in two deployment models:

- **Astra Control Service**: A NetApp-managed service that provides application-aware data management of Kubernetes clusters in Google Kubernetes Engine (GKE) and Azure Kubernetes Service (AKS).
- **Astra Control Center**: Self-managed software that provides application-aware data management of Kubernetes clusters running in your on-premises environment.

	Astra Control Service	Astra Control Center
How is it offered?	As a fully managed cloud service from NetApp	As software that you download, install, and manage
Where is it hosted?	On a public cloud of NetApp's choice	On your provided Kubernetes cluster
How is it updated?	Managed by NetApp	You manage any updates
What are the app data management capabilities?	Same capabilities on both platforms with exceptions to backend storage or to external services	Same capabilities on both platforms with exceptions to backend storage or to external services
What is the backend storage support?	NetApp cloud service offerings	NetApp ONTAP AFF and FAS systems

Supported apps

Astra Control Center does not support apps that are deployed with Operator Lifecycle Manager (OLM)-enabled operators or cluster-scoped operators.

NetApp has validated some apps to ensure the safety and consistency of the snapshots and backups.

- Learn the difference between a validated app and a standard app in Astra Control Service.
- Learn the difference between a validated app and a standard app in Astra Control Center.

No matter which type of app that you use with Astra Control, you should always test the backup and restore workflow yourself to ensure that you can meet your disaster recovery requirements.

How Astra Control Service works

Astra Control Service is a NetApp-managed cloud service that is always on and updated with the latest capabilities. It utilizes several components to enable application data lifecycle management.

At a high level, Astra Control Service works like this:

- You get started with Astra Control Service by setting up your cloud provider and by registering for an Astra account.
  - For GKE clusters, Astra Control Service uses NetApp Cloud Volumes Service for Google Cloud as the backend storage for your persistent volumes.
  - For AKS clusters, Astra Control Service uses Azure NetApp Files as the backend storage for your persistent volumes.
- You add your first Kubernetes compute to Astra Control Service. Astra Control Service then does the following:
  - Creates an object store in your cloud provider account, which is where backup copies are stored.

    In Azure, Astra Control Service also creates a resource group, a storage account, and keys for the Blob container.
  - Creates a new admin role and Kubernetes service account on the cluster.
  - Uses that new admin role to install Astra Trident on the cluster and to create one or more storage classes.
  - Uses Astra Trident to provision persistent volumes for your apps.
- At this point, you can add apps to your cluster. Persistent volumes will be provisioned on the new default storage class.
- You then use Astra Control Service to manage these apps, and start creating snapshots, backups, and clones.

  Astra Control Service continually watches your compute for state changes, so it's aware of any new apps that you add along the way.

Astra Control's Free Plan enables you to manage up to 10 apps in your account. If you want to manage more than 10 apps, then you'll need to set up billing by upgrading from the Free Plan to the Premium Plan.

How Astra Control Center works

Astra Control Center runs locally in your own private cloud.

For the first release, Astra Control Center will support OpenShift Kubernetes clusters and Trident storage backends with ONTAP 9.5 and above.

In a cloud connected environment Astra Control Center uses Cloud Insights to provide advanced monitoring and telemetry. In the absence of a Cloud Insights connection, limited (7-days of metrics) monitoring and telemetry is available in Astra Control Center and also exported to Kubernetes native monitoring tools (such as Prometheus and Grafana) through open metrics end points.

Astra Control Center is fully integrated into the AutoSupport and Active IQ ecosystem to provide users and NetApp support with troubleshooting and usage information.

You can try Astra Control Center out using a 90-day evaluation license. The evaluation version is supported through email and community (Slack channel) options. Additionally, you have access to Knowledgebase articles and documentation from the in-product support dashboard.

To install and use Astra Control Center, you'll need to meet certain requirements.

At a high level, Astra Control Center works like this:

- You install Astra Control Center in your local environment. Learn more about how to install Astra Control Center.
- You complete some setup tasks such as these:
  - Set up licensing.
  - Add your first cluster.
  - Add backend storage that is discovered when you added the cluster.
  - Add an object store bucket that will store your app backups.

Learn more about how to set up Astra Control Center.

Astra Control Center does this:

- Discovers details about the managed Kubernetes clusters.
- Discovers your Astra Trident configuration on the clusters that you choose to manage and lets you monitor the storage backends.
- Discovers apps on those clusters and enables you to manage and protect the apps.

You can add apps to your cluster. Or, if you have some apps already in the cluster being managed, you can use Astra Control Center to discover and manage them. Then, use Astra Control Center to create snapshots, backups, and clones.

For more information

- Astra Control Service documentation
- Astra Control Control documentation
- Astra Trident documentation
- Use the Astra API

- Cloud Insights documentation
- ONTAP documentation

Supported Kubernetes deployments

Astra Control Service can manage apps that are running on a managed Kubernetes cluster in Google Kubernetes Engine (GKE) and Azure Kubernetes Service (AKS).

- Learn how to set up Google Cloud for Astra Control Service.
- Learn how to set up Microsoft Azure for Astra Control Service.

Quick start for Astra Control Service

This page provides a high-level overview of the steps that you need to complete to get started with Astra Control Service. The links within each step take you to a page that provides more details.

[One] Set up your cloud provider

a. Google Cloud:
   - Review GKE cluster requirements.
   - Purchase Cloud Volumes Service for Google Cloud from the Google Cloud Marketplace.
   - Enable the required APIs.
   - Create a service account and service account key.
   - Set up network peering from your VPC to Cloud Volumes Service for Google Cloud.

   Learn more about Google Cloud requirements.

b. Microsoft Azure:
   - Review AKS cluster requirements.
   - Register for Azure NetApp Files.
   - Create a NetApp account.
   - Set up a capacity pool.
   - Delegate a subnet to Azure NetApp Files.
   - Create an Azure service principal that has the Contributor role.

   Learn more about Microsoft Azure requirements.

[Two] Complete the Astra Control registration

a. Create a NetApp Cloud Central account.
b. Specify your NetApp Cloud Central email ID when creating your Astra Control account from the Astra product page.

Learn more about the registration process.

[Three] Add clusters to Astra Control

After you log in, click **Add cluster** to start managing your cluster with Astra Control.

Learn more about adding clusters.

Set up your cloud provider

Set up Google Cloud

A few steps are required to prepare your Google Cloud project before you can manage Google Kubernetes Engine clusters with Astra Control Service.

Quick start for setting up Google Cloud

Get started quickly by following these steps or scroll down to the remaining sections for full details.

[One] Review Astra Control Service requirements for Google Kubernetes Engine

Ensure that clusters are healthy and running a Kubernetes version in the range of 1.18 to 1.20, that worker nodes are online and running Container-Optimized OS or Ubuntu, and more. Learn more about this step.

[Two] Purchase Cloud Volumes Service for Google Cloud

Go to the NetApp Cloud Volumes Service page in the Google Cloud Marketplace and click Purchase. Learn more about this step.

[Three] Enable APIs in your Google Cloud project

Enable the following Google Cloud APIs:

- Google Kubernetes Engine
- Cloud Storage
- Cloud Storage JSON API
- Service Usage
- Cloud Resource Manager API
- NetApp Cloud Volumes Service
- Service Consumer Management API
- Service Networking API
- Service Management API

Follow step-by-step instructions.

[Four] Create a service account that has the required permissions

Create a Google Cloud service account that has the following permissions:

- Kubernetes Engine Admin
- NetApp Cloud Volumes Admin

- Storage Admin
- Service Usage Viewer
- Compute Network Viewer

Read step-by-step instructions.

[Five] Create a service account key

Create a key for the service account and save the key file in a secure location. Follow step-by-step instructions.

[Six] Set up network peering for your VPC

Set up network peering from your VPC to Cloud Volumes Service for Google Cloud. Follow step-by-step instructions.

The following image depicts each of these steps that you'll need to complete.

GKE cluster requirements

A Kubernetes cluster must meet the following requirements so you can discover and manage it from Astra Control Service.

Kubernetes version
A cluster must be running a Kubernetes version in the range of 1.18 to 1.20.

Image type
The image type for each worker node must be one of the following:

- Container-Optimized OS with Containerd
- Container-Optimized OS with Docker
- Ubuntu with Docker

Cluster state
Clusters must be running in a healthy state and have at least one online worker node with no worker nodes in a failed state.

Google Cloud region
Clusters must be running in a Google Cloud region where Cloud Volumes Service for Google Cloud is supported. Note that Astra Control Service supports both service types: CVS and CVS-Performance.

Networking
The cluster must reside in a VPC that is peered with Cloud Volumes Service for Google Cloud. This step is described below.

Private clusters
If the cluster is private, the authorized networks must allow the Astra Control Service IP addresses:

- 54.164.233.140/32

- 3.218.120.204/32
- 34.193.99.138/32

Mode of operation for a GKE cluster

You should use the Standard mode of operation. The Autopilot mode hasn't been tested at this time. Learn more about modes of operation.

Purchase Cloud Volumes Service for Google Cloud

Astra Control Service uses Cloud Volumes Service for Google Cloud as the backend storage for your persistent volumes. You need to purchase Cloud Volumes Service for Google Cloud from the Google Cloud Marketplace to enable billing for persistent volumes.

Step

1. Go to the NetApp Cloud Volumes Service page in the Google Cloud Marketplace, click **Purchase**, and follow the prompts.

   Follow step-by-step instructions in the Google Cloud documentation to purchase and enable the service.

Enable APIs in your project

Your project needs permissions to access specific Google Cloud APIs. APIs are used to interact with Google Cloud resources, such as Google Kubernetes Engine (GKE) clusters and NetApp Cloud Volumes Service storage.

Step

1. Use the Google Cloud console or gcloud CLI to enable the following APIs:
   - Google Kubernetes Engine
   - Cloud Storage
   - Cloud Storage JSON API
   - Service Usage
   - Cloud Resource Manager API
   - NetApp Cloud Volumes Service
   - Service Consumer Management API
   - Service Networking API
   - Service Management API

The following video shows how to enable the APIs from the Google Cloud console.

► https://docs.netapp.com/us-en/astra-control-service/media/get-started/video-enable-gcp-apis.mp4 *(video)*

Create a service account

Astra Control Service uses a Google Cloud service account to facilitate Kubernetes application data management on your behalf.

Steps

1. Go to Google Cloud and create a service account by using the console, gcloud command, or another preferred method.

2. Grant the service account the following roles:
    - **Kubernetes Engine Admin** - Used to list clusters and create admin access to manage apps.
    - **NetApp Cloud Volumes Admin** - Used to manage persistent storage for apps.
    - **Storage Admin** - Used to manage buckets and objects for backups of apps.
    - **Service Usage Viewer** - Used to check if the required Cloud Volumes Service for Google Cloud APIs are enabled.
    - **Compute Network Viewer** - Used to check if the Kubernetes VPC is allowed to reach Cloud Volumes Service for Google Cloud.

If you'd like to use gcloud, you can follow steps from within the Astra Control interface. Click **Account > Credentials > Add Credentials**, and then click **Instructions**.

If you'd like to use the Google Cloud console, the following video shows how to create the service account from the console.

► https://docs.netapp.com/us-en/astra-control-service/media/get-started/video-create-gcp-service-

account.mp4 *(video)*

Configure the service account for a shared VPC

To manage GKE clusters that reside in one project, but use a VPC from a different project (a shared VPC), then you need to specify the Astra service account as a member of the host project with the **Compute Network Viewer** role.

Steps

1. From the Google Cloud console, go to **IAM & Admin** and select **Service Accounts**.
2. Find the Astra service account that has the required permissions and then copy the email address.
3. Go to your host project and then select **IAM & Admin** > **IAM**.
4. Click **Add** and add an entry for the service account.
    a. **New members**: Enter the email address for the service account.
    b. **Role**: Select **Compute Network Viewer**.
    c. Click **Save**.

Result

Adding a GKE cluster using a shared VPC will fully work with Astra.

Create a service account key

Instead of providing a user name and password to Astra Control Service, you'll provide a service account key when you add your first cluster. Astra Control Service uses the service account key to establish the identity of the service account that you just set up.

The service account key is plaintext stored in the JavaScript Object Notation (JSON) format. It contains information about the GCP resources that you have permission to access.

You can only view or download the JSON file when you create the key. However, you can create a new key at any time.

Steps

1. Go to Google Cloud and create a service account key by using the console, gcloud command, or another preferred method.
2. When prompted, save the service account key file in a secure location.

The following video shows how to create the service account key from the Google Cloud console.

► https://docs.netapp.com/us-en/astra-control-service/media/get-started/video-create-gcp-service-account-

key.mp4 *(video)*

Set up network peering for your VPC

The final step is to set up networking peering from your VPC to Cloud Volumes Service for Google Cloud.

The easiest way to set up network peering is by obtaining the gcloud commands directly from Cloud Volumes Service. The commands are available from Cloud Volumes Service when creating a new file system.

Steps

1. Go to NetApp Cloud Central's Global Regions Maps and identify the service type that you'll be using in the Google Cloud region where your cluster resides.

   Cloud Volumes Service provides two service types: CVS and CVS-Performance. Learn more about these service types.

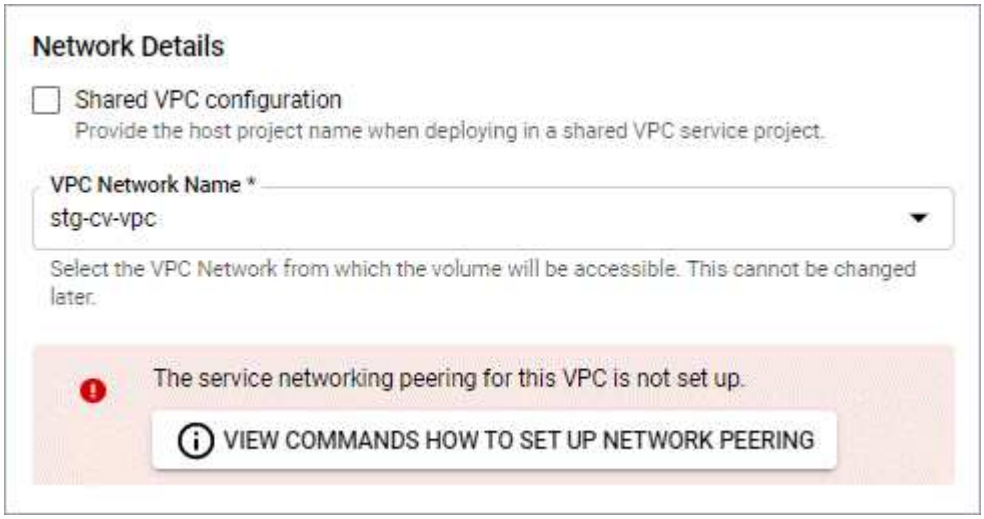
2. Go to Cloud Volumes in Google Cloud Platform.
3. On the **Volumes** page, click **Create**.
4. Under **Service Type**, select either **CVS** or **CVS-Performance**.

   You need to choose the correct service type for your Google Cloud region. This is the service type that you identified in step 1. After you select a service type, the list of regions on the page updates with the regions where that service type is supported.

   After this step, you'll only need to enter your networking information to obtain the commands.

5. Under **Region**, select your region and zone.
6. Under **Network Details**, select your VPC.

   If you haven't set up network peering, you'll see the following notification:



7. Click the button to view the network peering set up commands.
8. Copy the commands and run them in Cloud Shell.

   For more details about using these commands, refer to the Quickstart for Cloud Volumes Service for GCP.

   Learn more about configuring private services access and setting up network peering.

9. After you're done, you can click cancel on the **Create File System** page.

   We started creating this volume only to get the commands for network peering.

Set up Microsoft Azure

A few steps are required to prepare your Microsoft Azure subscription before you can manage Azure Kubernetes Service clusters with Astra Control Service.

Quick start for setting up Azure

Get started quickly by following these steps or scroll down to the remaining sections for full details.

[One] Review Astra Control Service requirements for Azure Kubernetes Service

Ensure that clusters are healthy and running Kubernetes version 1.17 or later, that node pools are online and running **Linux**, and more. Learn more about this step.

[Two] Register for Azure NetApp Files

Register the NetApp Resource Provider. Learn more about this step.

[Three] Create a NetApp account

In the Azure portal, go to Azure NetApp Files and create a NetApp account. Learn more about this step.

[Four] Set up capacity pools

Set up one or more capacity pools for your persistent volumes. Learn more about this step.

[Five] Delegate a subnet to Azure NetApp Files

Delegate a subnet to Azure NetApp Files so that Astra Control Service can create persistent volumes in that subnet. Learn more about this step.

[Six] Create an Azure service principal

Create an Azure service principal that has the Contributor role. Read step-by-step instructions.

AKS cluster requirements

A Kubernetes cluster must meet the following requirements so you can discover and manage it from Astra Control Service.

Kubernetes version
: Clusters must be running Kubernetes version 1.17 or later.

Image type
: The image type for all node pools must be Linux.

Cluster state
: Clusters must be running in a healthy state and have at least one online worker node with no worker nodes in a failed state.

Azure region

Clusters must reside in a region where Azure NetApp Files is available. View Azure products by region.

Subscription

Clusters must reside in a subscription where Azure NetApp Files is enabled. You'll choose a subscription when you register for Azure NetApp Files.

VNet

- Clusters must reside in a VNet that has direct access to an Azure NetApp Files delegated subnet. Learn how to set up a delegated subnet.
- If your Kubernetes clusters are in a VNet that's peered to the Azure NetApp Files delegated subnet that's in another VNet, then both sides of the peering connection must be online.
- Be aware that the default limit for the number of IPs used in a VNet (including immediately peered VNets) with Azure NetApp Files is 1,000. View Azure NetApp Files resource limits.

  If you're close to the limit, you have two options:

  - You can submit a request for a limit increase. Contact your NetApp representative if you need help.
  - When creating a new AKS cluster, specify a new network for the cluster. Once the new network is created, provision a new subnet and delegate the subnet to Azure NetApp Files.

Private networking

Private networking must not be enabled on a cluster.

External volume snapshot controller

Clusters must have a CSI volume snapshot controller installed. This controller is installed by default starting with K8s version 1.21, but you'll need to check on clusters running versions 1.17, 1.18, 1.19, or 1.20. Learn more about an external snapshot controller for on-demand volume snapshots.

Install a CSI volume snapshot controller

As noted in the list of requirements, Kubernetes clusters must have a CSI volume snapshot controller installed. Follow these steps to install the controller on your clusters.

Steps for K8s versions 1.17, 1.18, and 1.19

1. Install volume snapshot CRDs.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-
3.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshotclasses.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-
3.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshotcontents.yam
l
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-
3.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshots.yaml
```

2. Create the snapshot controller.

If you want the snapshot controller in a specific namespace, download and edit the following files before you apply them.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-3.0/deploy/kubernetes/snapshot-
controller/rbac-snapshot-controller.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-3.0/deploy/kubernetes/snapshot-
controller/setup-snapshot-controller.yaml
```

Steps for K8s version 1.20

1. Install volume snapshot CRDs.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-
snapshotter/v4.0.0/client/config/crd/snapshot.storage.k8s.io_volumesnaps
hotclasses.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-
snapshotter/v4.0.0/client/config/crd/snapshot.storage.k8s.io_volumesnaps
hotcontents.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-
snapshotter/v4.0.0/client/config/crd/snapshot.storage.k8s.io_volumesnaps
hots.yaml
```

2. Create the snapshot controller.

   If you want the snapshot controller in a specific namespace, download and edit the following files before you apply them.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/v4.0.0/deploy/kubernetes/snapshot-
controller/rbac-snapshot-controller.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/v4.0.0/deploy/kubernetes/snapshot-
controller/setup-snapshot-controller.yaml
```

Register for Azure NetApp Files

If you don’t have a Microsoft Azure account, begin by signing up for Microsoft Azure. Then, get access to Azure NetApp Files by registering the NetApp Resource Provider.

Steps

1. If you already have a Microsoft Azure account, skip to step 4.
2. Go to the Azure subscription page to subscribe to the Azure service.
3. Select a plan and follow the instructions to complete the subscription.
4. Log in to the Azure portal.
5. Follow Azure NetApp Files documentation to register the NetApp Resource Provider.

Create a NetApp account

After you've registered, create a NetApp account in Azure NetApp Files.

Step

1. Follow Azure NetApp Files documentation to create a NetApp account from the Azure portal.

Set up a capacity pool

One or more capacity pools are required so that Astra Control Service can provision persistent volumes in a capacity pool. Astra Control Service doesn't create capacity pools for you.

Take the following into consideration as you set up capacity pools for your Kubernetes apps:

- A capacity pool can have an Ultra, Premium, or Standard service level. Each of these service levels are designed for different performance needs. Astra Control Service supports all three.

  You need to set up a capacity pool for each service level that you want to use with your Kubernetes clusters.

  Learn more about service levels for Azure NetApp Files.

- Before you create a capacity pool for the apps that you intend to protect with Astra Control Service, choose the required performance and capacity for those apps.

  Provisioning the right amount of capacity ensures that users can create persistent volumes as they are needed. If capacity isn't available, then the persistent volumes can't be provisioned.

- An Azure NetApp Files capacity pool can use the manual or auto QoS type. Astra Control Service supports auto QoS capacity pools. Manual QoS capacity pools aren't supported.

Step

1. Follow Azure NetApp Files documentation to set up an auto QoS capacity pool.

Delegate a subnet to Azure NetApp Files

You need to delegate a subnet to Azure NetApp Files so that Astra Control Service can create persistent volumes in that subnet. Note that Azure NetApp Files enables you to have only one delegated subnet in a VNet.

If you're using peered VNets, then both sides of the peering connection must be online: the VNet where your Kubernetes clusters reside and the VNet that has the Azure NetApp Files delegated subnet.

Step

1. Follow the Azure NetApp Files documentation to delegate a subnet to Azure NetApp Files.

After you're done

Wait about 10 minutes before discovering the cluster running in the delegated subnet.

Create an Azure service principal

Astra Control Service requires a Azure service principal that is assigned the Contributor role. Astra Control Service uses this service principal to facilitate Kubernetes application data management on your behalf.

A service principal is an identity created specifically for use with applications, services, and tools. Assigning a role to the service principal restricts access to specific Azure resources.

Follow the steps below to create a service principal using the Azure CLI. You'll need to save the output in a JSON file and provide it to Astra Control Service later on. Refer to Azure documentation for more details about using the CLI.

The following steps assume that you have permission to create a service principal and that you have the Microsoft Azure SDK (az command) installed on your machine.

Requirements

- The service principal must use regular authentication. Certificates aren't supported.
- The service principal must be granted Contributor or Owner access to your Azure subscription.
- The Azure subscription must contain the AKS clusters and your Azure NetApp Files account.

Steps

1. Identify the subscription and tenant ID where your AKS clusters reside (these are the clusters that you want to manage in Astra Control Service).

   ```
   az configure --list-defaults
   az account list --output table
   ```

2. Create the service principal, assign the Contributor role, and specify the scope to the entire subscription where the clusters reside.

   ```
   az ad sp create-for-rbac --name http://sp-astra-service-principal --role
   contributor --scopes /subscriptions/SUBSCRIPTION-ID
   ```

3. Store the resulting Azure CLI output as a JSON file.

   You'll need to provide this file so that Astra Control Service can discover your AKS clusters and manage Kubernetes data management operations. Learn about managing credentials in Astra Control Service.

4. Optional: Add the subscription ID to the JSON file so that Astra Control Service automatically populates the ID when you select the file.

   Otherwise, you'll need to enter the subscription ID in Astra Control Service when prompted.

   Example

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Optional: Test your service principal.

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --subscription SUBSCRIPTION-ID
```

Register for an Astra Control account

Sign up to NetApp Cloud Central and then complete the registration process to obtain an Astra Control account.

Sign up to Cloud Central

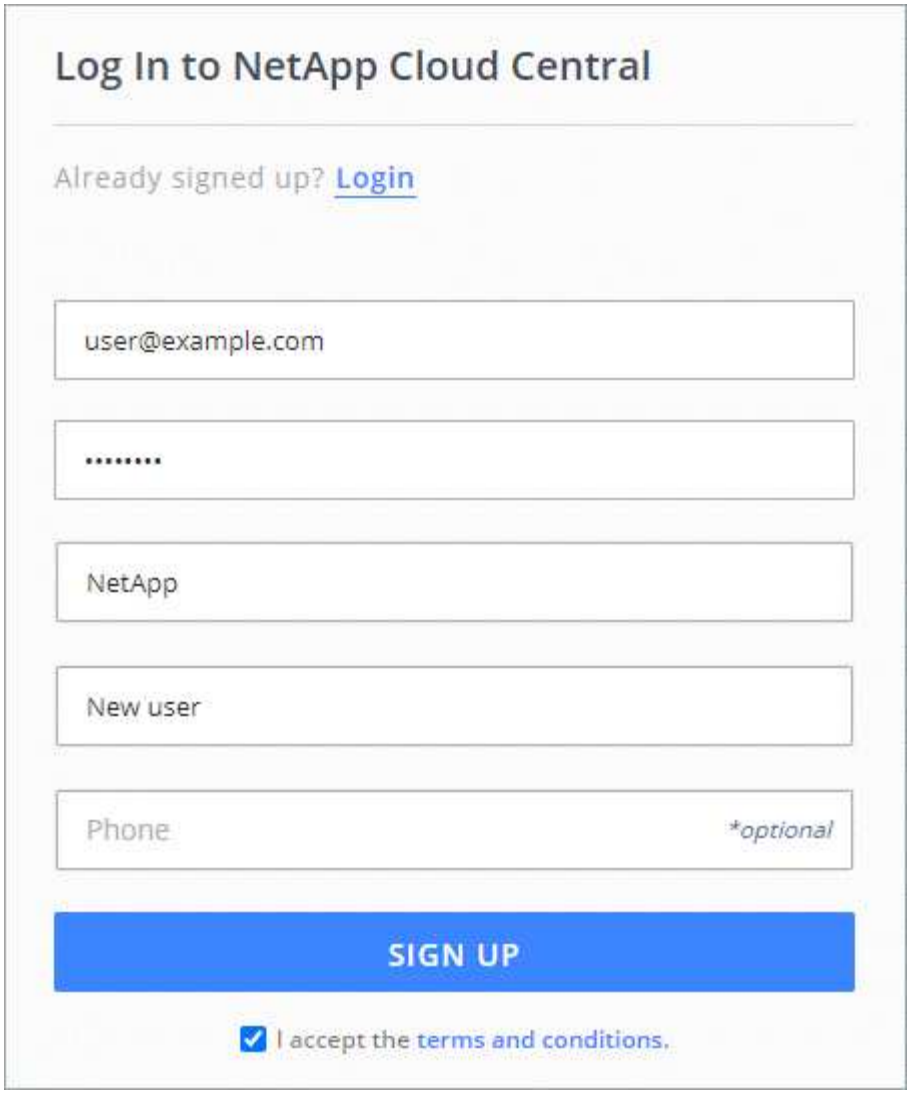
Astra Control Service is integrated within NetApp Cloud Central's authentication service. Sign up to Cloud Central so you can access Astra Control Service and NetApp's other cloud services.

You can use single sign-on to log in to Cloud Central using credentials from your corporate directory (federated identity). To learn more, go to the Cloud Central Help Center and then click **Cloud Central sign-in options**.

Steps

1. Open your web browser and go to NetApp Cloud Central.
2. In the top right, click **Sign up**.
3. Fill out the form and click **Sign up**.

The email address that you enter in this form is for your NetApp Cloud Central user ID. Use this Cloud Central user ID when you sign up for a new Astra Control account, or when an Astra Control admin invites you to an existing Astra Control account.



4. Wait for an email from NetApp Cloud Central.
5. Click the link in the email to verify your email address.

Result

You now have an active Cloud Central user login.

Register for an account

Before you can log in to Astra Control, you need to complete a registration process to obtain an Astra Control account.

When you use Astra Control, you'll manage your apps from within an account. An account includes users who can view and manage the apps within the account, as well as your billing details.

Steps

1. Go to the Astra Control page on Cloud Central.
2. Click **Get Started with Astra Control**.
3. Provide the required information in the form.

   A few important things to note as you fill out the form:

- Your business name and address must be accurate because we verify them to meet the requirements of Global Trade Compliance.
- The **Astra Account Name** is the name of your business's Astra Control account. You'll see this name in the Astra Control user interface. Note that you can create additional accounts (up to 5), if that's required for your needs.

4. Click **Submit**.

   If you're logged in to Cloud Central already, you'll see a registration status and then you'll be redirected to the Astra Control Dashboard. Otherwise, you'll be prompted to log in first.

   Now that you're registered, you can access Astra Control directly from https://astra.netapp.io.

Start managing Kubernetes clusters from Astra Control Service

After you set up your environment, you're ready to create a Kubernetes cluster and then add it to Astra Control Service.

Create a Kubernetes cluster

If you don't have a cluster yet, create one that meets Astra Control Service requirements for Google Kubernetes Engine (GKE) or Astra Control Service requirements for Azure Kubernetes Service (AKS).

Start managing Kubernetes clusters

After you log in to Astra Control Service, your first step is to start managing your clusters.

What you'll need

- For GKE, you should have the service account key file for a service account that has the required permissions. Learn how to set up a service account.
- For AKS, you should have the JSON file that contains the output from the Azure CLI when you created the service principal. Learn how to set up a service principal.

  You'll also need your Azure subscription ID, if you didn't add it to the JSON file.

Steps

1. On the Dashboard, click **Manage Kubernetes cluster**.

   Follow the prompts to add the cluster.

2. **Provider**: Select your cloud provider and then provide the required credentials.
   a. **Microsoft Azure**: Provide details about your Azure service principal by uploading a JSON file or by pasting the contents of that JSON file from your clipboard.

      The JSON file should contain the output from the Azure CLI when you created the service principal. It can also include your subscription ID so it's automatically added to Astra. Otherwise, you need to manually enter the ID after providing the JSON.

   b. **Google Cloud Platform**: Provide the service account key file either by uploading the file or by pasting the contents from your clipboard.

Astra Control Service uses the service account to discover clusters running in Google Kubernetes Engine.

3. **Cluster**: Select the cluster that you'd like to add.

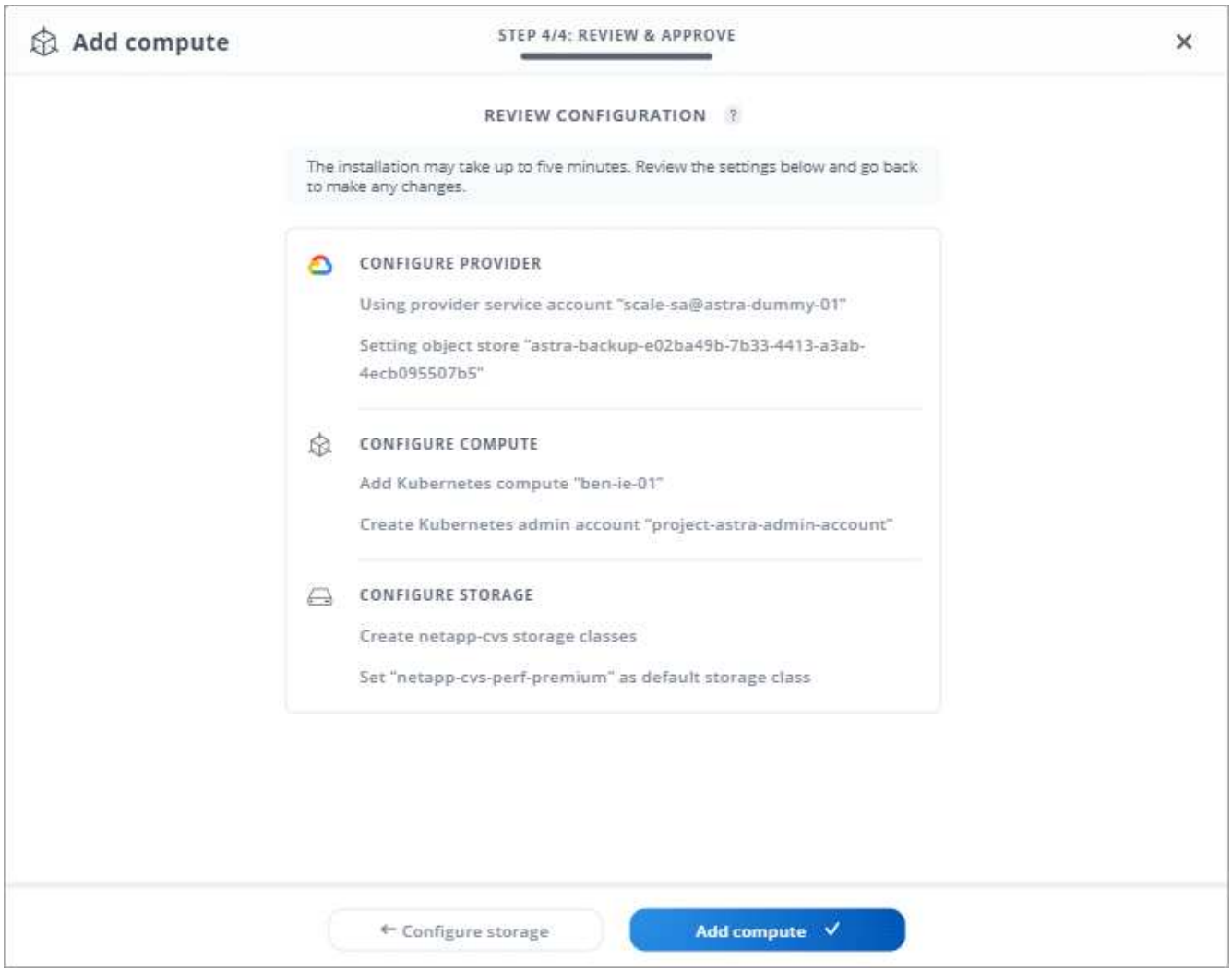
   Pay careful attention to the Eligible tab. If a warning appears, hover over the warning to determine if there's an issue with the cluster. For example, it might identify that the cluster doesn't have a worker node.

4. **Storage**: Select the storage class that you'd like Kubernetes applications deployed to this cluster to use by default.

   Each storage class utilizes Cloud Volumes Service for Google Cloud or Azure NetApp Files.

   - Learn about storage classes for GKE clusters.
   - Learn about storage classes for AKS clusters.

5. **Review & Approve**: Review the configuration details and click **Add cluster**.



The following video shows each of these steps for a GKE cluster.

► https://docs.netapp.com/us-en/astra-control-service/media/get-started/video-manage-cluster.mp4 *(video)*

Result

Astra Control Service creates an object store for application backups, creates an admin account on the cluster, and sets the default storage class that you specified. This process can take up to 5 minutes.

What's next?

Now that you've logged in and added a cluster to Astra Control, you're ready to start using Astra Control's application data management features.

- Start managing apps
- Protect apps
- Clone apps
- Set up billing
- Invite and manage users
- Manage cloud provider credentials
- Manage notifications

Astra Control Service videos

Many of the pages on this doc site include videos that show you how to complete a task for Astra Control Service. If you're just interested in videos, we've made it easy for you by collecting all of the videos on this single page (kind of like a playlist).

Videos for setting up Google Cloud

The following videos show how to complete set up requirements in Google Cloud before you can discover Kubernetes clusters running in GCP.

Enable APIs

Your project needs permissions to access specific Google Cloud APIs. The following video shows how to enable the APIs from the Google Cloud console. Learn more about enabling APIs.

► https://docs.netapp.com/us-en/astra-control-service/media/get-started/video-enable-gcp-apis.mp4 *(video)*

Create a service account

Astra Control Service uses a Google Cloud service account to facilitate Kubernetes application data management on your behalf. The following video shows how to create the service account from the Google Cloud console. Learn more about creating a service account.

► https://docs.netapp.com/us-en/astra-control-service/media/get-started/video-create-gcp-service-

account.mp4 *(video)*

Create a service account key

Astra Control Service uses a service account key to establish the identity of the service account that you just set up. The following video shows how to create the service account key from the Google Cloud console. Learn more about creating a service account key.

► https://docs.netapp.com/us-en/astra-control-service/media/get-started/video-create-gcp-service-account-

key.mp4 *(video)*

Videos for using Astra Control

The following videos show how to complete common tasks using Astra Control.

Manage clusters from Astra Control

After you log in to Astra Control Service, your first step is to add Kubernetes compute. Learn more about managing clusters.

► https://docs.netapp.com/us-en/astra-control-service/media/get-started/video-manage-cluster.mp4 *(video)*

Configure a protection policy

A protection policy protects an app by creating snapshots, backups, or both at a defined schedule. You can choose to create snapshots and backups hourly, daily, weekly, and monthly, and you can specify the number of copies to retain. Learn more about configuring protection policies.

► https://docs.netapp.com/us-en/astra-control-service/media/use/video-set-protection-policy.mp4 *(video)*

Frequently asked questions for Astra Control Service

This FAQ can help if you're just looking for a quick answer to a question.

Overview

Astra Control aims to simplify your application data lifecycle management operations for Kubernetes native applications. Astra Control Service supports Kubernetes clusters running on Google Kubernetes Engine (GKE) and Azure Kubernetes Service (AKS).

The following sections provide answers to some additional questions that you might come across as you use Astra Control. For any additional clarifications, please reach out to astra.feedback@netapp.com

Access to Astra Control

Why do I need to provide so many details when registering for Astra Control?

Astra Control requires accurate customer information when registering. This information is required to go through a Global Trade Compliance (GTC) check.

Why am I getting a "Registration Failed" error when registering for Astra Control?

Astra Control requires you to provide accurate customer information in the onboarding section. You will get a "Registration Failed" error if you provided incorrect information. Other accounts that you are a member of also get locked.

What's the Astra Control Service URL?

You can access Astra Control Service at https://astra.netapp.io.

I sent an email invitation to a colleague, but they haven't received it. What should I do?

Ask them to check their spam folder for an email from do-not-reply@netapp.com, or search their inbox for

"invitation." You can also remove the user and attempt to re-add them.

I upgraded to the Premium PayGO Plan from the Free Plan. Will I get charged for the first 10 applications?

Yes. After upgrading to the Premium Plan, Astra Control starts charging you for all managed applications in your account.

I upgraded to the Premium PayGO Plan in the middle of a month. Will I get charged for the entire month?

No, billing starts from the time that you upgraded to the Premium Plan.

I am using the Free Plan, will I get charged for the Persistent Volume Claims?

Yes, you will be charged for the Persistent Volumes used by GKE clusters from Cloud Volumes Service for Google Cloud or by AKS clusters from Azure NetApp Files.

Registering Kubernetes clusters

Do I need to install CSI drivers on my cluster before adding it to Astra Control Service?

No. When your cluster is added to Astra Control, the service will automatically install NetApp's Trident Container Storage Interface (CSI) driver on the Kubernetes cluster. This CSI driver is used to provision persistent volumes for GKE clusters backed by NetApp Cloud Volumes Service for Google Cloud, and for AKS clusters backed by Azure NetApp Files.

I need to add worker nodes to my cluster after adding to Astra Control Service. What should I do?

New worker nodes can be added to existing pools, or new pools can be created as long as they are the Ubuntu image type. These will be automatically discovered by Astra Control. If the new nodes are not visible in Astra Control, check if the new worker nodes are running the supported image type. You can also verify the health of the new worker nodes by using the `kubectl get nodes` command.

Registering GKE clusters

Can I add a private GKE cluster to Astra Control Service?

Yes, you can add private clusters to Astra Control Service. To create a Google Kubernetes Engine (GKE) private cluster, follow the instructions in this knowledgebase article.

Private clusters must have the authorized networks set to allow the Astra Control IP addresses:

- 54.164.233.140/32
- 3.218.120.204/32
- 34.193.99.138/32

Can my GKE cluster reside on a shared VPC?

Yes, Astra Control can manage clusters that reside in a shared VPC. Learn how to set up the Astra service account for a shared VPC configuration.

Where can I find my service account credentials on GCP?

After you log in to the Google Cloud Console, your service account details will be in the **IAM and Admin** section. For more details, refer to how to set up Google Cloud for Astra Control.

I would like to add different GKE clusters from different GCP projects. Is this supported in Astra Control?

No, this isn't a supported configuration. Only a single GCP project is supported.

Removing clusters

How do I properly unregister, bring down a cluster, and delete the associated volumes?

1. Unmanage the applications from Astra Control.
2. Unregister the cluster from Astra Control.
3. Delete the persistent volume claims.
4. Delete the cluster.

What happens to my applications and data after removing the cluster from Astra Control?

Removing a cluster from Astra Control will not make any changes to the cluster's configuration (applications and persistent storage). Any Astra Control snapshots or backups taken of applications on that cluster will be unavailable to restore. Volume snapshot data stored within the backend storage will not be removed. Persistent Storage backups created by Astra Control will remain within your cloud provider's object store, but they are unavailable for restore.

Always remove a cluster from Astra Control before you delete it through GCP. Deleting a cluster from GCP while it's still being managed by Astra Control can cause problems for your Astra Control account.

Will Astra Trident be uninstalled when I remove a cluster from Astra Control?

Astra Trident will not be uninstalled from a cluster when you remove it from Astra Control.

Managing applications

Can Astra Control deploy an application?

Astra Control doesn't deploy applications. Applications must be deployed outside of Astra Control.

My application is not showing up on the Discovered Apps list. What can I check to identify the problem?

When applications are not listed in **Discovered Apps**, check the status and health of the Kubernetes pod by running `kubectl get pod -A |grep [pod name]`. If the pods are healthy and running, check to see if the application is listed under **Ignored Apps**.

Can Astra Control manage an application that is on non-NetApp storage?

No. While Astra Control can discover applications that are using non-NetApp storage, it can't manage an application that's using non-NetApp storage.

I don't see any of my application's PVCs bound to GCP CVS. What's wrong?

The Astra Trident operator sets the default storage class to `netapp-cvs-premium` after it's successfully added to Astra Control. When an application's PVCs are not bound to Cloud Volumes Service for Google Cloud, there are a few steps that you can take:

- Run `kubectl get sc` and check the default storage class.
- Check the yaml file or Helm chart that was used to deploy the application and see if a different storage class is defined.
- Check to make sure that the worker node image type is Ubuntu and the NFS mount succeeded.

What happens to applications after I stop managing them from Astra Control?

Any existing backups or snapshots will be deleted. Applications and data remain available. Data management operations will not be available for unmanaged applications or any backups or snapshots that belong to it.

Data management operations

Where does Astra Control create the object store bucket?

The geography of the first managed cluster determines the location of the object store. For example, if the first cluster that you add is in a European zone, then the bucket is created in that same geography. If needed, you can add additional buckets.

There are snapshots in my account that I didn't create. Where did they come from?

In some situations, Astra Control will automatically create a snapshot as part of performing another process. If these snapshots are more than a few minutes old, you can safely delete them.

My application uses several PVs. Will Astra Control take snapshots and backups of all these PVCs?

Yes. A snapshot operation on an application by Astra Control includes snapshot of all the PVs that are bound to the application's PVCs.

Can I manage snapshots taken by Astra Control directly through my cloud provider?

No. Snapshots and backups taken by Astra Control can only be managed with Astra Control.