Astra Control Service documentation

Astra

NetApp
August 10, 2021

This PDF was generated from https://docs.netapp.com/us-en/astra/index.html on August 10, 2021.
Always check docs.netapp.com for the latest.

Table of Contents

Astra Control Service documentation . . . 1
Release notes . . . 2
- What's new with Astra Control Service . . . 2
- Known issues . . . 6
- Known limitations . . . 6

Get started . . . 8
- Intro to Astra Control . . . 8
- Supported Kubernetes deployments . . . 10
- Quick start for Astra Control Service . . . 10
- Set up your cloud provider . . . 11
- Register for an Astra Control account . . . 22
- Start managing Kubernetes compute from Astra Control Service . . . 24
- What's next? . . . 26
- Astra Control Service videos . . . 26
- Frequently asked questions for Astra Control Service . . . 27

Use Astra Control Service . . . 31
- Log in to Astra Control Service . . . 31
- Manage and protect apps . . . 31
- View app and compute health . . . 44
- Manage buckets . . . 48
- Manage your account . . . 51
- Unmanage apps and compute . . . 59

Automation using the Astra Control REST API . . . 62

Concepts . . . 63
- Architecture and components . . . 63
- Storage classes and PV size for AKS clusters . . . 64
- Service type, storage classes, and PV size for GKE clusters . . . 65
- Validated vs standard apps . . . 67
- Define a custom app . . . 67

Deploy apps . . . 70
- Deploy Jenkins from a Helm chart . . . 70
- Deploy MariaDB from a Helm chart . . . 71
- Deploy MySQL from a Helm chart . . . 72
- Deploy Postgres from a Helm chart . . . 73

Knowledge and support . . . 75
- Register for support . . . 75
- Get help . . . 78

Legal notices . . . 80
- Copyright . . . 80
- Trademarks . . . 80
- Patents . . . 80
- Privacy policy . . . 80
- Astra Control API license . . . 80

Open source 80

Astra Control Service documentation

Release notes

What's new with Astra Control Service

NetApp periodically updates Astra Control Service to bring you new features, enhancements, and bug fixes.

5 Aug 2021

This release includes the following new features and enhancements.

Astra Control Center

Astra Control is now available in a new deployment model. *Astra Control Center* is self-managed software that you install and operate in your data center so that you can manage Kubernetes application lifecycle management for on-premise Kubernetes clusters.

Go to the Astra Control Center documentation to learn more.

Bring your own bucket

You can now manage the buckets that Astra uses for backups and clones by adding additional buckets and by changing the default bucket for the Kubernetes clusters in your cloud provider.

Learn more about managing buckets.

2 June 2021

This release includes bug fixes and the following enhancements to Google Cloud support.

Support for shared VPCs

You can now manage GKE clusters in GCP projects with a shared VPC network configuration.

Persistent volume size for the CVS service type

Astra Control Service now creates persistent volumes with a minimum size of 300 GiB when using the CVS service type.

Learn how Astra Control Service uses Cloud Volumes Service for Google Cloud as the backend storage for persistent volumes.

Support for Container-Optimized OS

Container-Optimized OS is now supported with GKE worker nodes. This is in addition to support for Ubuntu.

Learn more about GKE cluster requirements.

15 Apr 2021

This release includes the following new features and enhancements.

Support for AKS clusters

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

Learn how to get started.

REST API

The Astra Control REST API is now available for use. The API is based on modern technologies and current best practices.

Learn how to automate application data lifecycle management using the REST API.

Annual subscription

Astra Control Service now offers a *Premium Subscription*.

Pre-pay at a discounted rate with an annual subscription that enables you to manage up to 10 apps per *application pack*. Contact NetApp Sales to purchase as many packs as needed for your organization—for example, purchase 3 packs to manage 30 apps from Astra Control Service.

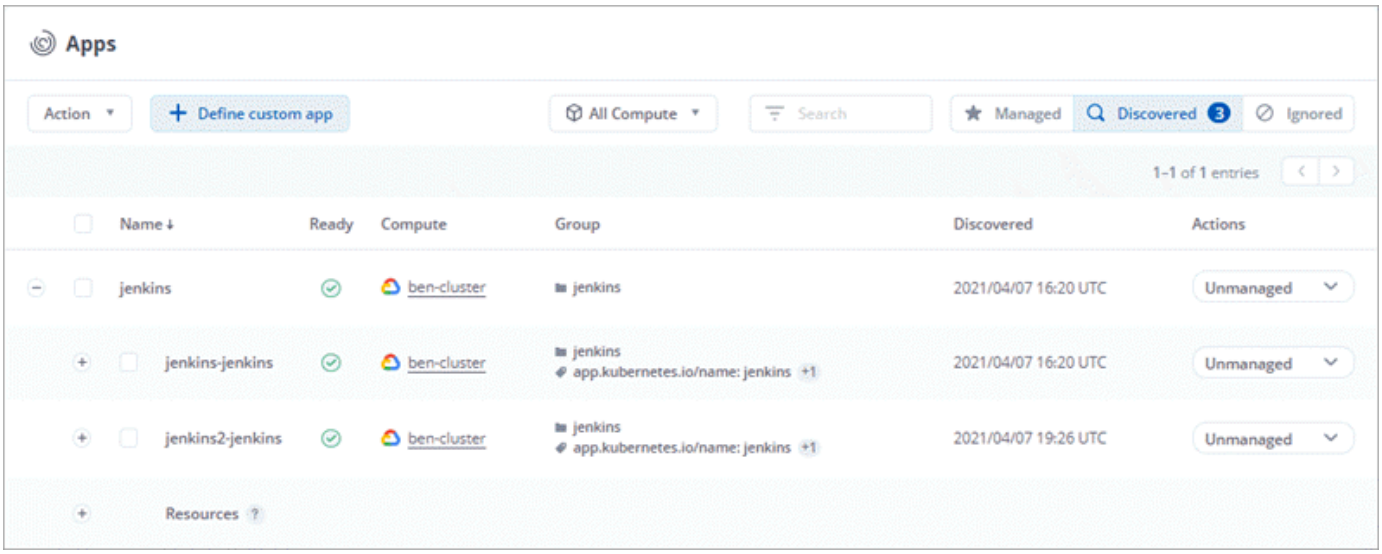
If you manage more apps than allowed by your annual subscription, then you'll be charged at the overage rate of $0.005 per minute, per application (the same as Premium PayGo).

Learn more about Astra Control Service pricing.

Namespace and app visualization

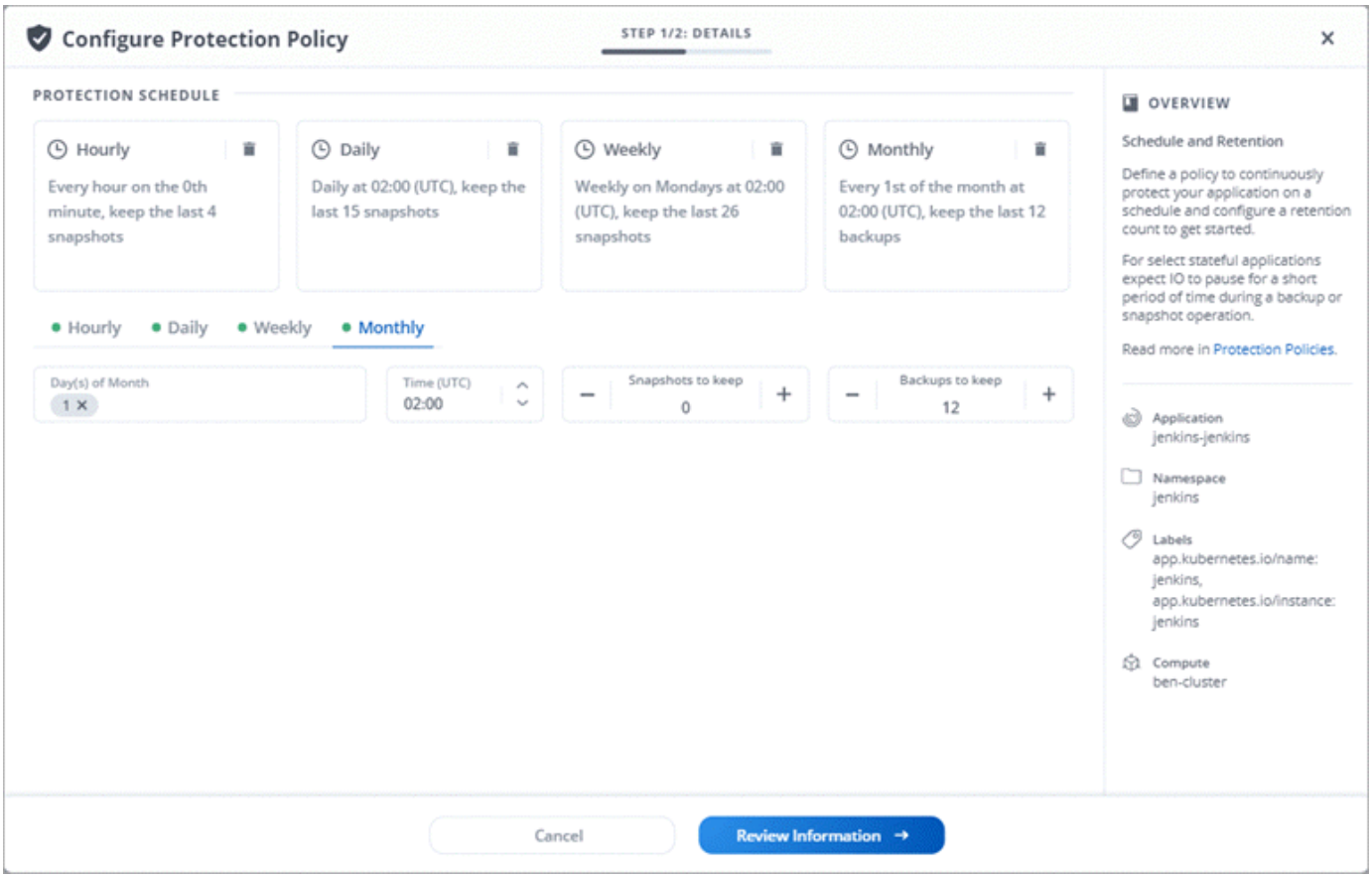
We enhanced the Discovered Apps page to better show the hierarchy between namespaces and apps. Just expand a namespace to see the apps contained in that namespace.

Learn more about managing apps.



User interface enhancements

Data protection wizards were enhanced for ease of use. For example, we refined the Protection Policy wizard to more easily view the protection schedule as you define it.



Activity enhancements

We’ve made it easier to view details about the activities in your Astra Control account.

- Filter the activity list by managed app, severity level, user, and time range.
- Download your Astra Control account activity to a CSV file.
- View activities directly from the Compute page or the Apps page after selecting compute or an app.

Learn more about viewing your account activity.

1 Mar 2021

Astra Control Service now supports the *CVS* service type with Cloud Volumes Service for Google Cloud. This is in addition to already supporting the *CVS-Performance* service type. Just as a reminder, Astra Control Service uses Cloud Volumes Service for Google Cloud as the backend storage for your persistent volumes.

This enhancement means that Astra Control Service can now manage app data for Kubernetes clusters that are running in *any* Google Cloud region where Cloud Volumes Service is supported.

If you have the flexibility to choose between Google Cloud regions, then you can pick either CVS or CVS-Performance, depending on your performance requirements. Learn more about choosing a service type.

25 Jan 2021

We’re pleased to announce that Astra Control Service is now Generally Available. We incorporated a lot of the feedback that we received from the Beta release and made a few other notable enhancements.

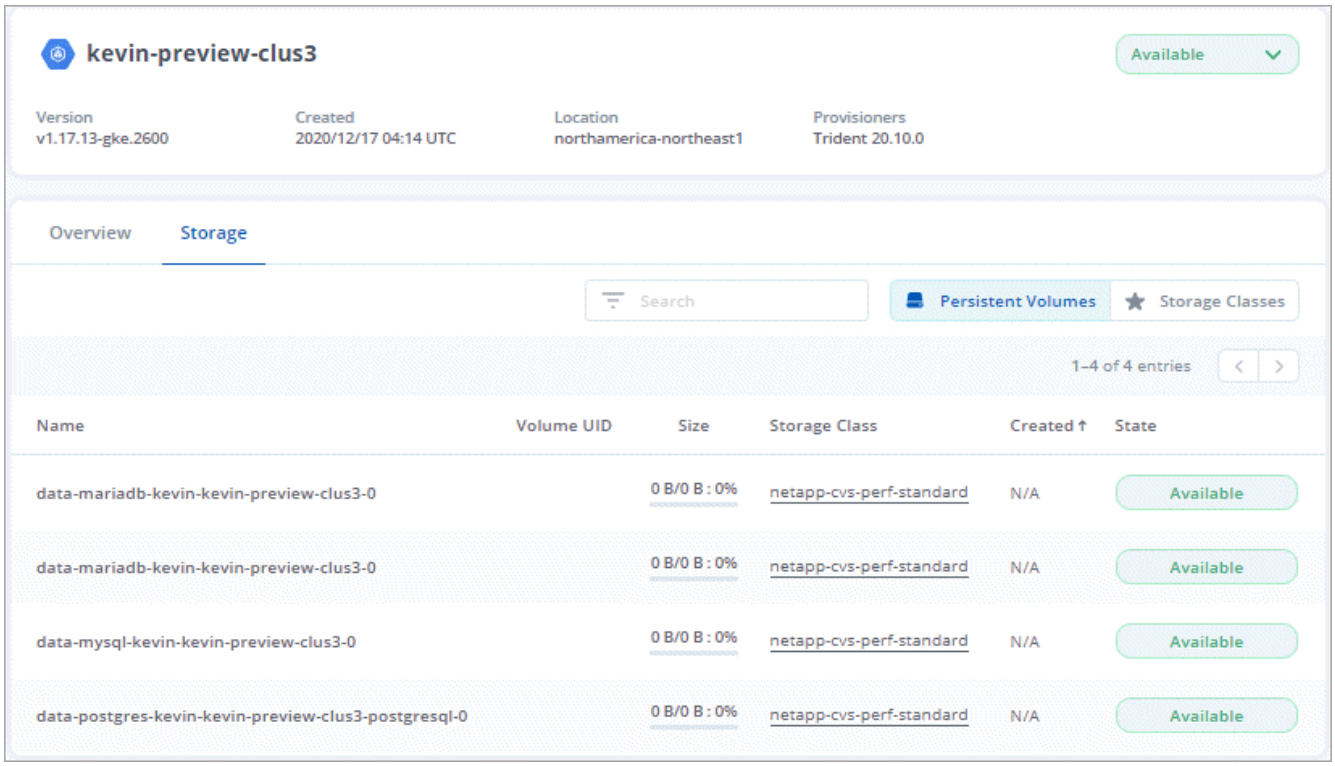
- Billing is now available, which enables you to move from the Free Plan to the Premium Plan. Learn more about billing.
- Astra Control Service now creates Persistent Volumes with a minimum size of 100 GiB when using the CVS-Performance service type.
- Astra Control Service can now discover apps faster.
- You can now create and delete accounts on your own.
- We've improved notifications when Astra Control Service can no longer access Kubernetes compute.

  These notifications are important because Astra Control Service can't manage apps for disconnected compute.

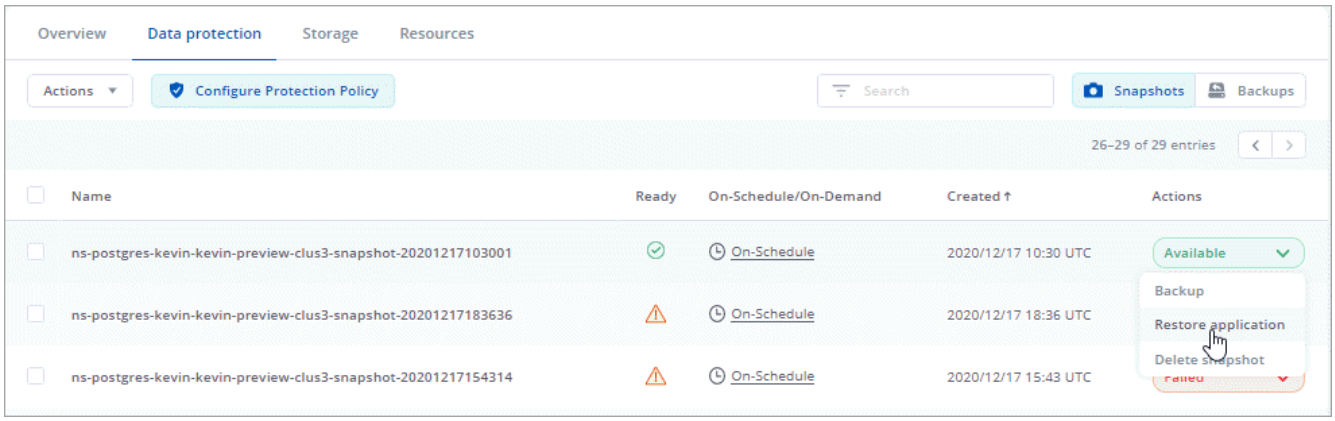
17 Dec 2020 (Beta update)

We primarily focused on bug fixes to improve your experience, but we made a few other notable enhancements:

- When you add your first Kubernetes compute to Astra Control Service, the object store is now created in the geography where the cluster resides.
- Details about persistent volumes is now available when you view storage details at the compute level.



- We added an option to restore an application from an existing snapshot or backup.



- If you delete a Kubernetes cluster that Astra Control Service is managing, the cluster now shows up in a **Removed** state. You can then remove the cluster from Astra Control Service.
- Account owners can now modify the assigned roles for other users.
- We added a section for billing, which will be enabled when Astra Control Service is released for General Availability (GA).

Known issues

Known issues identify problems that might prevent you from using this release of the product successfully.

Backup taken from new snapshot instead of existing snapshot

When you create a backup and select **Backup from existing snapshot**, Astra Control creates an ad-hoc snapshot and uses that snapshot to create the backup. Astra Control doesn't use the existing snapshot.

Clone performance impacted by large persistent volumes

Clones of very large and consumed persistent volumes might be intermittently slow, dependent on cluster access to the object store. If the clone is hung and no data has been copied for more than 30 minutes, Astra Control terminates the clone action.

Known limitations

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

General limitations

The following limitations affect Astra Control Service's management of Kubernetes clusters in any supported Kubernetes deployment.

Unhealthy pods affect app management

If a managed app has pods in an unhealthy state, Astra Control Service can't create new backups and clones.

Trident isn't uninstalled from a cluster

When you unmanage a cluster from Astra Control Service, Trident isn't automatically uninstalled from the

cluster. To uninstall Trident, you'll need to follow these steps in the Trident documentation.

Existing connections to a Postgres pod causes failures

When you perform operations on Postgres pods, you shouldn't connect directly within the pod to use the psql command. Astra Control Service requires psql access to freeze and thaw the databases. If there is a pre-existing connection, the snapshot, backup, or clone will fail.

Limitations for management of GKE clusters

The following limitations apply to the management of Kubernetes clusters in Google Kubernetes Engine (GKE).

One GCP project and one service account are supported

Astra Control Service supports one Google Cloud Platform project and one service account. You should not add more than one service account to Astra Control Service and you shouldn't rotate service account credentials.

Google Marketplace apps haven't been validated

NetApp hasn't validated apps that were deployed from the Google Marketplace. Some users report issues with discovery or back up of Postgres, MariaDB, and MySQL apps that were deployed from the Google Marketplace.

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

Persistent volume limit

You can have up to 100 volumes per Google Cloud region. If you reach this limit, creation of new clones or volumes will fail. Contact support to increase the volume limit.

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

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 supports all applications running on your Kubernetes clusters. 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.

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 NetApp's Trident on the cluster and to create one or more storage classes.
  - Uses 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.
  - Learn about storage classes for GKE clusters.
  - Learn about storage classes for AKS clusters.
- 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 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.

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.

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.

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.

Add compute to Astra Control

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

Learn more about adding compute.

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.

1 Review Astra Control Service requirements for Google Kubernetes Engine

Ensure that clusters are healthy and running a Kubernetes version in the range of 1.17 to 1.20, that worker nodes are online and running Container-Optimized OS or Ubuntu, and more. Learn more about this step.

2 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.

3 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.

4 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.

5 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.

6 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 1.17 to 1.20.

Image type

The image type for each worker node must be Container-Optimized OS or Ubuntu.

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/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/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/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.

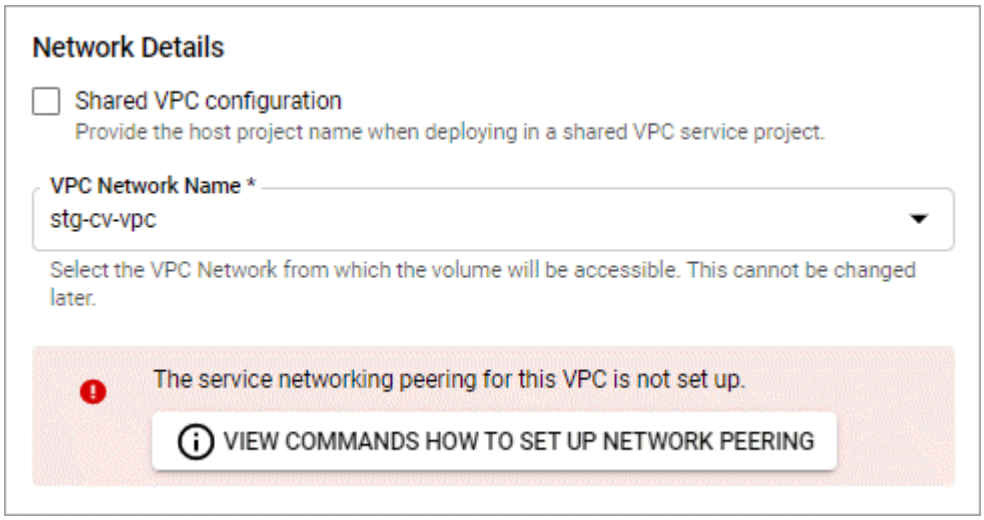
2. Go to Cloud Volumes in Google Cloud Platform.
3. On the **Volumes** page, click **Create**.
4. Under **Service Type**, select either **CVS** or **CVS-Performance**.

   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.

1. **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.

2. **Register for Azure NetApp Files**

Request access to the Azure NetApp Files service and then register the NetApp Resource Provider. Learn more about this step.

3. **Create a NetApp account**

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

4. **Set up capacity pools**

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

5. **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.

6. **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

Get access to Azure NetApp Files by submitting a waitlist request. After you're approved, you'll need to register the NetApp Resource Provider.

Steps

1. Submit a waitlist request to access Azure NetApp Files.
2. Wait for a confirmation email from the Azure NetApp Files team.
3. Follow Azure NetApp Files documentation to register the NetApp Resource Provider.

Create a NetApp account

After you've been granted access, 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 compute 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

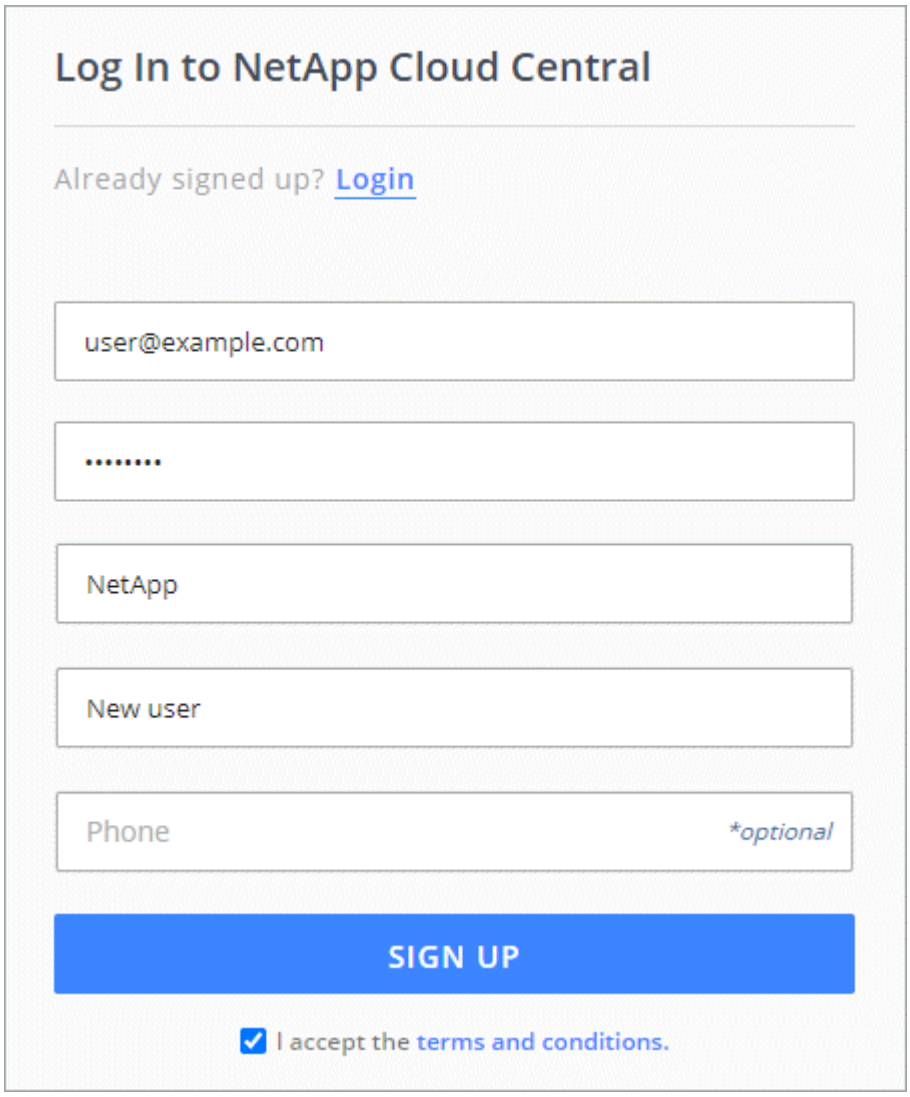
Astra Control Service is integrated within NetApp Cloud Central's authentication service. Sign up to Cloud Central so you can access Astra Control Service and NetApp's other cloud services.

> 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 **Sign up for the Free Plan**.
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 compute 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 compute

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

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 compute**.

   Follow the prompts to add the compute.

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 compute running in Google Kubernetes Engine.

3. **Compute**: Select the compute that you'd like to add.

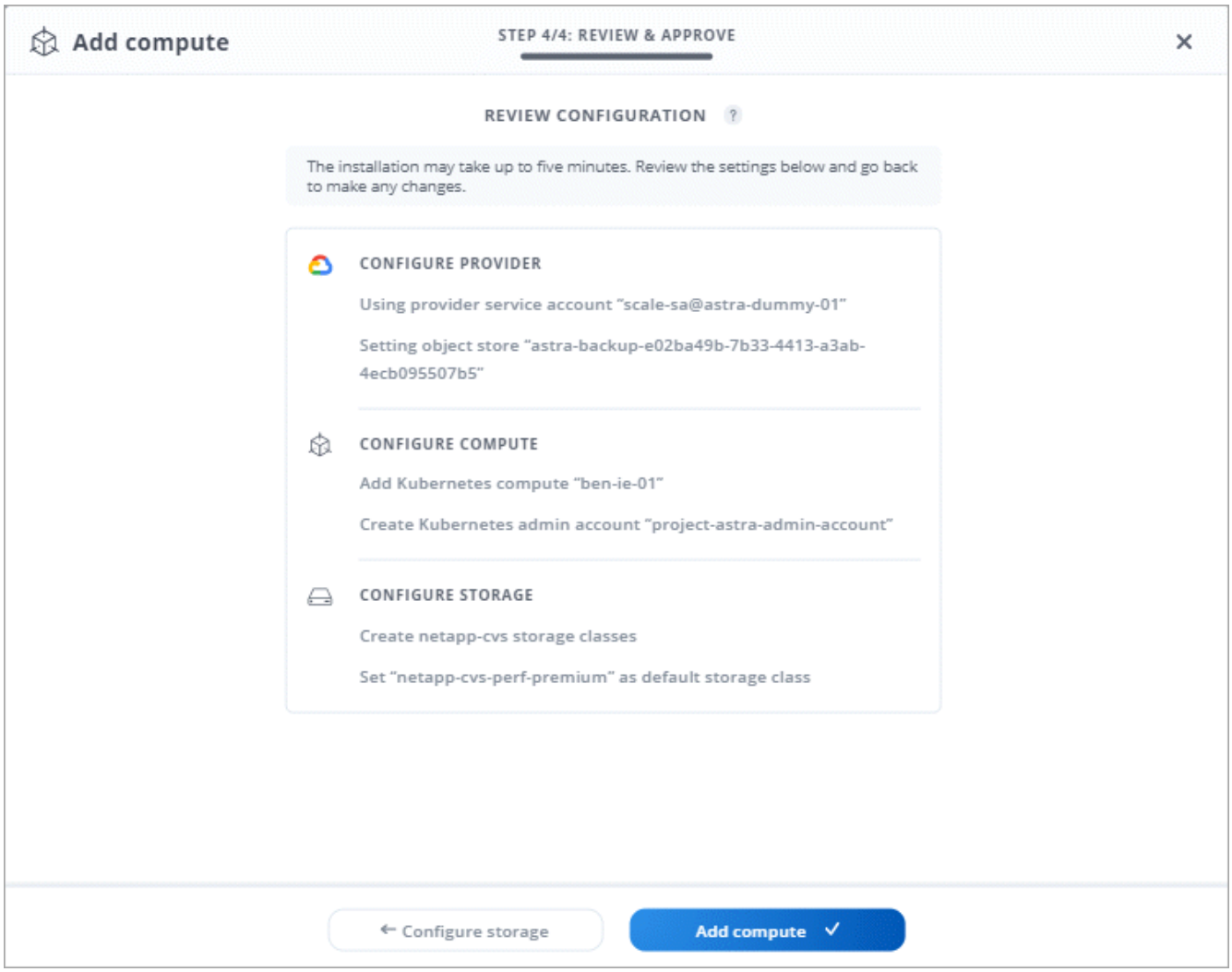
   Pay careful attention to the Eligible tab. If a warning appears, hover over the warning to determine if there's an issue with the compute. For example, it might identify that the cluster doesn't have a worker node.

4. **Storage**: Select the storage class that you'd like Kubernetes applications deployed to this compute 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 compute**.



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

▶ https://docs.netapp.com/us-en/astra/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 compute 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/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/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/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 compute from Astra Control

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

▶ https://docs.netapp.com/us-en/astra/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/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 NetApp Trident be uninstalled when I remove a cluster from Astra Control?

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 NetApp 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.

Use Astra Control Service

Log in to Astra Control Service

Astra Control Service is accessible through a SaaS-based user interface by going to https://astra.netapp.io.

> You can use single sign-on to log in 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**.

What you'll need

- A Cloud Central user ID.
- A new Astra Control account or an invitation to an existing account.
- A supported web browser.

  Astra Control Service supports recent versions of Firefox, Safari, and Chrome with a minimum resolution of 1280 x 720.

Steps

1. Open a web browser and go to https://astra.netapp.io.
2. Log in using your NetApp Cloud Central credentials.

Manage and protect apps

Start managing apps

After you add Kubernetes compute to Astra Control, you can install apps on the cluster (outside of Astra Control), and then go to the Apps page in Astra Control to start managing the apps.

Install apps on your cluster

Now that you've added your compute to Astra Control, you can install apps on the cluster. Persistent volumes will be provisioned on the new storage classes by default. After the pods are online, you can manage the app with Astra Control.

Astra Control will manage stateful apps only if the storage is on a storage class installed by Astra Control.

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

For help with deploying common applications from Helm charts, refer to the following:

- Deploy MariaDB from a Helm chart
- Deploy MySQL from a Helm chart
- Deploy Postgres from a Helm chart
- Deploy Jenkins from a Helm chart

Manage apps

Astra Control enables you to manage your apps at the namespace level or by Kubernetes label.

Manage apps by namespace

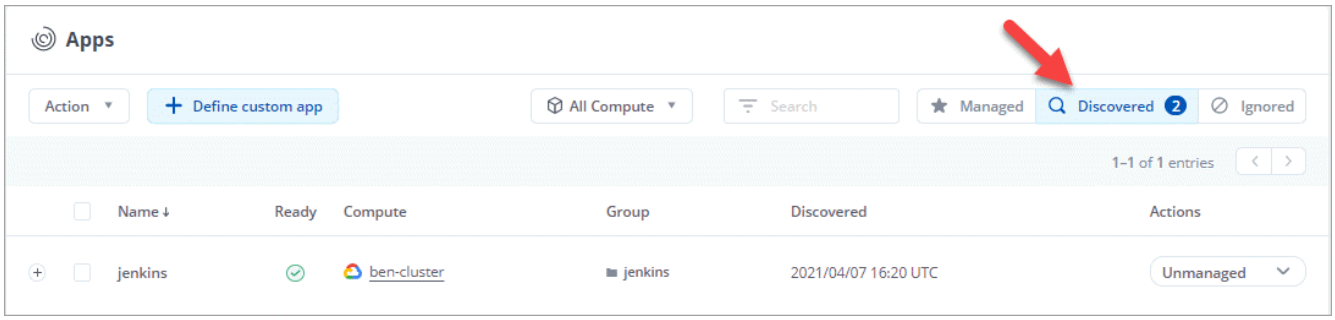
The **Discovered** section of the Apps page shows namespaces and the Helm-installed apps or custom-labeled apps in those namespaces. You can choose to manage each app individually or at the namespace level. It all comes down to the level of granularity that you need for data protection operations.

For example, you might want to set a backup policy for "maria" that has a weekly cadence, but you might need to back up "mariadb" (which is in the same namespace) more frequently than that. Based on those needs, you would need to manage the apps separately and not under a single namespace.

While Astra Control allows you to separately manage both levels of the hierarchy (the namespace and the apps in that namespace), the best practice is to choose one or the other. Actions that you take in Astra Control can fail if the actions take place at the same time at both the namespace and app level.

Steps

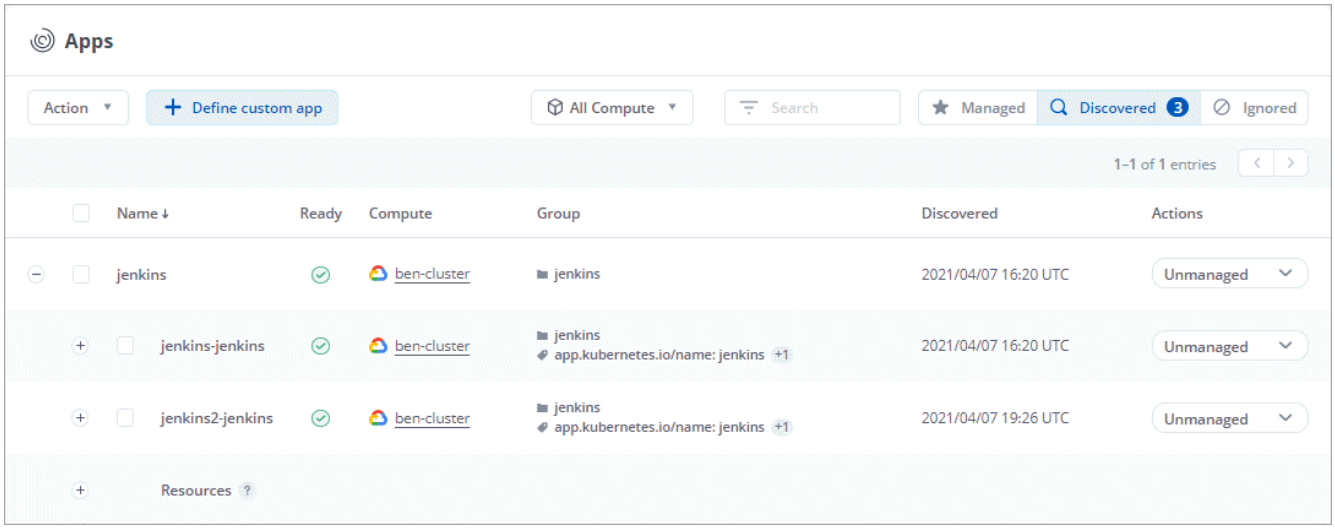
1. Click **Apps** and then click **Discovered**.



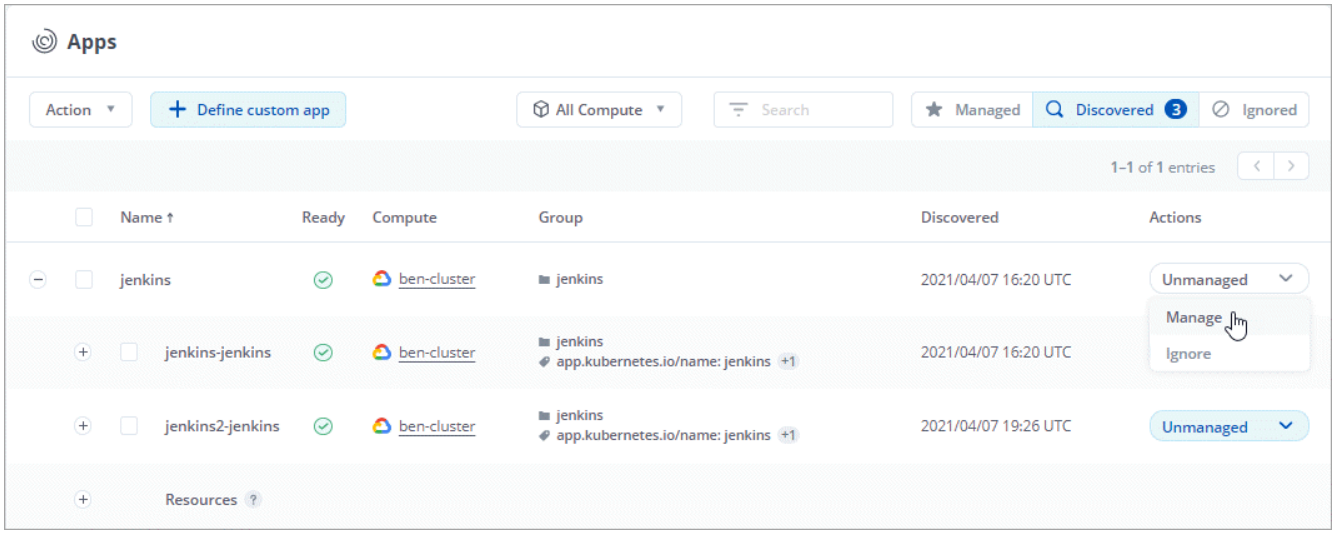
2. View the list of discovered namespaces and expand a namespace to view the apps and associated resources.

   Astra Control shows you Helm apps and custom-labeled apps in namespace. If Helm labels are available, they're designated with a tag icon.

   Here's an example with two apps in a namespace:

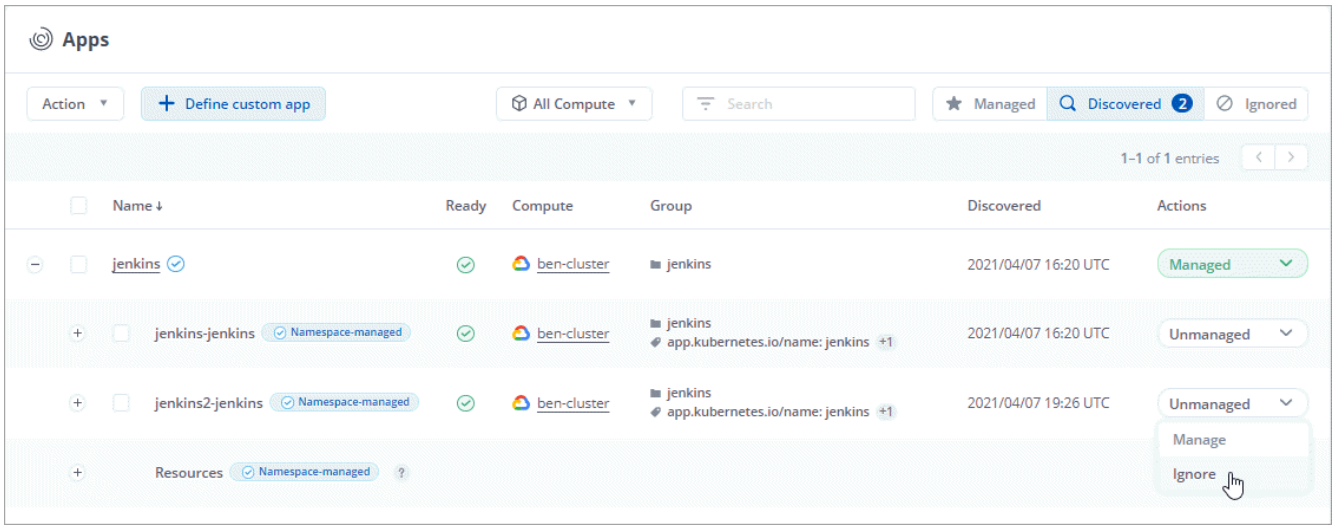


3. Decide whether you want to manage each app individually or at the namespace level.
4. At the desired level in the hierarchy, click the drop-down list in the **Actions** column and click **Manage**.



5. If you don't want to manage an app, click the drop-down list in the **Actions** column for the desired app and click **Ignore**.

   For example, if you wanted to manage all apps under the "jenkins" namespace together so that they have the same snapshot and backup policies, you would manage the namespace and ignore the apps in the namespace:



Result

Apps that you chose to manage are now available from the **Managed** tab. Any ignored apps will move to the **Ignored** tab. Ideally, the Discovered tab will show zero apps, so that as new apps are installed, they are easier to find and manage.

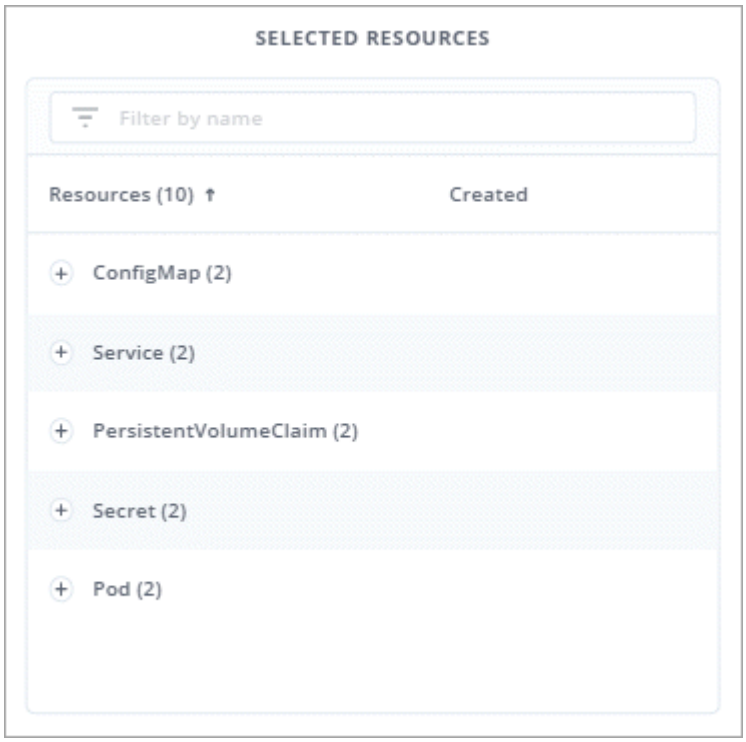
Manage apps by Kubernetes label

Astra Control includes an action at the top of the Apps page named **Define custom app**. You can use this action to manage apps that are identified with a Kubernetes label. Learn more about defining apps by Kubernetes label.

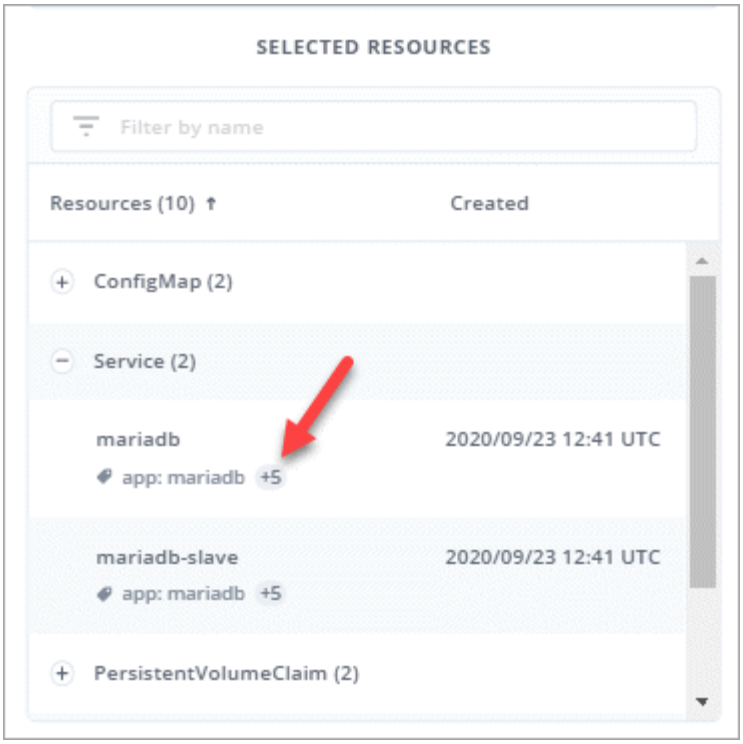
Steps

1. Click **Apps > Define custom app**.
2. In the **Define Custom Application** dialog box, provide the required information to manage the app:
   a. **New App**: Enter the display name of the app.
   b. **Compute**: Select the compute where the app resides.
   c. **Namespace:** Select the namespace for the app.
   d. **Label:** Enter a label or select a label from the resources below.
   e. **Selected Resources**: View and manage the selected Kubernetes resources that you'd like to protect (pods, secrets, persistent volumes, and more).

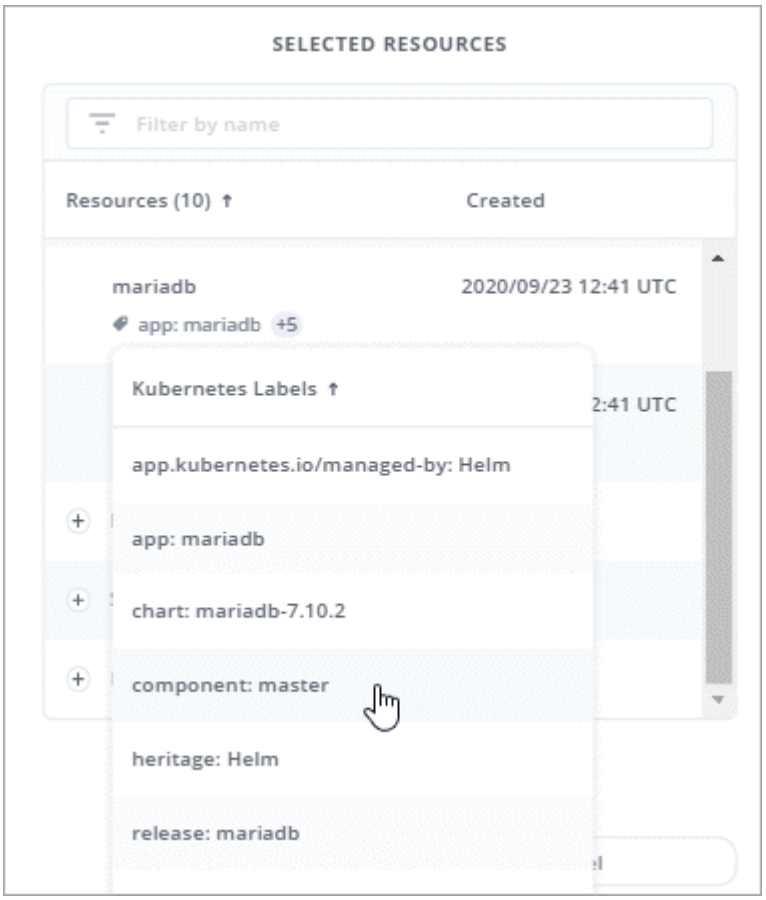
      Here's an example:



      - View the available labels by expanding a resource and clicking the number of labels.

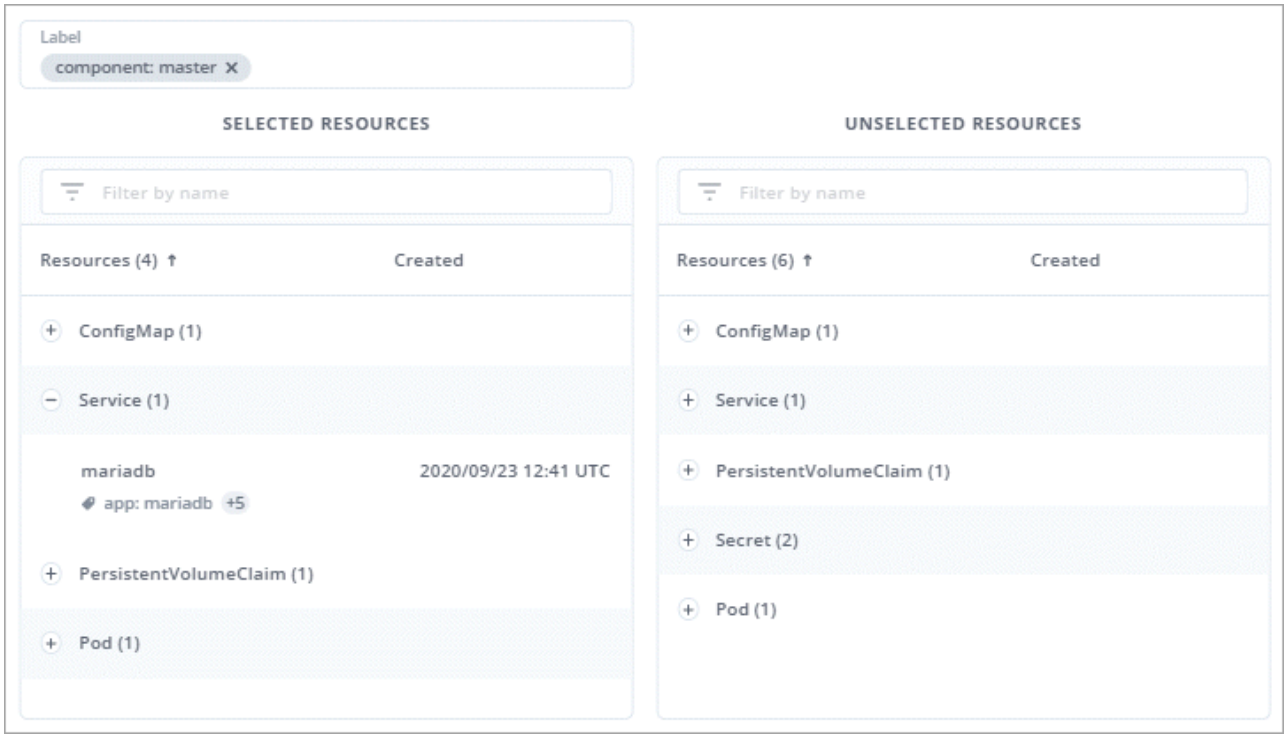


- Select one of the labels.



After you choose a label, it displays in the **Label** field. Astra Control also updates the **Unselected Resources** section to show the resources that don't match the selected label.

f. **Unselected Resources**: Verify the app resources that you don't want to protect.



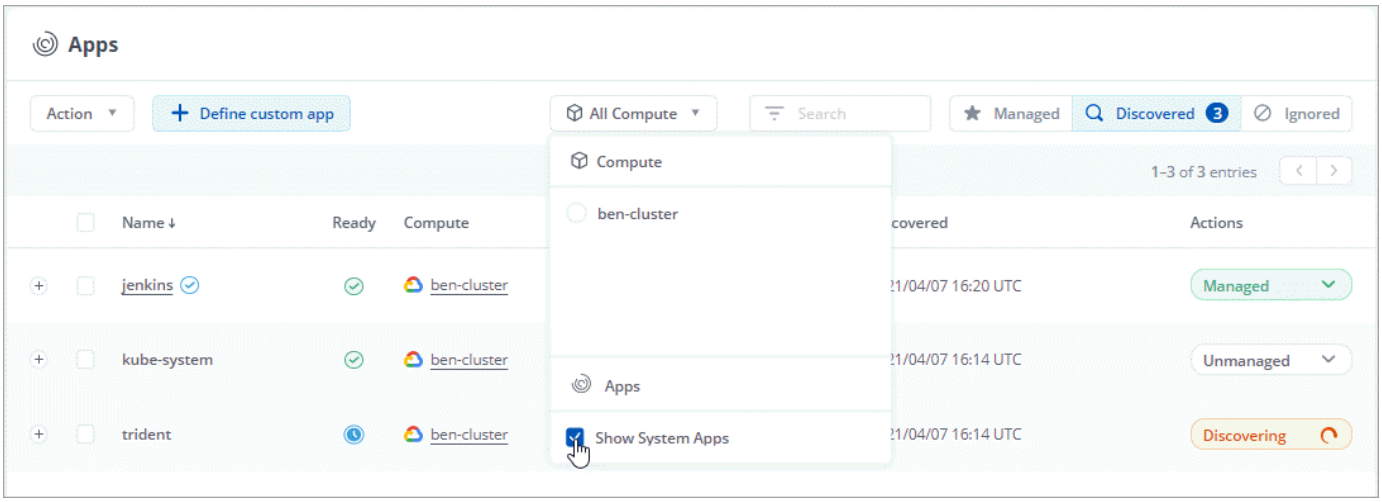
3. Click **Define Custom App**.

Result

Astra Control enables management of the app. You can now find it in the **Managed** tab.

What about system apps?

Astra Control also discovers the system apps running on a Kubernetes cluster. You can view them by filtering the Apps list.



We don't show you these system apps by default because it's rare that you'd need to back them up.

Protect apps with snapshots and backups

Protect your apps by taking snapshots and backups using an automated protection policy or on an ad-hoc basis.

Snapshots and backups

A *snapshot* is a point-in-time copy of an app that's stored on the same provisioned volume as the app. They are usually fast. Local snapshots are used to restore the application to an earlier point in time.

A *backup* is stored on object storage in the cloud. A backup can be slower to take compared to the local snapshots. But they can be accessed across regions in the cloud to enable app migrations. You can also choose a longer retention period for backups.

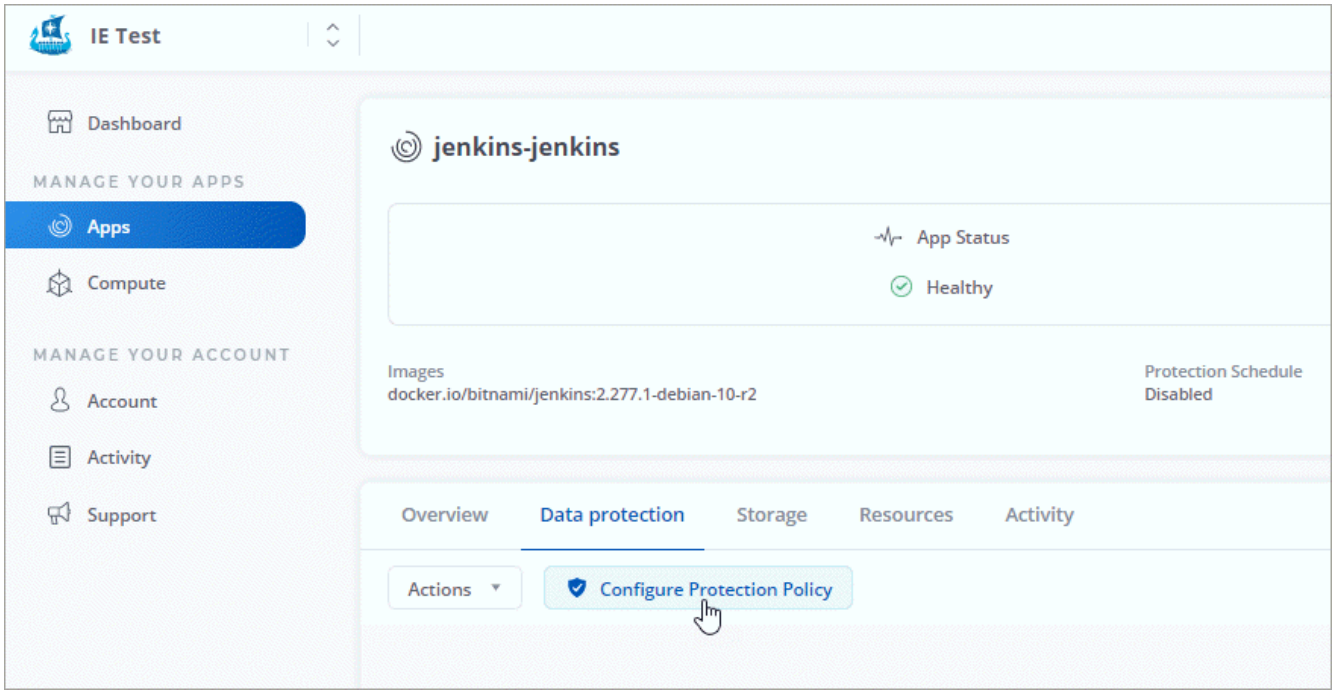
> *You can't be fully protected until you have a recent backup*. This is important because backups are stored in an object store away from the persistent volumes. If a failure or accident wipes out the cluster and it's persistent storage, then you need a backup to recover. A snapshot wouldn't enable you to recover.

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.

Steps

1. Click **Apps** and then click the name of a managed app.
2. Click **Data Protection**.
3. Click **Configure Protection Policy**.

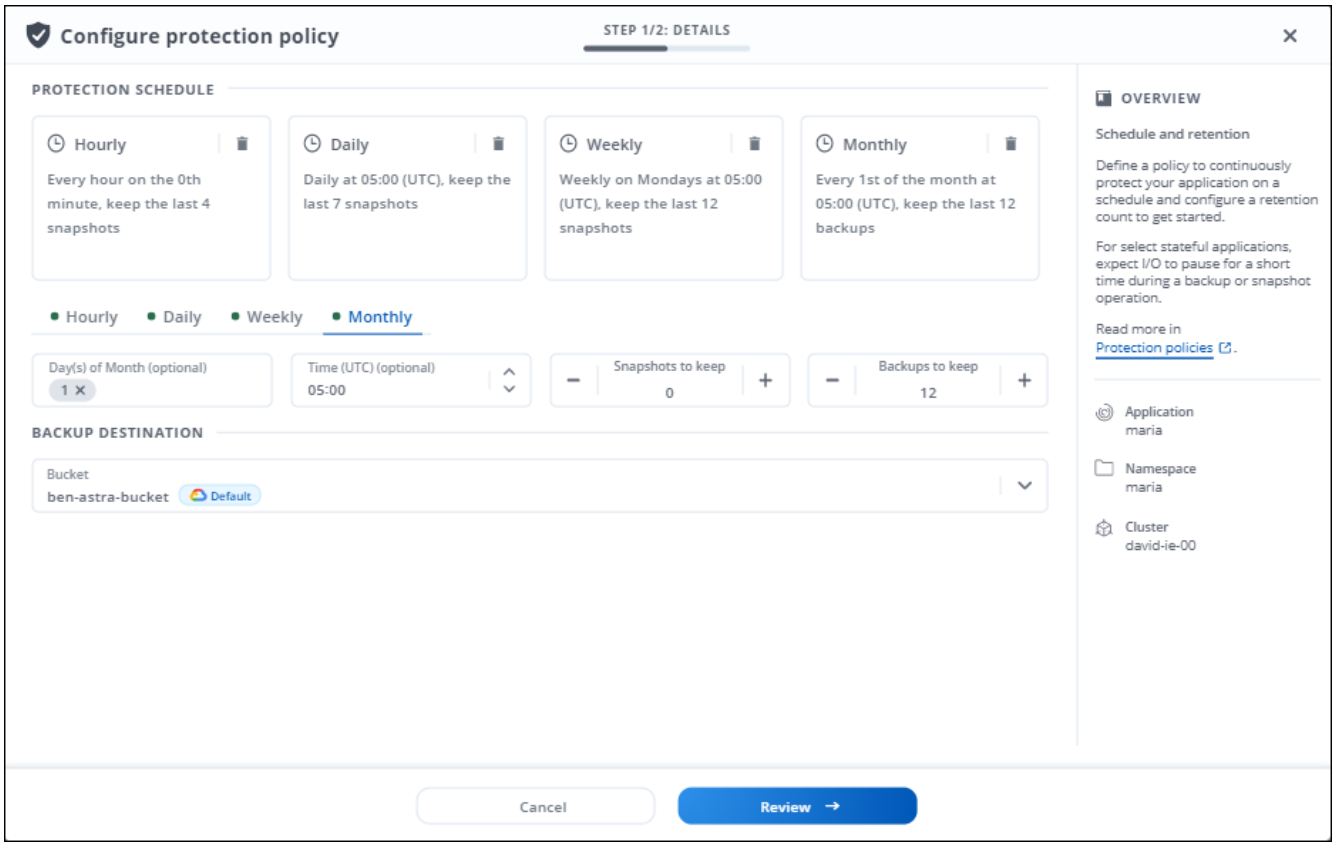


4. Define a protection schedule by choosing the number of snapshots and backups to keep for the hourly, daily, weekly, and monthly schedules.

You can define the hourly, daily, weekly, and monthly schedules concurrently. A schedule won't turn active until you set a retention level for snapshots and backups.

When you set a retention level for backups, you can choose the bucket where you'd like to store the backups.

The following example sets four protection schedules: hourly, daily, weekly, and monthly for snapshots and backups.



5. Click **Review**.
6. Click **Configure**.

Here's a video that shows each of these steps.

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

Result

Astra Control implements the data protection policy by creating and retaining snapshots and backups using the schedule and retention policy that you defined.

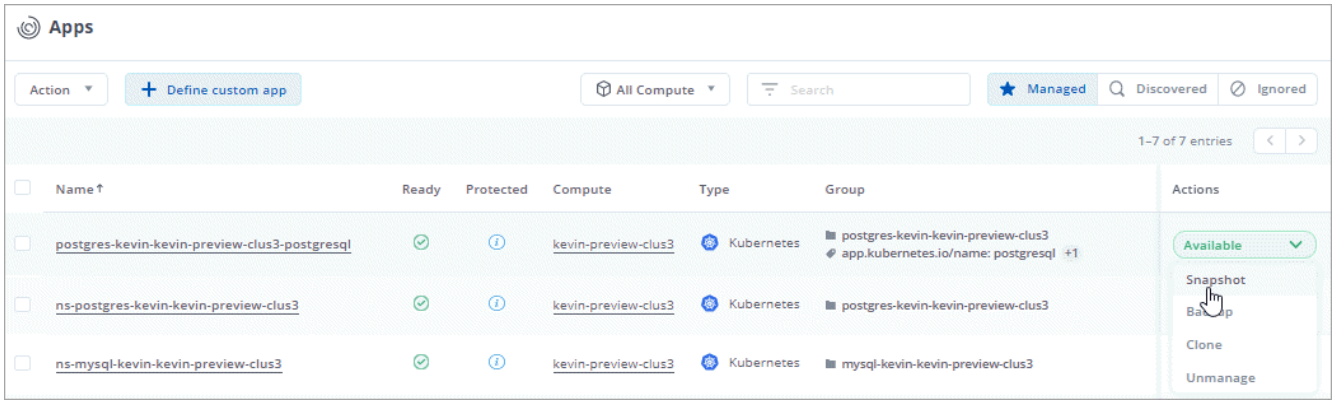
Create a snapshot

You can create an on-demand snapshot at any time.

Steps

1. Click **Apps**.
2. Click the drop-down list in the **Actions** column for the desired app.

3. Click **Snapshot**.



4. Customize the name of the snapshot and then click **Review Information**.
5. Review the snapshot summary and click **Snapshot App**.

Result

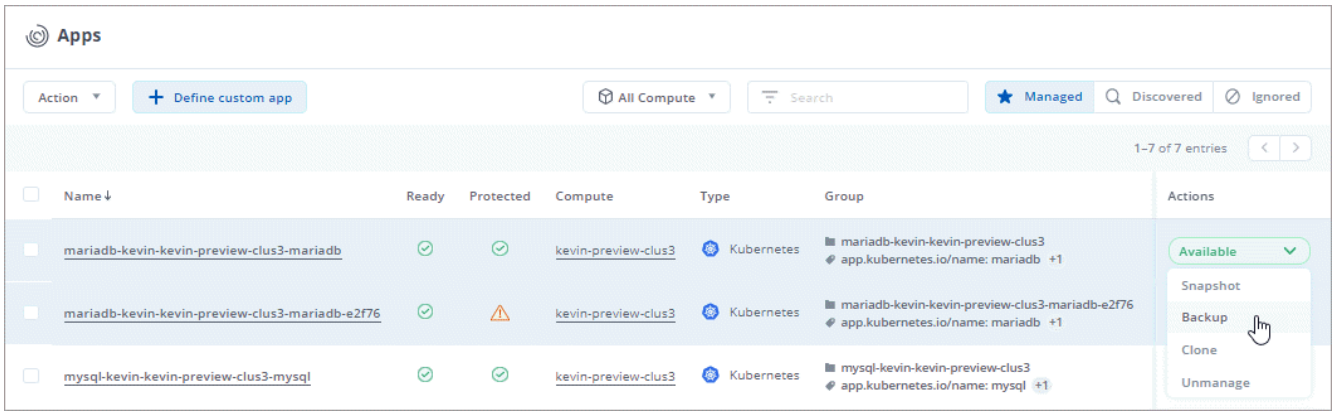
Astra Control creates a snapshot of the apps.

Create a backup

You can also back up an app at any time.

Steps

1. Click **Apps**.
2. Click the drop-down list in the **Actions** column for the desired app.
3. Click **Backup**.



4. Customize the name of the backup, choose whether to back up the app from an existing snapshot, and then click **Review Information**.
5. Review the backup summary and click **Backup App**.

Result

Astra Control creates a backup of the app.

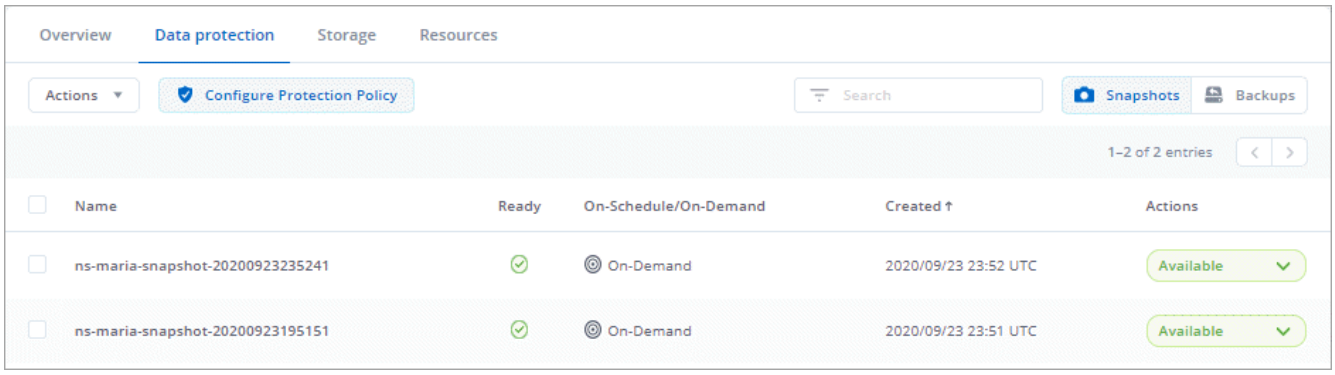
View snapshots and backups

You can view the snapshots and backups of an app from the Data Protection tab.

Steps

1. Click **Apps** and then click the name of a managed app.
2. Click **Data Protection**.

   The snapshots display by default.



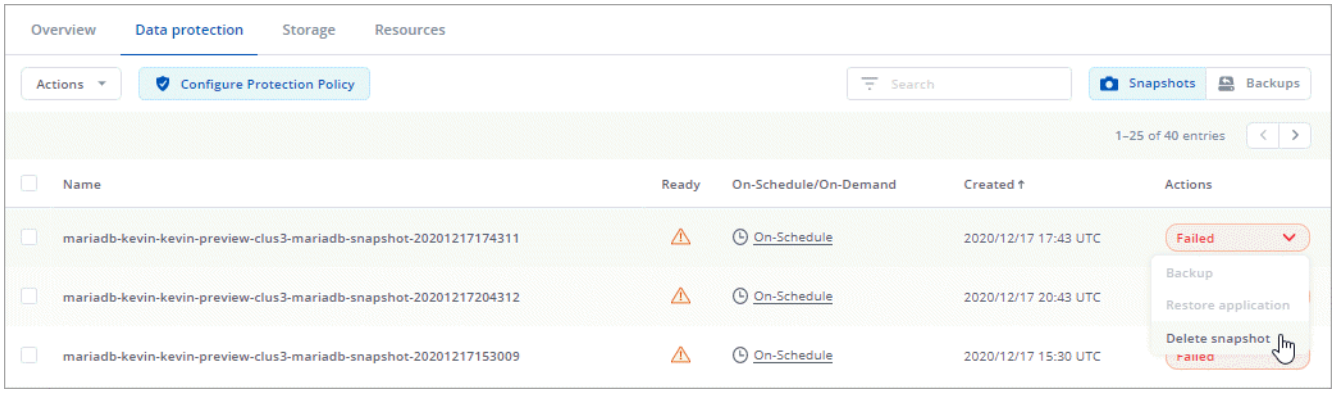
3. Click **Backups** to see the list of backups.

Delete snapshots

Delete the scheduled or on-demand snapshots that you no longer need.

Steps

1. Click **Apps** and then click the name of a managed app.
2. Click **Data Protection**.
3. Click the drop-down list in the **Actions** column for the desired snapshot.
4. Click **Delete snapshot**.



5. Type the name of the snapshot to confirm deletion and then click **Yes, Delete snapshot**.

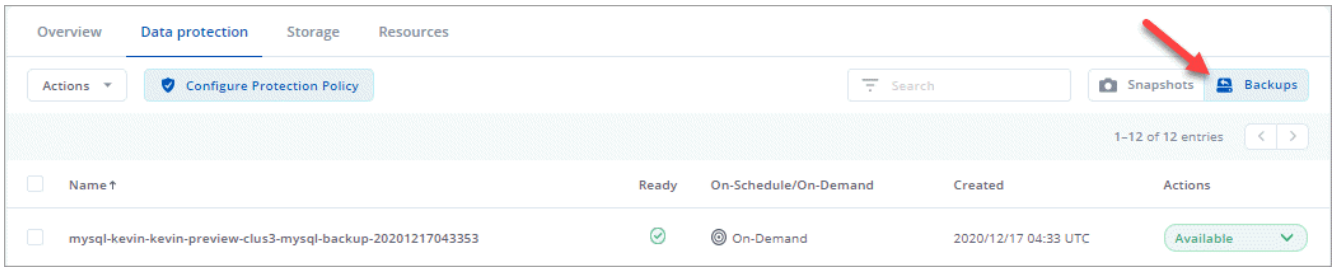
Result

Astra Control deletes the snapshot.

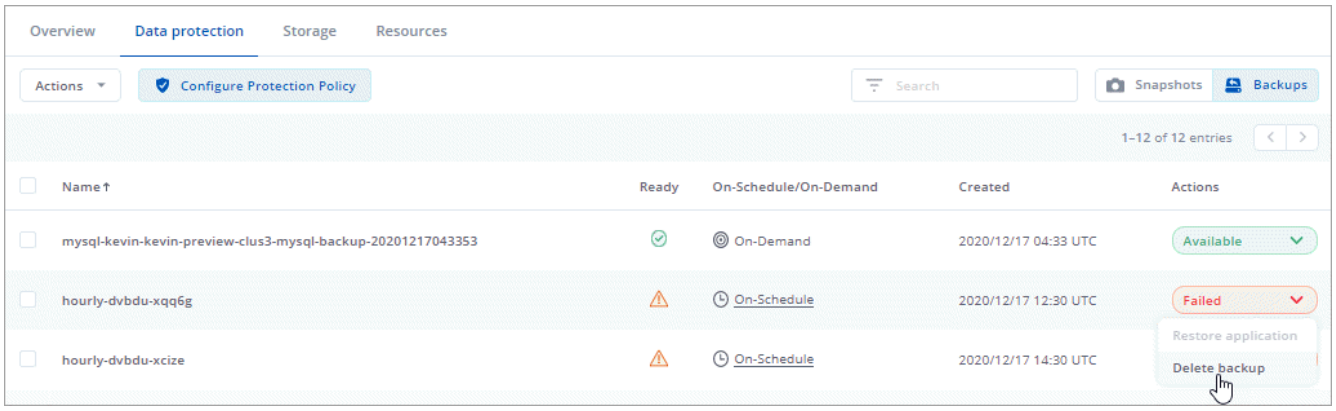
Delete backups

Delete the scheduled or on-demand backups that you no longer need.

1. Click **Apps** and then click the name of a managed app.
2. Click **Data Protection**.
3. Click **Backups**.



4. Click the drop-down list in the **Actions** column for the desired backup.
5. Click **Delete backup**.



6. Type the name of the backup to confirm deletion and then click **Yes, Delete backup**.

Result

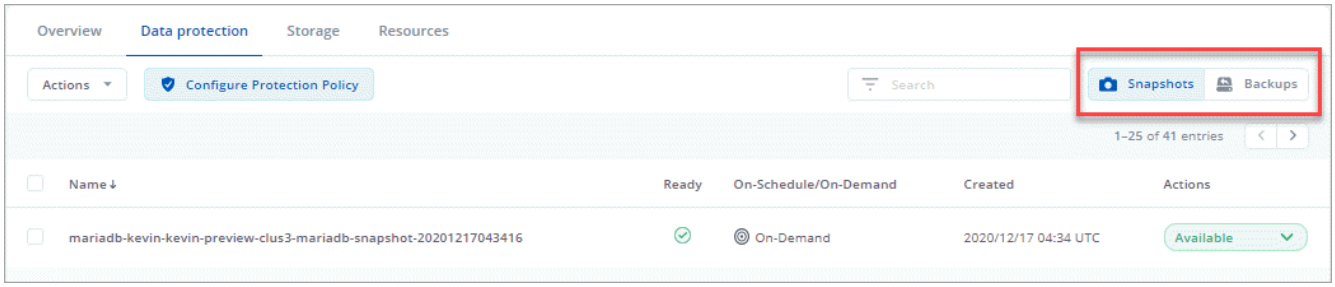
Astra Control deletes the backup.

Restore apps

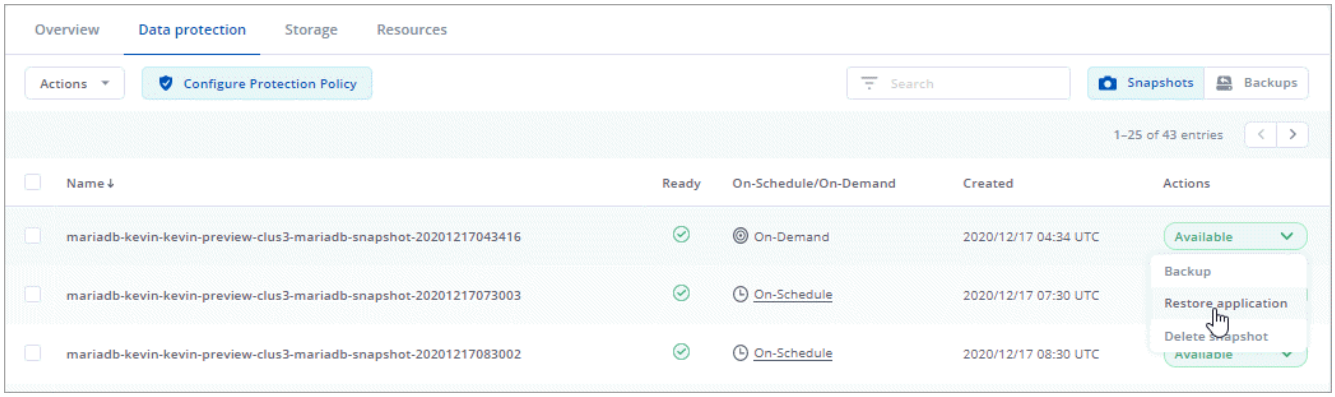
Astra Control can restore your application configuration and persistent storage from a snapshot or backup. Persistent storage backups are transferred from your object store, so restoring from an existing backup will complete the fastest.

Steps

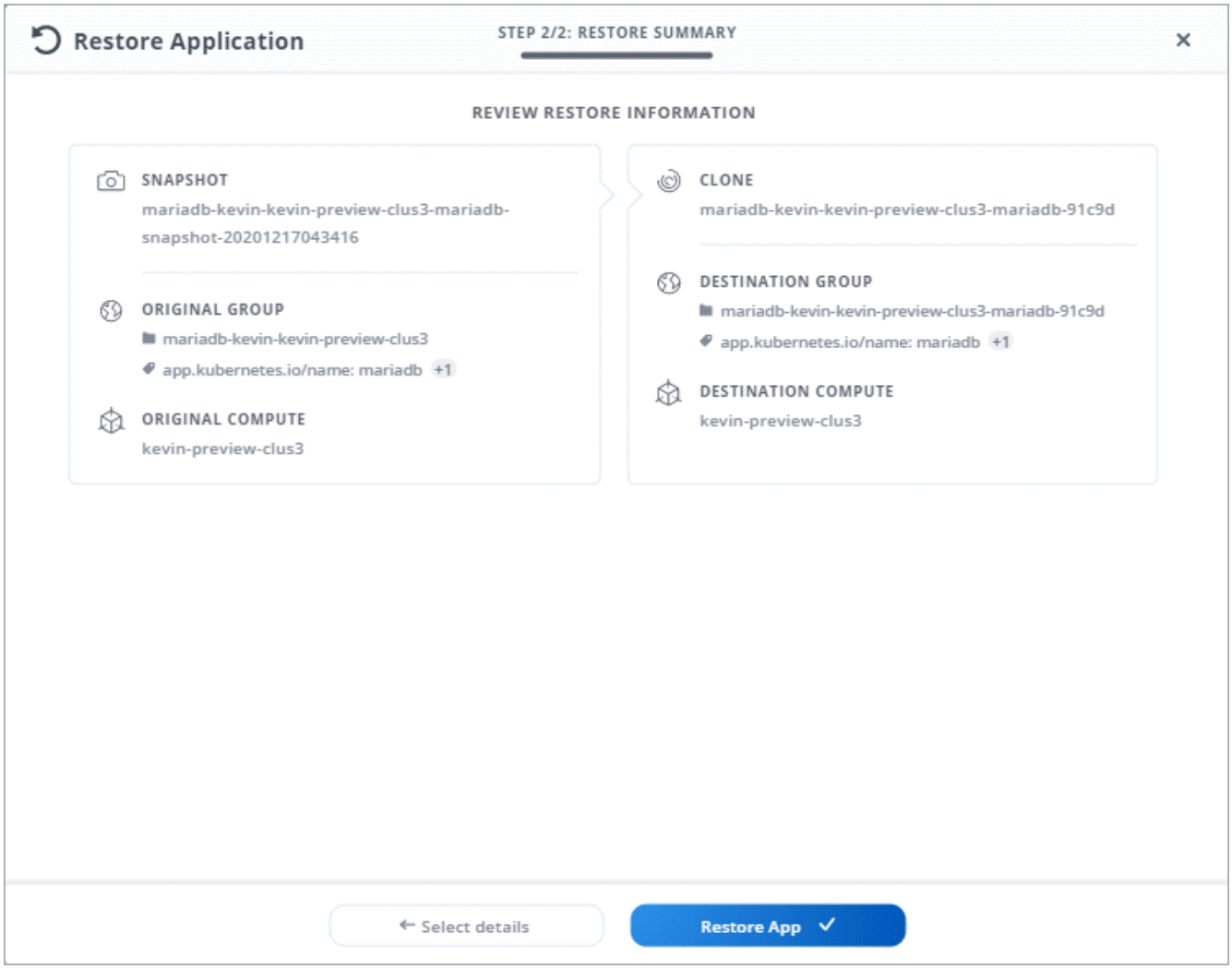
1. Click **Apps** and then click the name of a managed app.
2. Click **Data protection**.
3. If you want to restore from a snapshot, keep **Snapshots** selected. Otherwise, click **Backups** to restore from a backup.



4. Click the drop-down list in the **Actions** column for the snapshot or backup from which you want to restore.
5. Click **Restore application**.



6. **Restore details**: Specify details for the clone:
   - Enter a name and namespace for the app.
   - Choose the destination compute for the app.
   - Click **Review information**.
7. **Restore Summary**: Review details about the restore action and click **Restore App**.



Result

Astra Control restores the app based on the information that you provided.

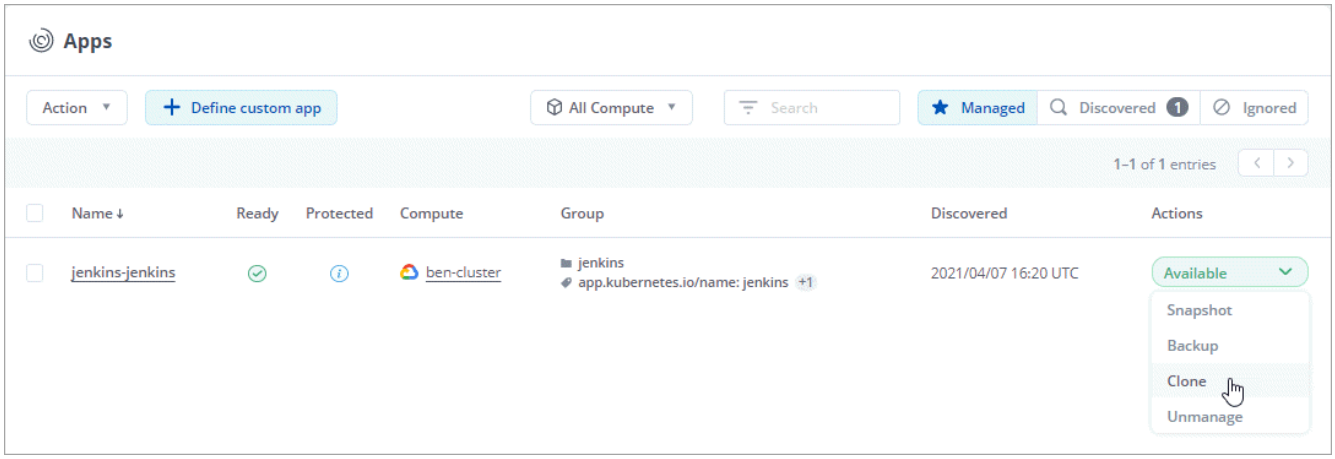
Clone and migrate apps

Clone an existing app to create a duplicate app on the same Kubernetes cluster or on another cluster. Cloning can help if you need to move applications and storage from one Kubernetes cluster to another. For example, you might want to move workloads through a CI/CD pipeline and across Kubernetes namespaces.

When Astra Control clones an app, it creates a clone of your application configuration and persistent storage.

Steps

1. Click **Apps**.
2. Click the drop-down list in the **Action** column for the desired app.
3. Click **Clone**.



4. **Clone details**: Specify details for the clone:
   - Keep the default name and namespace, or edit them.
   - Choose a destination compute for the clone.
   - Choose whether you want to create the clone from an existing snapshot or backup. If you don't select this option, Astra Control creates the clone from the app's current state.
5. **Clone Summary**: Review the details about the clone and click **Clone App**.

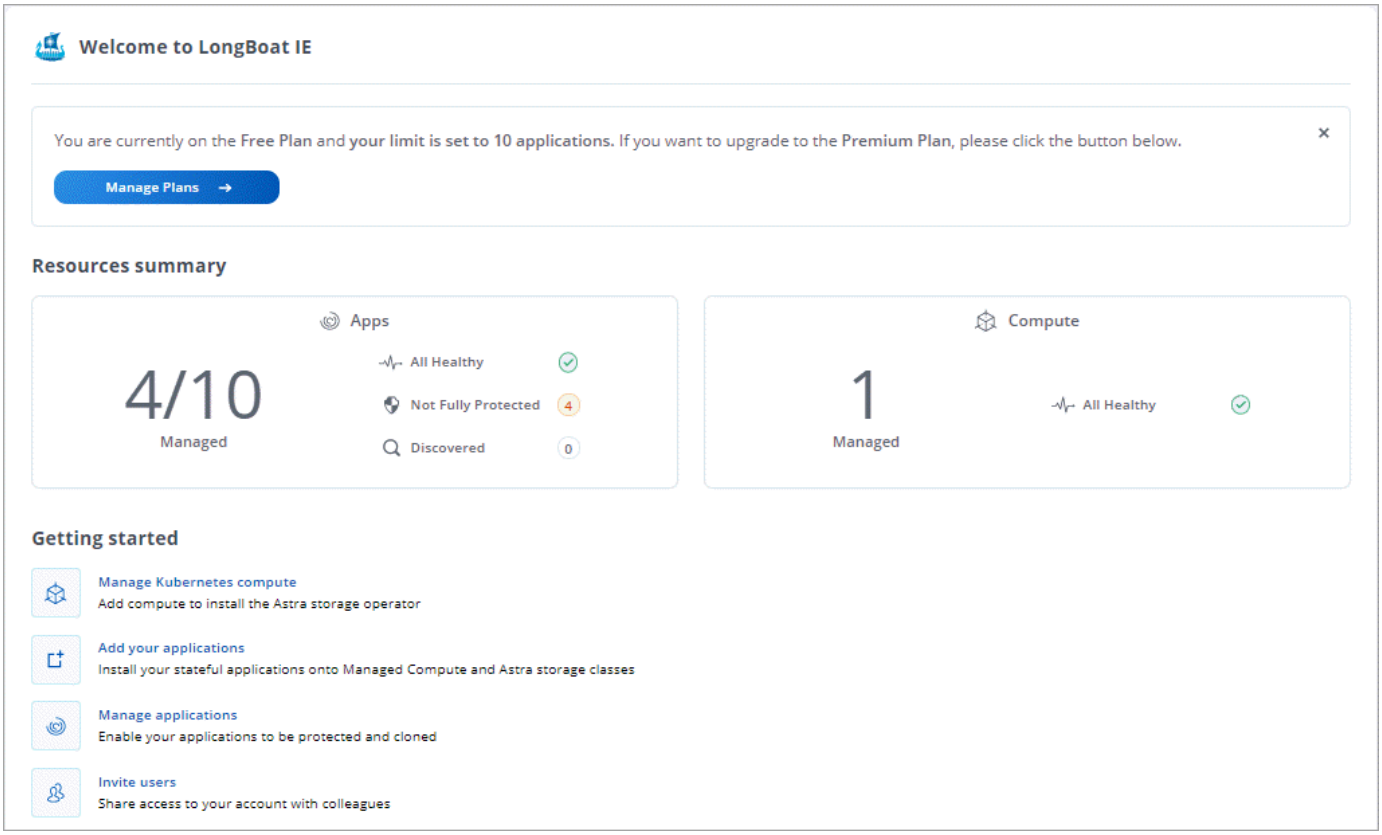
Result

Astra Control clones that app based on the information that you provided.

View app and compute health

View a summary of app and compute health

Click the **Dashboard** to see a high-level view of your apps, compute, and their health.

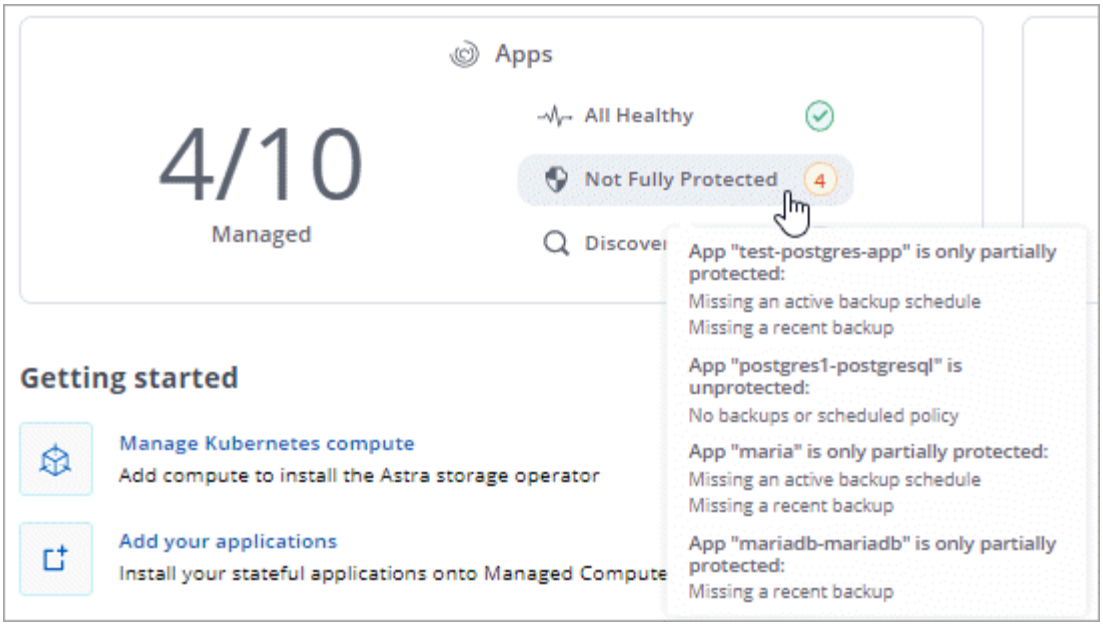


The Apps tile helps you identify the following:

- How many apps you're currently managing.
- Whether those managed apps are healthy.
- Whether the apps are fully protected (they're protected if recent backups are available).
- The number of apps that were discovered, but are not yet managed.

  Ideally, this number would be zero because you would either manage or ignore apps after they're discovered. And then you would monitor the number of discovered apps on the Dashboard to identify when developers add new apps to a cluster.

Note that these aren't just numbers or statuses—you can drill down from each of these. For example, if apps aren't fully protected, you can hover over the icon to identify which apps aren't fully protected, which includes a reason why.



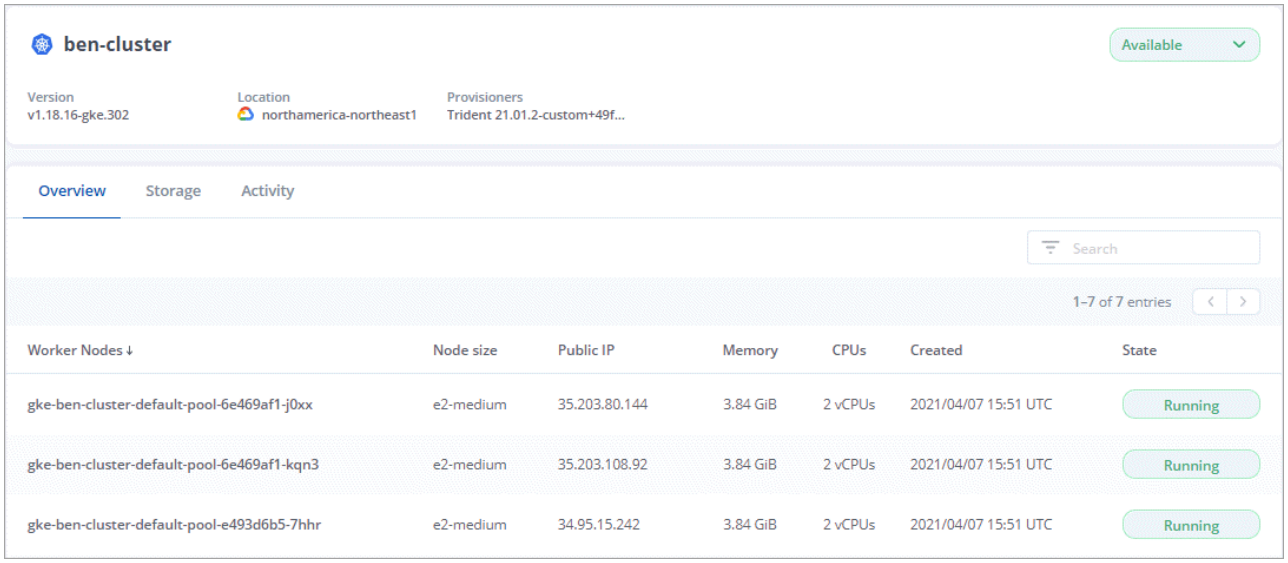
The Compute tile provides similar details about the health of the compute and you can drill down to get more details just like you can with an app.

View the health and details of compute

After you add Kubernetes compute to Astra Control, you can view details about the compute, such as its location, the worker nodes, persistent volumes, and storage classes.

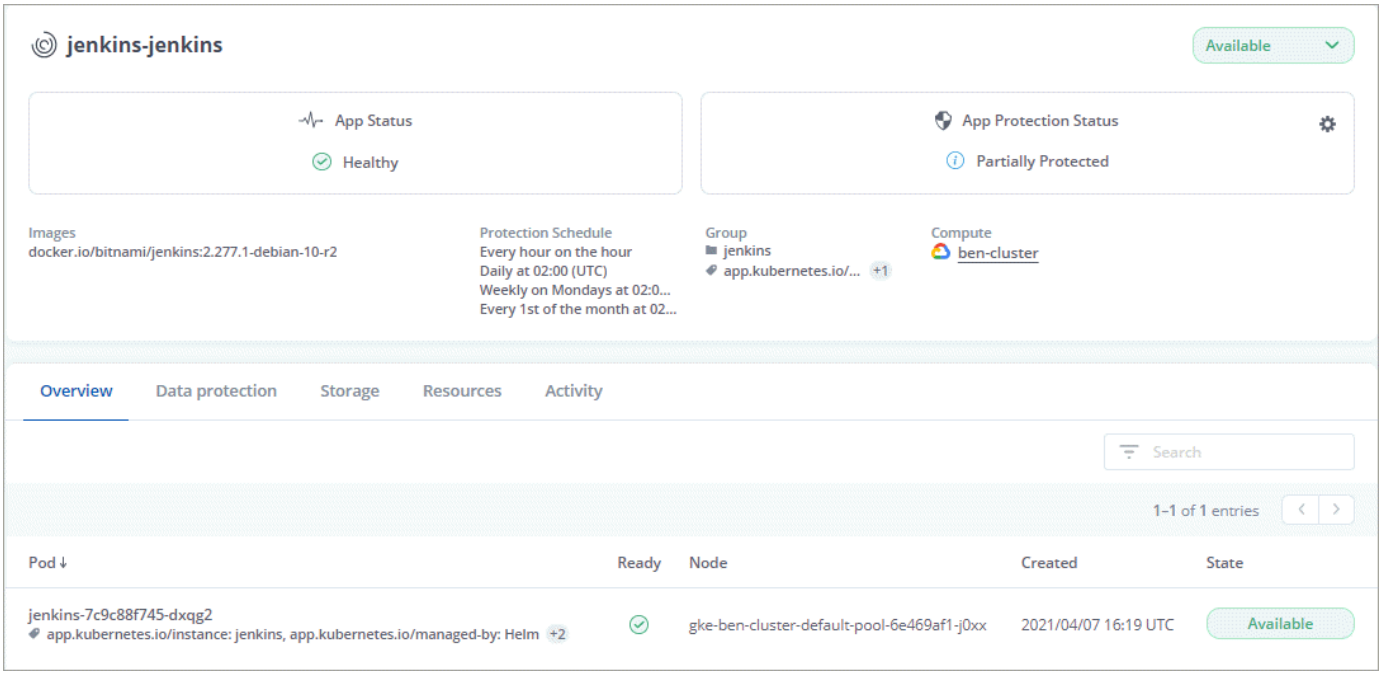
Steps

1. Click **Compute**.
2. Click the compute name.
3. View the information in the **Overview** and **Storage** tabs to find the information that you're looking for.
    - **Overview**: Details about the worker nodes, including their state.
    - **Storage**: The persistent volumes associated with the compute, including the storage class and state.
    - **Activity**: The Astra activities related to the compute.



View the health and details of an app

After you start managing an app, Astra Control provides details about the app that enables you to identify its status (whether it's healthy), its protection status (whether it's fully protected in case of failure), the pods, persistent storage, and more.



Steps

1. Click **Apps** and then click the name of an app.
2. Click around to find the information that you're looking for:

   App Status

   Provides a status that reflects the app's state in Kubernetes. For example, are pods and persistent volumes online? If an app is unhealthy, you'll need to go and troubleshoot the issue on the cluster by looking at Kubernetes logs. Astra Control doesn't provide information to help you fix a broken app.

App Protection Status

Provides a status of how well the app is protected:

- **Fully protected**: The app has an active backup schedule and a successful backup that's less than a week old
- **Partially protected**: The app has an active backup schedule, an active snapshot schedule, or a successful backup or snapshot
- **Unprotected**: Apps that are neither fully protected or partially protected.

  You can't be fully protected until you have a recent backup. This is important because backups are stored in an object store away from the persistent volumes. If a failure or accident wipes out the cluster and it's persistent storage, then you need a backup to recover. A snapshot wouldn't enable you to recover.

Overview

Information about the state of the pods that are associated with the app.

Data protection

Enables you to configure a data protection policy and to view the existing snapshots and backups.

Storage

Shows you the app-level persistent volumes. The state of a persistent volume is from the perspective of the Kubernetes cluster.

Resources

Enables you to verify which resources are being backed up and managed.

Activity

The Astra Control activities related to the app.

Manage buckets

Manage the buckets that Astra uses for backups and clones by adding additional buckets and by changing the default bucket for the Kubernetes clusters in your cloud provider.

Only Admins can add and modify buckets.

How Astra Control uses buckets

When you start managing your first Kubernetes cluster, Astra Control Service creates the default bucket for your cloud provider in the same geography as the managed cluster.

Astra Control Service uses this default bucket for the backups and clones that you create. You can then use the backups to restore and clone apps between clusters.

If you add additional buckets to Astra Control Service, you can select from those buckets when you create a protection policy. You can also change the default bucket that Astra Control Service uses for ad-hoc backups and clones.

Astra Control Service checks whether a destination bucket is accessible prior to starting a backup or a clone.

View existing buckets

View the list of buckets that are available to Astra Control Service to determine their status and to identify the default bucket for your cloud provider.

A bucket can have any of the following states:

Pending

After you add a bucket, it starts in the pending state while Astra Control looks at it for the first time.

Available

The bucket is available for use by Astra Control.

Removed

The bucket isn't operational at the moment. Hover your mouse over the status icon to identify what the problem is.

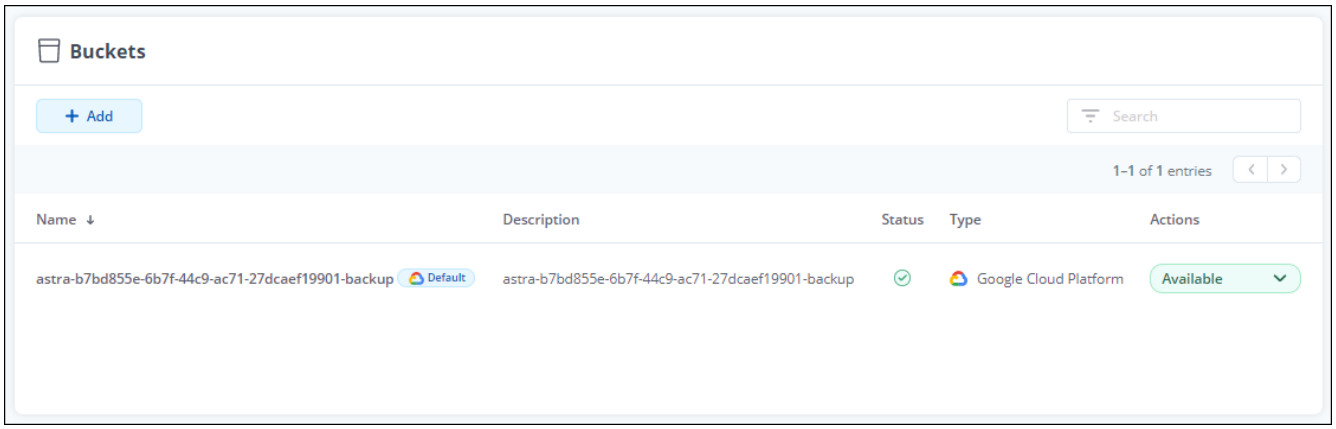
If a bucket is in the Removed state, you can still set it as the default bucket and assign it to a protection schedule. But if the bucket isn't in the Available state by the time a data protection operation starts, then that operation will fail.

Step

1. Under **Manage your storage**, click **Buckets**.

   The list of buckets available to Astra Control Service displays.

   As you can see from the following example, there is only one bucket available: the default bucket that Astra created.



Add an additional bucket

After you start managing a cluster in your cloud provider, you can add additional buckets at any time. This enables you to choose between buckets when creating a protection policy and to change the default bucket for ad-hoc backups and clones.

Note that Astra Control Service doesn't enable you to remove a bucket after you've added it.

What you'll need

- The name of an existing bucket in your cloud provider.
- If your bucket is in Azure, it must belong to the resource group named *astra-backup-rg*.

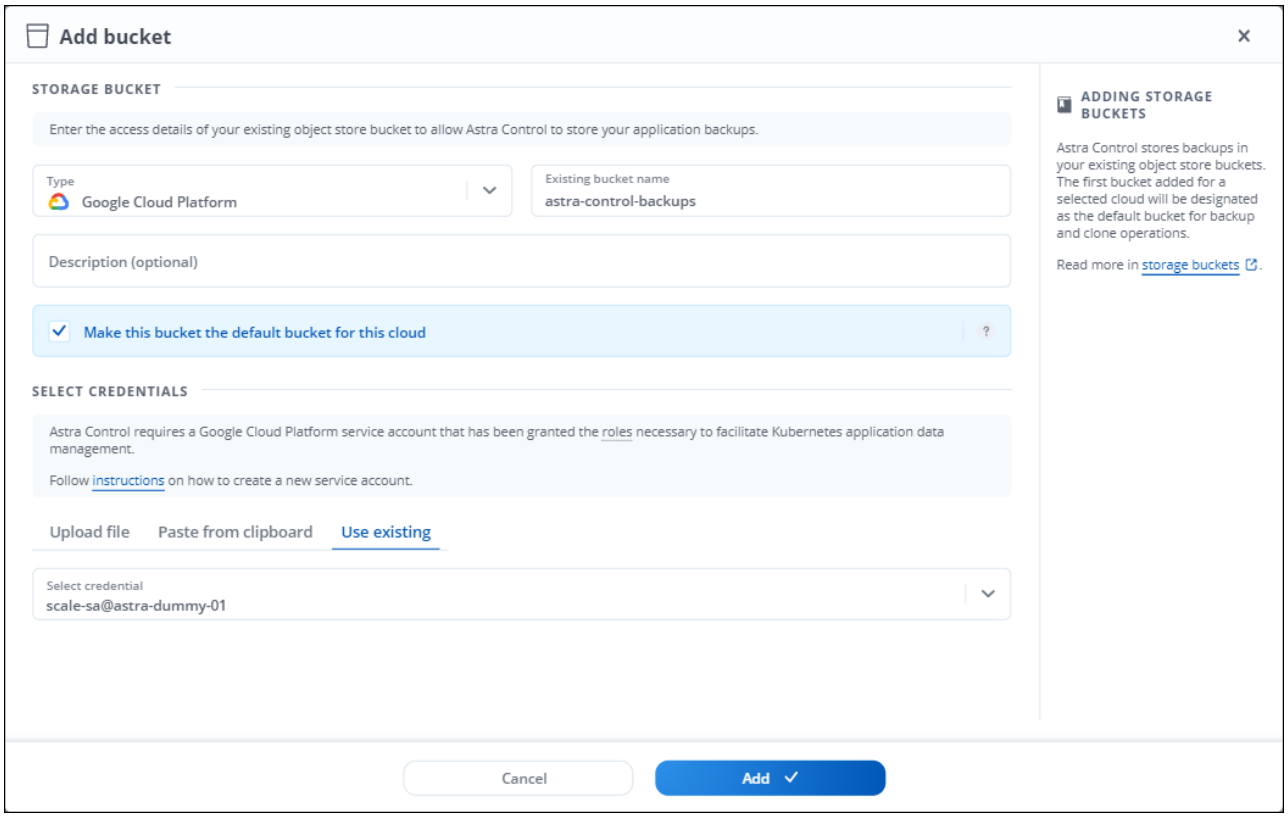
Steps

1. Under **Manage your storage**, click **Buckets**.
2. Click **Add** and follow the prompts to add the bucket.
   - **Type**: Choose your cloud provider.

     Your cloud provider is available only after Astra Control Service has started managing a cluster that's running in that cloud provider.

   - **Existing bucket name**: Enter the name of the bucket.
   - **Description**: Optionally enter a description of the bucket.
   - **Make this bucket the default bucket for this cloud**: Choose whether you would like to use this bucket as the default bucket for ad-hoc backups and clones.
   - **Select credentials**: Choose the credentials that provide Astra Control Service with the permissions that it needs to manage the bucket.

     Here's an example that shows adding a new bucket in Google Cloud Platform.



3. Click **Add** to add the bucket.

Result

Astra Control Service adds the additional bucket. You can now choose the bucket when creating a protection policy.

Change the default bucket

Change the default bucket that Astra Control Service should use for backups and clones. Each cloud provider has its own default bucket.

Astra Control Service uses the default bucket for a cloud provider for ad-hoc backups and for ad-hoc clones when you don't choose to clone from an existing backup.

Steps

1. Under **Manage your storage**, click **Buckets**.
2. Click the drop-down list in the **Actions** column for the bucket that you want to edit.
3. Select **Make this bucket the default bucket for this cloud**.
4. Click **Update**.

Manage your account

Set up billing

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.

Billing overview

There are two types of costs associated with using Astra Control Service: charges from NetApp for the Astra Control Service and charges from your cloud provider for persistent volumes and object storage.

Astra Control Service billing

Astra Control Service offers three plans:

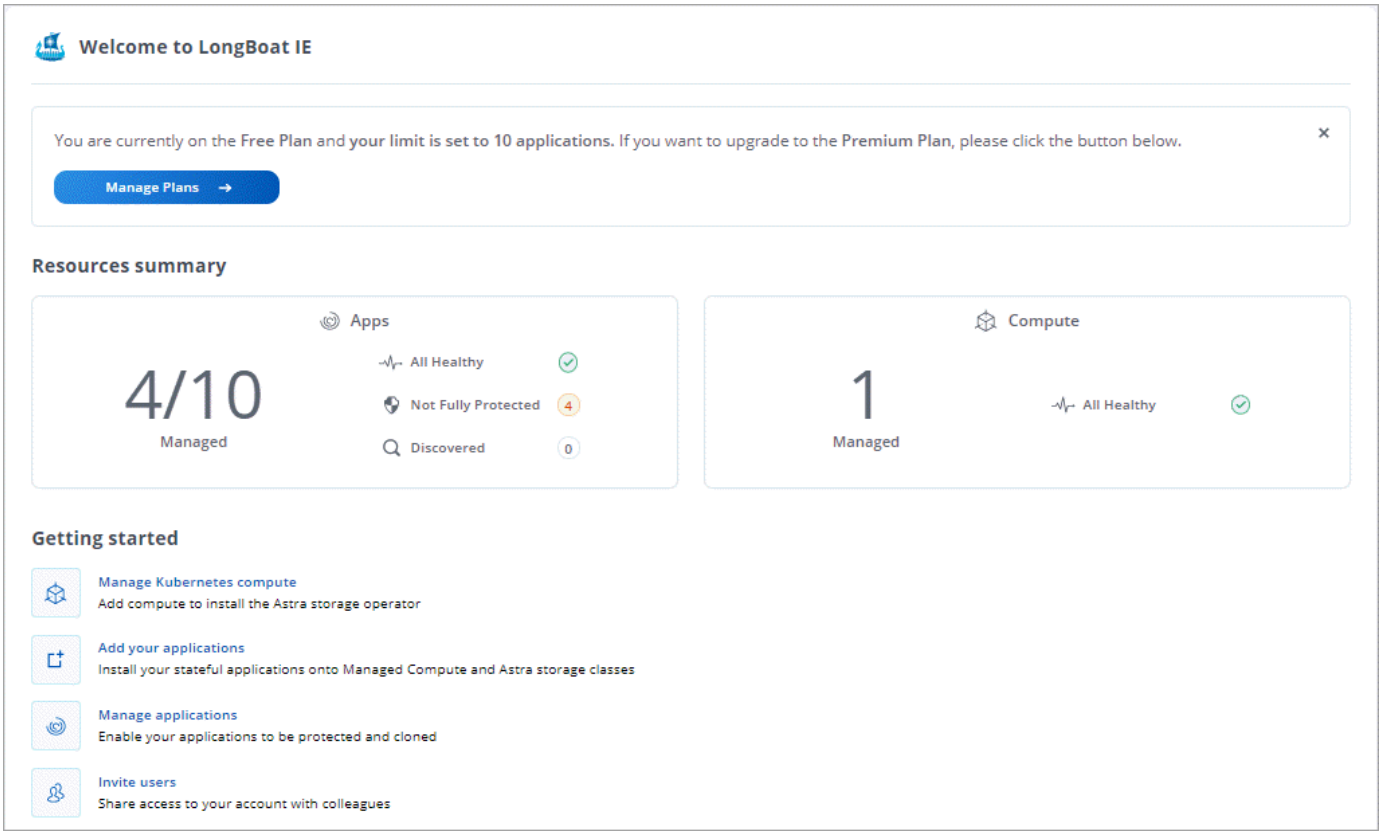
Free Plan
: Manage up to 10 apps for free.

Premium PayGo
: Manage an unlimited amount of apps at a rate of $.005 per minute, per app.

Premium Subscription
: Pre-pay at a discounted rate with an annual subscription that enables you to manage up to 10 apps per *application pack*. Contact NetApp Sales to purchase as many packs as needed for your organization—for example, purchase 3 packs to manage 30 apps from Astra Control Service. If you manage more apps than allowed by your annual subscription, then you'll be charged at the overage rate of $0.005 per minute, per application (the same as Premium PayGo).

  If you don't have an Astra Control account yet, purchasing the Premium Subscription automatically creates an Astra Control account for you. If you have an existing Free Plan, then you're automatically converted to the Premium Subscription.

When you create an Astra Control account, you're automatically signed up for the Free Plan. Astra Control's Dashboard shows you how many apps you're currently managing out of the 10 free apps that you're allowed:



If you try to manage an 11th app, Astra Control notifies you that you've reached the limit of the Free Plan. It then prompts you to upgrade from the Free Plan to a Premium Plan.

You can upgrade to a Premium Plan at any time. After you upgrade, Astra Control starts charging you for *all* managed apps in the account. The first 10 apps don't stay in the Free Plan.

Google Cloud billing

When you manage GKE clusters with Astra Control Service, persistent volumes are backed by NetApp Cloud Volumes Service and backups of your apps are stored in a Google Cloud Storage bucket.

- View pricing details for Cloud Volumes Service.

  Note that Astra Control Service supports all service types and service levels. The service type that you use depends on your Google Cloud region.

- View pricing details for Google Cloud storage buckets.

Microsoft Azure billing

When you manage AKS clusters with Astra Control Service, persistent volumes are backed by Azure NetApp Files and backups of your apps are stored in an Azure Blob container.

- View pricing details for Azure NetApp Files.
- View pricing details for Microsoft Azure Blob storage.

Important notes

- Your billing plan is per Astra Control account.

If you have multiple accounts, then each has its own billing plan.

- Your Astra Control bill includes charges for managing your Kubernetes apps. You're charged separately by your cloud provider for the backend storage for persistent volumes.

  Learn more about Astra Control pricing.

- Each billing period ends on the last day of the month.
- You can't downgrade from a Premium Plan to the Free Plan.

Upgrade from the Free Plan to the Premium PayGo Plan

Upgrade your billing plan at any time to start managing more than 10 apps from Astra Control by paying as you go. All you need is a valid credit card.

Steps

1. Click **Account** and then click **Billing**.
2. Under **Plans**, go to **Premium PayGo** and click **Upgrade Now**.
3. Provide payment details for a valid credit card and click **Upgrade to Premium Plan**.

> Astra Control will email you if the credit card is nearing expiration.

Result

You can now manage more than 10 apps. Astra Control starts charging you for *all* apps that you're currently managing.

Upgrade from the Free Plan to the Premium Subscription

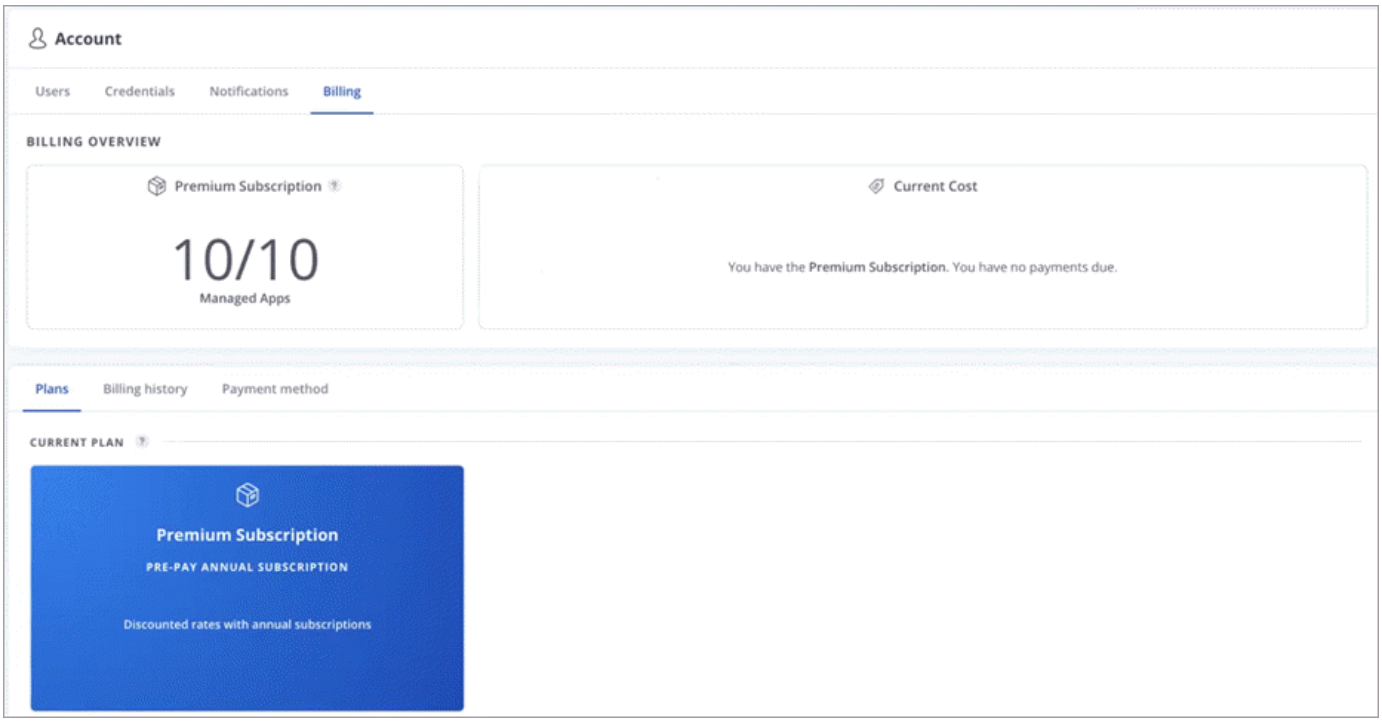
Contact NetApp Sales to pre-pay at a discounted rate with an annual subscription.

Steps

1. Click **Account** and then click **Billing**.
2. Under **Plans**, go to **Premium Subscription** and click **Contact Sales**.
3. Provide details to the sales team to start the process.

Result

A NetApp Sales representative will contact you to process your purchase order. After the order is complete, Astra Control will reflect your current plan on the Billing tab.



View your current costs and billing history

Astra Control shows you your current monthly costs, as well as a detailed billing history by app.

Steps

1. Click **Account** and then click **Billing**.

   Your current costs appear under the billing overview.

2. To view the billing history by app, click **Billing history**.

   Astra Control shows you the usage minutes and cost for each app. A usage minute is how many minutes Astra Control managed your app during a billing period.

3. Click the drop-down list to select a previous month.

Change the credit card for Premium PayGo

If needed, you can change the credit card that Astra Control has on file for billing.

Steps

1. Click **Account > Billing > Payment method**.
2. Click the configure icon.
3. Modify the credit card.

Invite and remove users

Invite users to join your Astra Control account and remove users that should no longer have access to the account.

Invite users

Account Owners and Admins can invite other users to join the Astra Control account.

Steps

1. Make sure that the user has a Cloud Central login.
2. Click **Account**.
3. In the **Users** tab, click **+ Invite users**.
4. Enter the user's name, email address, and their role.

   Note the following:

   - The email address must match the email address that the user used to sign up to Cloud Central.
   - Each role provides the following permissions:
     - An **Owner** has Admin permissions and can delete accounts.
     - An **Admin** has Member permissions and can invite other users.
     - A **Member** can fully manage apps and compute.
     - A **Viewer** can view resources.

5. Click **Send invite(s)**.

Result

The user will receive an email that invites them to join your account.

Change a user's role

An Account Owner can change the role of all users, while an Account Admin can change the role of users who have the Admin, Member, or Viewer role.

Steps

1. Click **Account**.
2. In the **Users** tab, select the drop-down list in the **Role** column for the user.
3. Select a new role and then click **Change Role** when prompted.

Result

Astra Control updates the user's permissions based on the new role that you selected.

Remove users

An Account Owner can remove other users from the account at any time.

Steps

1. Click **Account**.
2. In the **Users** tab, select the users that you want to remove.
3. Click **Actions** and select **Remove user/s**.
4. When you're prompted, confirm deletion by typing the user's name and then click **Yes, Remove User**.

Result

Astra Control removes the user from the account.

Add and remove credentials

Add and remove cloud provider credentials from your account at any time. Astra Control uses these credentials to discover Kubernetes compute, the apps on the compute, and to provision resources on your behalf.

Note that all users in Astra Control share the same sets of credentials.

Add credentials

The most common way to add credentials to Astra Control is when you manage compute, but you can also add credentials from the Account page. The credentials will then be available to choose when you manage additional Kubernetes compute.

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. Click **Account > Credentials**.
2. Click **Add Credentials**.
3. Select either **Microsoft Azure** or **Google Cloud Platform**.
4. Enter a name for the credentials that distinguishes them from other credentials in Astra Control.
5. Provide the required credentials.
   a. **Microsoft Azure**: Provide Astra Control with 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 Control. Otherwise, you need to manually enter the ID after providing the JSON.

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

Result

The credentials are now available to select when you add compute to Astra Control.

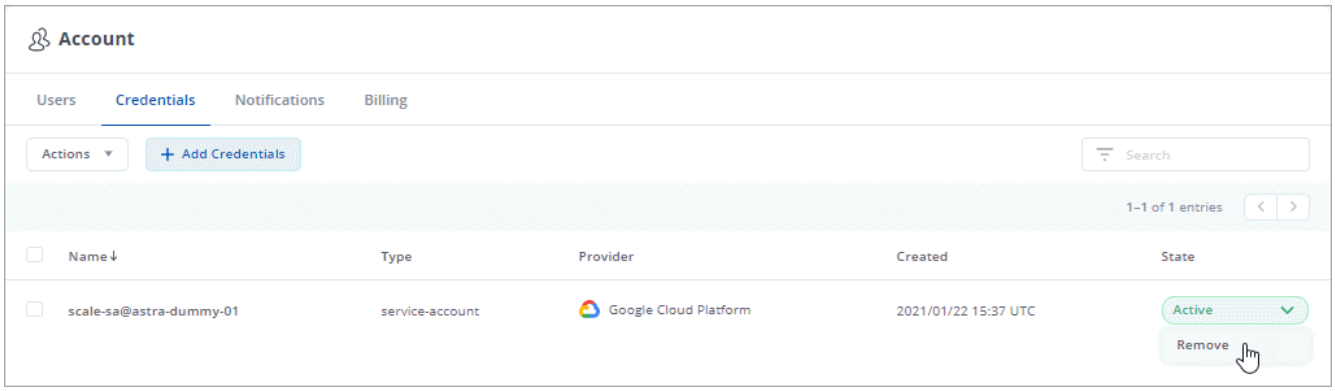
Remove credentials

Remove credentials from an account at any time. You should only remove credentials after unmanaging all compute.

The first set of credentials that you add to Astra Control is always in use because Astra Control uses the credentials to authenticate to the backup bucket. It's best not to remove these credentials.

Steps

1. Click **Account > Credentials**.
2. Click the drop-down list in the **State** column for the credentials that you want to remove.
3. Click **Remove**.



4. Type the name of the credentials to confirm deletion and then click **Yes, Remove Credentials**.

Result

Astra Control removes the credentials from the account.

View account activity

You can view details about the activities in your Astra Control account. For example, when new users were invited, when compute was added, or when a snapshot was taken. You also have the ability to export your account activity to a CSV file.

Steps to view all account activity in Astra Control

1. Click **Activity**.
2. Use the filters to narrow down the list of activities or use the search box to find exactly what you're looking for.
3. Click **Export to CSV** to download your account activity to a CSV file.

Steps to view account activity for a specific app

1. Click **Apps** and then click the name of an app.
2. Click **Activity**.

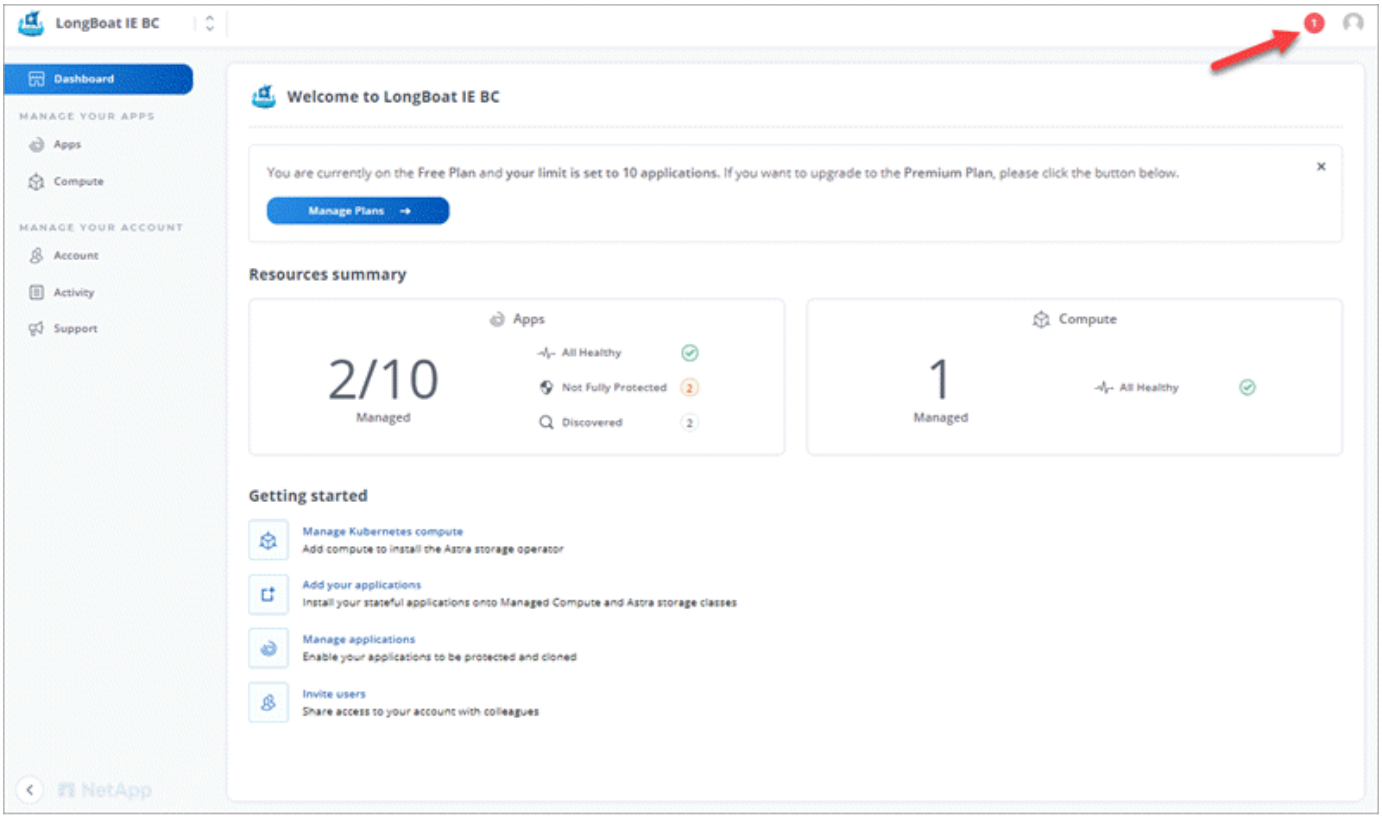
Steps to view account activity for compute

1. Click **Compute** and then click the name of the compute.
2. Click **Activity**.

View and manage notifications

Astra Control notifies you when actions have completed or failed. For example, you'll see a notification if a backup of an app completed successfully.

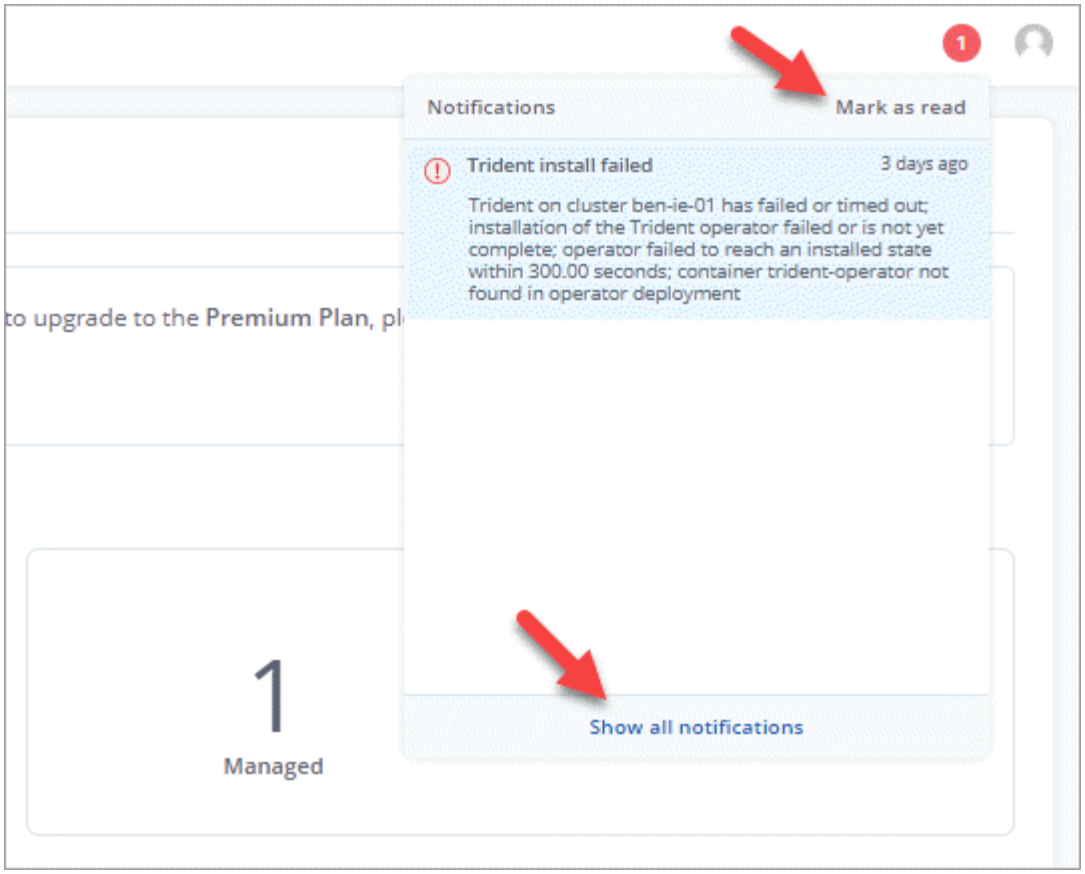
The number of unread notifications is available in the top right of the interface:



You can view these notifications and mark them as read (this can come in handy if you like to clear unread notifications like we do).

Steps

1. Click the number of unread notifications in the top right.



2. Review the notifications and then click **Mark as read** or **Show all notifications**.

   If you clicked **Show all notifications**, the Notifications page loads.

3. On the **Notifications** page, view the notifications, select the ones that you want to mark as read, click **Action** and select **Mark as read**.

Close your account

If you no longer need your Astra Control account, you can close it at any time.

> Buckets that Astra Control automatically created will be automatically deleted when you close your account.

Steps

1. Unmanage all apps and compute.
2. Remove credentials from Astra Control.
3. Click **Account > Billing > Payment method**.
4. Click **Close Account**.
5. Enter your account name and confirm to close the account.

Unmanage apps and compute

Remove any apps or compute that you no longer want to manage from Astra Control.

Stop managing an app

Stop managing apps that you no longer want to back up, snapshot, or clone from Astra Control.

- Any existing backups and snapshots will be deleted.
- Applications and data remain available.

Steps

1. Click **Apps**.
2. Click the checkbox for the apps that you no longer want to manage.
3. Click the **Action** drop-down and select **Unmanage application/s**.
4. Confirm that you want to unmanage the apps and then click **Yes, Unmanage Applications**.

Result

Astra Control stops managing the app.

Stop managing compute

Stop managing the compute that you no longer want to manage from Astra Control. As a best practice, we recommend that you remove compute from Astra Control before you delete it through GCP.

- This action stops your compute from being managed by Astra Control. It doesn't make any changes to the cluster's configuration and it doesn't delete the cluster.
- Trident won't be uninstalled from the cluster. Learn how to uninstall Trident.

Steps

1. Click **Compute**.
2. Click the checkbox for the compute that you no longer want to manage.
3. Click the **Actions** drop-down and select **Unmanage compute/s**.
4. Confirm that you want to unmanage the compute and then click **Yes, Unmanage Compute**.

Result

Astra Control stops managing the compute.

Deleting clusters from your cloud provider

Before you delete a Kubernetes cluster that has persistent volumes (PV) residing on NetApp storage classes, you need to first delete the persistent volume claims (PVC) following one of the methods below. Deleting the PVC and PV before deleting the cluster ensures that you don't receive unexpected bills from your cloud provider.

- **Method #1**: Delete the application workload namespaces from the cluster. Do *not* delete the Trident namespace.
- **Method #2**: Delete the PVCs and the pods, or the deployment where the PVs are mounted.

When you manage a Kubernetes cluster from Astra Control, applications on that cluster use Cloud Volumes Service or Azure NetApp Files as the backend storage for persistent volumes. If you delete the cluster from your cloud provider without first removing the PVs, the backend volumes are *not* deleted along with the cluster.

Using one of the above methods will delete the corresponding PVs from your cluster. Make sure that there are no PVs residing on NetApp storage classes on the cluster before you delete it.

If you didn’t delete the persistent volumes before you deleted the cluster, then you’ll need to manually delete the backend volumes from Cloud Volumes Service for Google Cloud or from Azure NetApp Files.

Automation using the Astra Control REST API

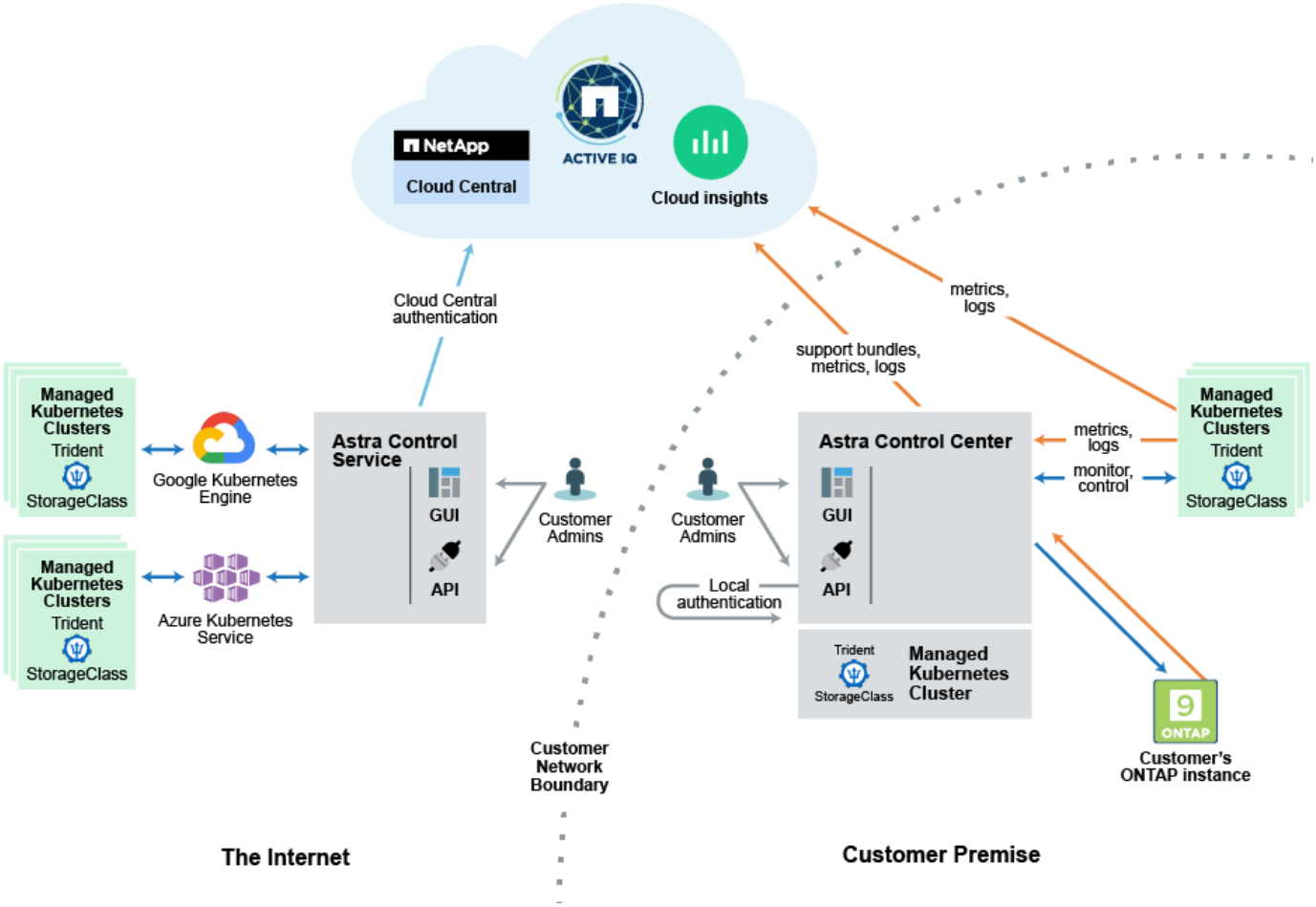
Astra Control has a REST API that enables you to directly access the Astra Control functionality using a programming language or utility such as Curl. You can also manage Astra Control deployments using Ansible and other automation technologies.

To learn more, go to the Astra automation docs.

Concepts

Architecture and components

Here's an overview of the various components of the Astra Control environment.



Astra Control components

- **Kubernetes clusters**: Kubernetes is a portable, extensible, open-source platform for managing containerized workloads and services, that facilitates both declarative configuration and automation. Astra Control provides management services for applications hosted in a Kubernetes cluster.
- **Trident**: As a fully supported open source storage provisioner and orchestrator maintained by NetApp, Trident enables you to create storage volumes for containerized applications managed by Docker and Kubernetes. When deployed with Astra Control, Trident includes a configured ONTAP storage backend.
- **Storage backend**: Astra Control Service uses NetApp Cloud Volumes Service for Google Cloud as the backend storage for GKE clusters and Azure NetApp Files as the backend storage for AKS clusters.

  Astra Control Center uses an ONTAP AFF and FAS storage backend. As a storage software and hardware platform, ONTAP provides core storage services, support for multiple storage access protocols, and storage management functionality, such as snapshots and mirroring.

- **Cloud Insights**: A NetApp cloud infrastructure monitoring tool, Cloud Insights enables you to monitor performance and utilization for your Kubernetes clusters managed by Astra Control Center. Cloud Insights

correlates storage usage to workloads.

Astra Control interfaces

You can complete tasks using different interfaces:

- **Web user interface (UI)**: Both Astra Control Service and Astra Control Center use the same web-based UI where you can manage, migrate and protect apps. Use the UI to manage user accounts and configuration settings.
- **API**: Both Astra Control Service and Astra Control Center use the same Astra API. Using the API, you can perform the same tasks that you would using the UI.

For more information

- Astra Control Center documentation
- Use the Astra API
- Trident documentation
- Cloud Insights documentation
- ONTAP documentation

Storage classes and PV size for AKS clusters

Astra Control Service uses Azure NetApp Files as the backend storage for Azure Kubernetes Service (AKS) clusters. You should understand how choosing a storage class and persistent volume size can help you meet your performance objectives.

Service levels and storage classes

Azure NetApp Files supports three service levels: Ultra storage, Premium storage, and Standard storage. Each of these service levels are designed for different performance needs:

Ultra storage
: Provides up to 128 MiB/s of throughput per 1 TiB.

Premium storage
: Provides up to 64 MiB/s of throughput per 1 TiB.

Standard storage
: Provides up to 16 Mib/s of throughput per 1 TiB.

These service levels are an attribute of a capacity pool. You need to set up a capacity pool for each service level that you want to use with your Kubernetes clusters. Learn how to set up capacity pools.

Astra Control Service uses these service levels as storage classes for your persistent volumes. When you add Kubernetes compute to Astra Control Service, you’re prompted to choose either Ultra, Premium, or Standard as the default storage class. The names of the storage classes are *netapp-anf-perf-ultra*, *netapp-anf-perf-premium*, and *netapp-anf-perf-standard*.

Learn more about these service levels in the Azure NetApp Files docs.

Persistent volume size and performance

As described above, the throughput for each service level is per 1 TiB of provisioned capacity. That means larger volumes provide better performance. So you should take both capacity and performance needs into consideration when provisioning volumes.

Minimum volume size

Astra Control Service provisions persistent volumes using a minimum volume size of 100 GiB, even if the PVC asks for a smaller volume size. For example, if the PVC in a Helm chart asks for 6 GiB, Astra Control Service automatically provisions a 100 GiB volume.

Service type, storage classes, and PV size for GKE clusters

Astra Control Service uses Cloud Volumes Service for Google Cloud as the backend storage for persistent volumes. You should understand how choosing a service type, storage class, and persistent volume size can help you meet your performance objectives.

Overview

Cloud Volumes Service for Google Cloud provides two service types: *CVS* and *CVS-Performance*. These service types are supported in specific Google Cloud regions. Go to NetApp Cloud Central's Global Regions Maps to identify the service type that's supported in the Google Cloud region where your clusters reside.

If your Kubernetes clusters must reside in a specific region, then you'll be using the service type supported in that region.

But if you have the flexibility to choose between Google Cloud regions, then we recommend the following based on your performance requirements:

- For K8s applications that have medium-to-high performance storage needs, choose a Google Cloud region that supports CVS-Performance and use the Premium or Extreme storage class. Such workloads include AI/ML pipelines, CI/CD pipelines, media processing, and databases including relational, noSQL, time series, etc.
- For K8s applications that have low-to-medium storage performance needs (web apps, general purpose file storage, etc.), choose a Google Cloud region that supports either CVS or CVS-Performance, with the Standard storage class.

The following table provides a quick comparison of the information described on this page.

Service type	Use case	Supported regions	Storage classes	Min volume size
CVS-Performance	Apps with medium-to-high storage performance needs	View supported Google Cloud regions	• netapp-cvs-standard • netapp-cvs-premium • netapp-cvs-extreme	100 GiB

Service type	Use case	Supported regions	Storage classes	Min volume size
CVS	Apps with low-to-medium storage performance needs	View supported Google Cloud regions	netapp-cvs-standard	300 GiB

CVS-Performance service type

Learn more about the CVS-Performance service type before you choose a storage class and create persistent volumes.

Storage classes

Three service levels are supported with the CVS-Performance service type: Standard, Premium, and Extreme. When you add compute to Astra Control Service, you're prompted to choose either Standard, Premium, or Extreme as the default storage class for persistent volumes. Each of these service levels are designed for different capacity and bandwidth needs.

The names of the storage classes are *netapp-cvs-standard*, *netapp-cvs-premium*, and *netapp-cvs-extreme*.

Learn more about these service levels in the Cloud Volumes Service for Google Cloud docs.

Persistent volume size and performance

As the Google Cloud docs explain, the allowed bandwidth for each service level is per GiB of provisioned capacity. That means larger volumes will provide better performance.

Be sure to read through the Google Cloud page linked to above. It includes cost comparisons and examples that can help you better understand how to couple a service level with volume size to meet your performance objectives.

Minimum volume size

Astra Control Service provisions persistent volumes using a minimum volume size of 100 GiB with the CVS-Performance service type, even if the PVC requests a smaller volume size. For example, if the PVC in a Helm chart asks for 6 GiB, Astra Control Service automatically provisions a 100 GiB volume.

CVS service type

Learn more about the CVS service type before you choose a storage class and create persistent volumes.

Storage class

One service level is supported with the CVS service type: Standard. When you manage clusters in regions where the CVS service type is supported, Astra Control Service uses the Standard service level as the default storage class for persistent volumes. The storage class is named *netapp-cvs-standard*.

Learn more about the Standard service level in the Cloud Volumes Service for Google Cloud docs.

Persistent volume size and performance

The allowed bandwidth for the CVS service type is per GiB of provisioned capacity. That means larger volumes will provide better performance.

Minimum volume size

Astra Control Service provisions persistent volumes using a minimum volume size of 300 GiB with the CVS service type, even if the PVC asks for a smaller volume size. For example, if 20 GiB is requested, Astra Control Service automatically provisions a 300 GiB volume.

Due to a limitation, if a PVC requests a volume between 700-999 GiB, Astra Control Service automatically provisions a volume size of 1000 GiB.

Validated vs standard apps

There are two types of applications you can bring to Astra Control: Validated and Standard. Learn the difference between these two categories, and the potential impacts on your projects and strategy.

> It’s tempting to think of these two categories as "supported" and "unsupported." But as you will see, there is no such thing as an "unsupported" app in Astra Control. You can add any app to Astra Control, although validated apps have more infrastructure built around their Astra Control workflows compared to standard apps.

Validated Apps

Validated apps for Astra Control include the following:

- MySQL 0.3.22
- MariaDB 14.14
- PostgreSQL 11.7
- Jenkins 2.249.1 LTS

The short list of validated apps represents applications that Astra Control recognizes. The Astra Control QA team has analyzed and confirmed these apps to be fully tested to restore.

Validated apps have also been checked by the Astra Control Development team, which creates custom workflows to help ensure the safety and consistency of your data. For example, when Astra Control takes a backup of a PostgreSQL database, it first quiesces the database. After the backup is complete, Astra Control restores the database to normal operation.

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

Let us know what apps you would like to see validated in the future. Contact us through the Feedback email address on the Support page.

Standard Apps

Any other app, including custom programs, is considered a standard app. You can add and manage standard apps through Astra Control. You can also create basic crash-consistent Snapshots and Backups of a standard app. However, these have not been QA-tested to restore the app to its original state.

Define a custom app

Creating a custom app lets you group elements of your Kubernetes cluster into a single

app.

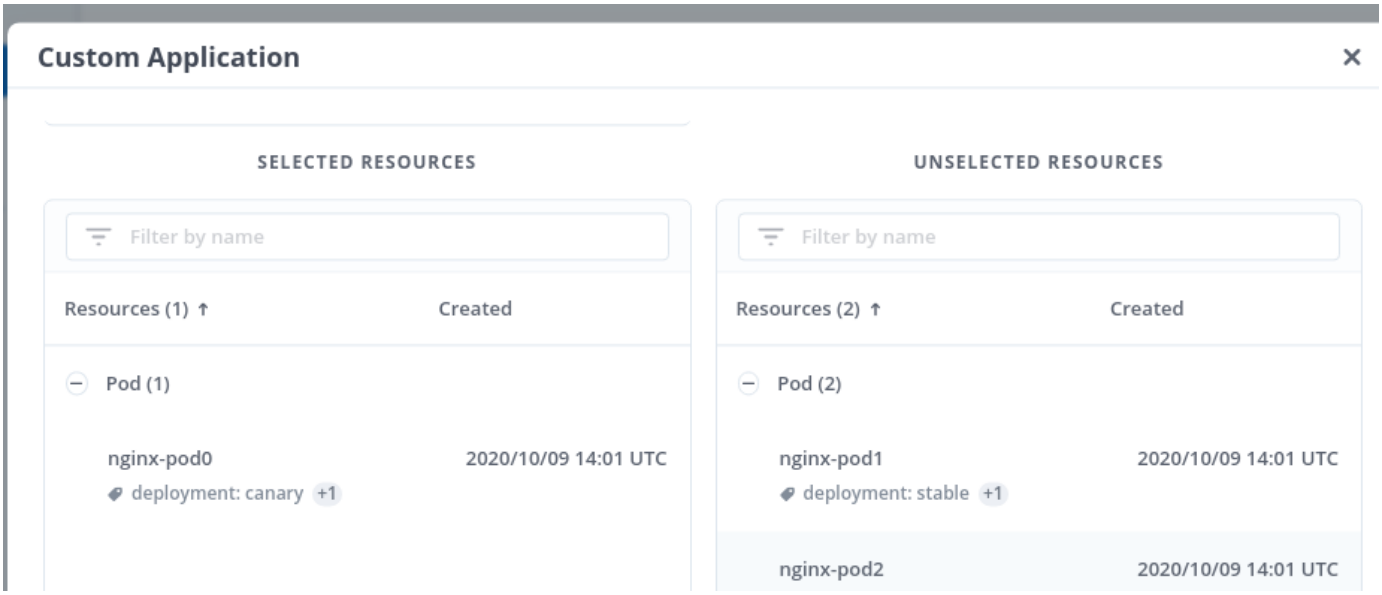
A custom app gives you more granular control over what to include in an Astra Control operation, including:

- Clone
- Snapshot
- Backup
- Protection policy

In most cases you will want to use Astra Control's features on your entire app. However, you can also create a custom app to use these features by the labels you assign to Kubernetes objects in a namespace.

To create a custom app, go to the Apps page and click **+ Define custom app**.

As you make your selections, the Custom App window will show you which resources will be included or excluded from your custom app. This helps you make sure you are choosing the correct criteria for defining your custom app.



In the above example, one resource (the pod `nginx-pod0` labeled `deployment:canary`) will be included in the custom app. Two pods (`nginx-pod` and `nginx-pod2` both labeled `deployment:stable`) will be excluded.

> Custom apps can only be created within a specified namespace on a single cluster. Astra Control does not support the ability for a custom app to span multiple namespaces or clusters.

A label is a key/value pair you can assign to Kubernetes objects for identification. Labels make it easier to sort, organize, and find your Kubernetes objects. To learn more about Kubernetes labels, see the official Kubernetes documentation.

> Overlapping policies for the same resource under different names can cause data conflicts. If you create a custom app for a resource, be sure it's not being cloned or backed up under any other policies.

Example: Separate Protection Policy for canary release

In this example, the DevOps team is managing a canary release deployment. Their cluster has three pods running NginX. Two of the pods are dedicated to the stable release. The third pod is for the canary release.

The team's Kubernetes admin adds the label `deployment=stable` to the stable release pods. The admin also adds the label `deployment=canary` to the canary release pod.

```
:~$ kubectl get pods --namespace=nginx-app --show-labels
NAME         READY   STATUS    RESTARTS   AGE   LABELS
nginx-pod0   1/1     Running   0          50s   deployment=canary,run=nginx-pod0
nginx-pod1   1/1     Running   0          45s   deployment=stable,run=nginx-pod1
nginx-pod2   1/1     Running   0          41s   deployment=stable,run=nginx-pod2
:~$
```

The team's stable release includes a requirement for hourly snapshots and daily backups. The canary release is more ephemeral, so they want to create a less aggressive, short-term protection policy for anything labeled `deployment=canary`.

In order to avoid possible data conflicts, the admin creates two custom apps: one for the canary release, and one for the stable release. This keeps the backups, snapshots, and clone operations separate for the two groups of Kubernetes objects.

After the admin adds the cluster to Astra Control, the next step is to define a custom app. To do this, the admin clicks the **+ Define custom app** button on the Apps page.

In the pop-up window which appears, the admin sets `devops-canary-deployment` as the app name. The admin then chooses the cluster in the **Compute** drop-down, then the app's namespace from the **Namespace** drop-down.

At this point, the admin can either type `deployment=canary` in the **Labels** field, or select that label from the resources listed below.

After defining the custom app for the canary deployment, the admin repeats the process for the stable deployment.

After creating the two custom apps, the admin can treat these resources as any other Astra Control application. The admin can clone them, create backups and snapshots, and create a custom protection policy for each group of resources based on the Kubernetes labels.

Deploy apps

Deploy Jenkins from a Helm chart

Learn how to deploy Jenkins from the Bitnami Helm chart. After you deploy Jenkins on your cluster, you can register the application with Astra Control.

Jenkins is a validated app for Astra Control. Learn the difference between Validated and Standard apps.

These instructions apply to both Astra Control Service and Astra Control Center.

Requirements

- A cluster that has been added to Astra Control.

> For Astra Control Center, you can add the cluster to Astra Control Center first or add the app first.

- Updated versions of Helm (version 3.2+) and Kubectl installed on a local machine with the proper kubeconfig for the cluster

Astra Control does not currently support the Kubernetes plugin for Jenkins. You can run Jenkins in a Kubernetes cluster without the plugin. The plugin provides scalability to your Jenkins cluster.

Install Jenkins

Two important notes on this process:

- You must deploy your app after the cluster is added to Astra Control Service, not before. Astra Control Center will accept applications before or after the cluster is added to Astra Control Center.
- You must deploy the Helm chart in a namespace other than the default.

Steps

1. Add the Bitnami chart repo:

```
helm repo add bitnami https://charts.bitnami.com/bitnami
```

2. Create the `jenkins` namespace and deploy Jenkins into it with the command:

```
Helm install <name> --namespace <namespace> --create-namespace --set
persistence.storageClass=<storage_class>
```

> If the volume size is changed, use Kibibyte (Ki), Mebibyte (Mi) or Gibibyte (Gi) units.

You need to define the storage class only in these situations:

- You are using Astra Control Service and you don't want to use the default storage class.

- You are using Astra Control Center and haven't yet imported the cluster into Astra Control Center. Or, you have imported the cluster, but don't want to use the default storage class.

Result

This does the following:

- Creates a namespace.
- Sets the correct storage class.

After the pods are online, you can manage the app with Astra Control. Astra Control enables you to manage an app at the namespace level or by using a helm label.

Deploy MariaDB from a Helm chart

Learn how to deploy MariaDB from the Bitnami Helm chart. After you deploy MariaDB on your cluster, you can manage the application with Astra Control.

MariaDB is a validated app for Astra. Learn the difference between Validated and Standard apps.

These instructions apply to both Astra Control Service and Astra Control Center.

Requirements

- A cluster that has been added to Astra Control.

> For Astra Control Center, you can add the cluster to Astra Control Center first or add the app first.

- Updated versions of Helm (version 3.2+) and Kubectl installed on a local machine with the proper kubeconfig for the cluster

Install MariaDB

Two important notes on this process:

- You must deploy your app after the cluster is added to Astra Control Service, not before. Astra Control Center will accept applications before or after the cluster is added to Astra Control Center.
- You must deploy the Helm chart in a namespace other than the default.

Steps

1. Add the Bitnami chart repo:

```
helm repo add bitnami https://charts.bitnami.com/bitnami
```

2. Deploy MariaDB with the command:

```
Helm install <name> --namespace <namespace> --create-namespace --set
persistence.storageClass=<storage_class>
```

> If the volume size is changed, use Kibibyte (Ki), Mebibyte (Mi) or Gibibyte (Gi) units.

You need to define the storage class only in these situations:

- You are using Astra Control Service and you don't want to use the default storage class.
- You are using Astra Control Center and haven't yet imported the cluster into Astra Control Center. Or, you have imported the cluster, but don't want to use the default storage class.

Result

This does the following:

- Creates a namespace.
- Deploys MariaDB on the namespace.
- Creates a database.

> This method of setting the password at deployment is insecure. We do not recommend this for a production environment.

After the pods are online, you can manage the app with Astra Control. Astra Control enables you to manage an app at the namespace level or by using a helm label.

Deploy MySQL from a Helm chart

Learn how to deploy MySQL from the standard stable chart. After you deploy MySQL on your Kubernetes cluster, you can manage the application with Astra Control.

MySQL is a validated app for Astra Control. Learn the difference between Validated and Standard apps.

These instructions apply to both Astra Control Service and Astra Control Center.

Requirements

- A cluster that has been added to Astra Control.

> For Astra Control Center, you can add the cluster to Astra Control Center first or add the app first.

- Updated versions of Helm (version 3.2+) and Kubectl installed on a local machine with the proper kubeconfig for the cluster

Install MySQL

Two important notes on this process:

- You must deploy your app after the cluster is added to Astra Control Service, not before. Astra Control Center will accept applications before or after the cluster is added to Astra Control Center.
- We recommend that you deploy the Helm chart in a namespace other than the default.

Steps

1. Add the Bitnami chart repo:

```
helm repo add bitnami https://charts.bitnami.com/bitnami
```

2. Deploy MySQL with the command:

```
Helm install <name> --namespace <namespace> --create-namespace --set
persistence.storageClass=<storage_class>
```

> If the volume size is changed, use Kibibyte (Ki), Mebibyte (Mi) or Gibibyte (Gi) units.

You need to define the storage class only in these situations:

- You are using Astra Control Service and you don't want to use the default storage class.
- You are using Astra Control Center and haven't yet imported the cluster into Astra Control Center. Or, you have imported the cluster, but don't want to use the default storage class.

Result

This does the following:

- Creates a namespace.
- Deploys MySQL on the namespace.

After the pods are online, you can manage the app with Astra Control. Astra Control allows you to manage an app with its name, at the namespace level, or by using a helm label.

Deploy Postgres from a Helm chart

Learn how to deploy Postgres from the Bitnami Helm chart. After you deploy Postgres on your cluster, you can register the application with Astra Control.

Postgres is a validated app for Astra. Learn the difference between Validated and Standard apps.

These instructions apply to both Astra Control Service and Astra Control Center.

Requirements

- A cluster that has been added to Astra Control.

> For Astra Control Center, you can add the cluster to Astra Control Center first or add the app first.

- Updated versions of Helm (version 3.2+) and Kubectl installed on a local machine with the proper kubeconfig for the cluster

Install Postgres

Two important notes on this process:

- You must deploy your app after the cluster is added to Astra Control Service, not before. Astra Control

Center will accept applications before or after the cluster is added to Astra Control Center.

- You must deploy the Helm chart in a namespace other than the default.

Steps

1. Add the Bitnami chart repo:

```
helm repo add bitnami https://charts.bitnami.com/bitnami
```

2. Deploy Postgres with the command:

```
Helm install <name> --namespace <namespace> --create-namespace --set
persistence.storageClass=<storage_class>
```

> If the volume size is changed, use Kibibyte (Ki), Mebibyte (Mi) or Gibibyte (Gi) units.

You need to define the storage class only in these situations:

- You are using Astra Control Service and you don't want to use the default storage class.
- You are using Astra Control Center and haven't yet imported the cluster into Astra Control Center. Or, you have imported the cluster, but don't want to use the default storage class.

Result

This does the following:

- Creates a namespace.
- Deploys Postgres on the namespace.

After the pods are online, you can manage the app with Astra Control. Astra Control enables you to manage an app at the namespace level or by using a helm label.

Knowledge and support

Register for support

Astra Control attempts to automatically register your account for support when you set up your account. If it can't, then you can manually register for support yourself. Support registration is required to obtain help from NetApp technical support.

Verify your support registration

Astra Control includes a Support Status field that enables you to confirm your support registration.

Steps

1. Click **Support**.
2. Take a look at the Support Status field.

   The Support Status starts off as "Not Registered" but then moves to "In-Progress" and finally to "Registered" once complete.

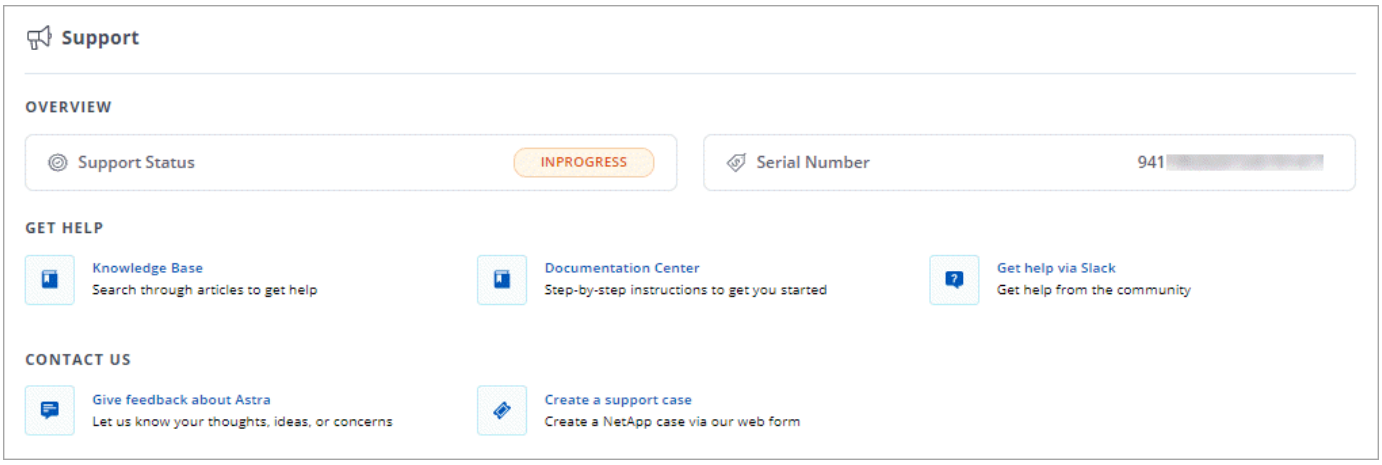
   This support registration status is polled every 15 minutes. New NetApp customers could take up to next business day to complete onboarding and support registration. If the serial number doesn't show "Registered" within 48 hours, you can reach out to NetApp using astra.feedback@netapp.com or register manually from https://register.netapp.com.

Obtain your serial number

When you register for an account, Astra Control uses the information that you provided about your company to generate a 20-digit NetApp serial number that starts with "941."

The NetApp serial number represents your Astra Control account. You'll need to use this serial number when opening a web ticket.

You can find your serial number in the Astra Control interface from the **Support** page.



Activate support entitlement

If Astra Control was unable to automatically register your account for support, then you must register the

NetApp serial number associated with Astra Control to activate support entitlement. We offer 2 options for support registration:

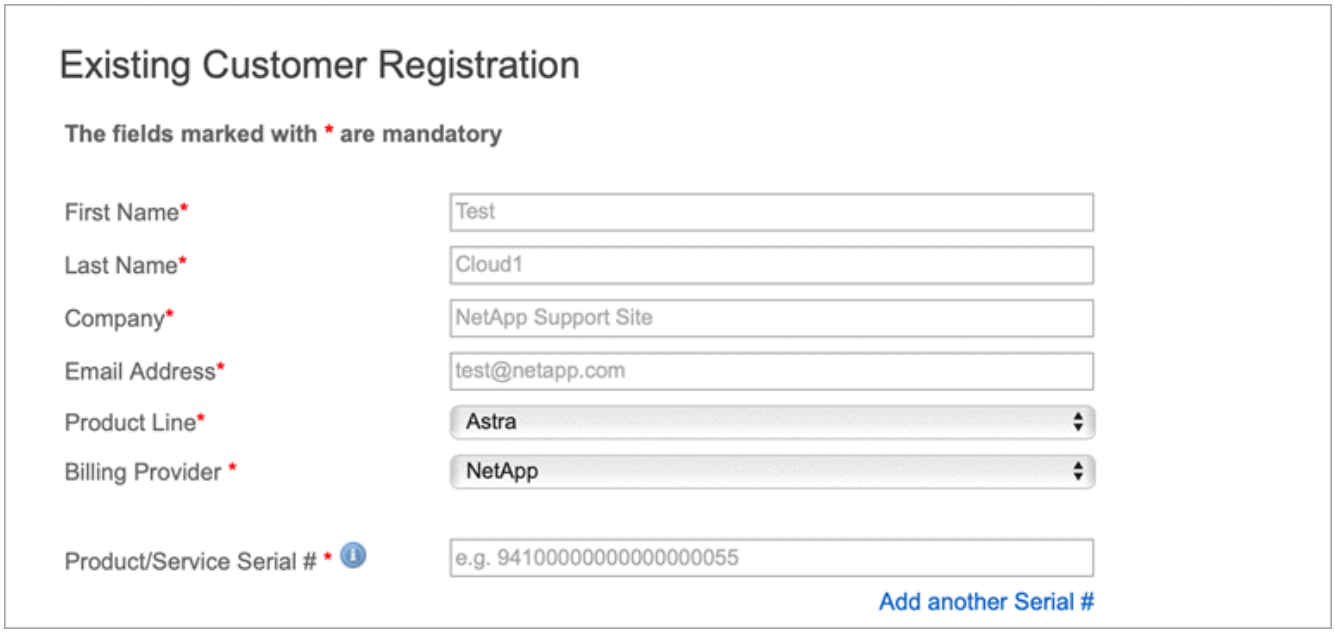
1. Current NetApp customer with existing NetApp Support Site (NSS) SSO account
2. New NetApp customer with no existing NetApp Support Site (NSS) SSO account

Option 1: Current NetApp customer with an existing NetApp Support Site (NSS) account

Steps

1. Navigate to the Cloud Data Services Support Registration page to create an NSS account.
2. Click **I am already registered as a NetApp customer**.
3. Enter your NetApp Support Site credentials to log in.

   The Existing Customer Registration page displays.



4. Complete the required information on the form:
   a. Enter your name, company, and email address.
   b. Select **Astra** as the product line.
   c. Enter your serial number.
   d. Click **Submit Registration**.

Result

You should be redirected to a "Registration Submitted Successfully" page. The email address associated with your registration will receive an email within a couple minutes stating that "your product is now eligible for support."

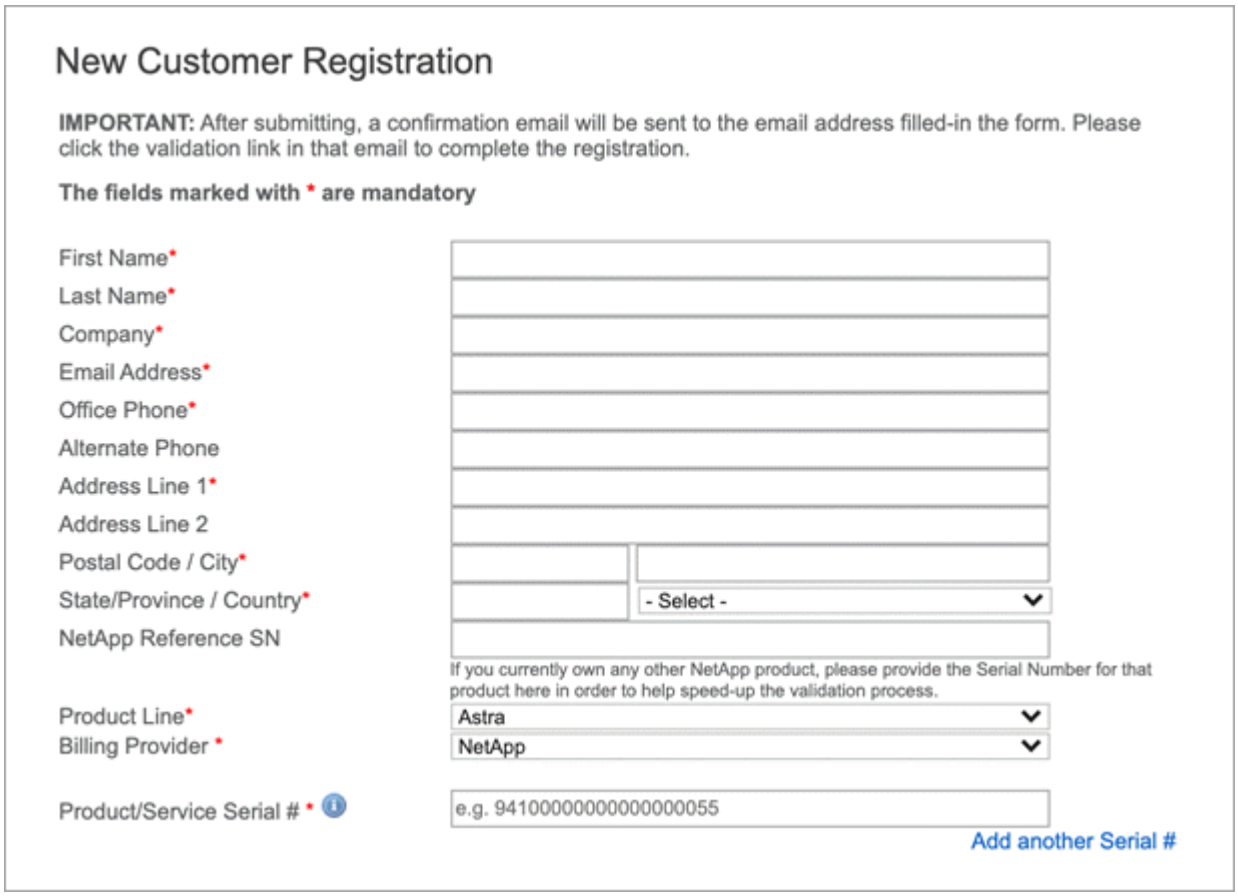
This is a one-time support registration for the applicable serial number.

Option 2: New NetApp customer with no existing NetApp Support Site (NSS) account

Steps

1. Navigate to the Cloud Data Services Support Registration page to create an NSS account.
2. Click **I am not a registered NetApp Customer**.

   The New Customer Registration page displays.



3. Complete the required information on the form:
   a. Enter your name and company information.
   b. Select **Astra** as the Product Line.
   c. Enter your serial number.
   d. Click **Submit Registration**.

      You will receive a confirmation email from your submitted registration. If no errors occur, you will be re-directed to a "Registration Submitted Successfully" page. You will also receive an email within an hour stating that "your product is now eligible for support".

      This is a one-time support registration for the applicable serial number.

4. As a new NetApp customer, you also need to create a NetApp Support Site (NSS) user account for future support activations and for access to the support portal for technical support chat and web ticketing.

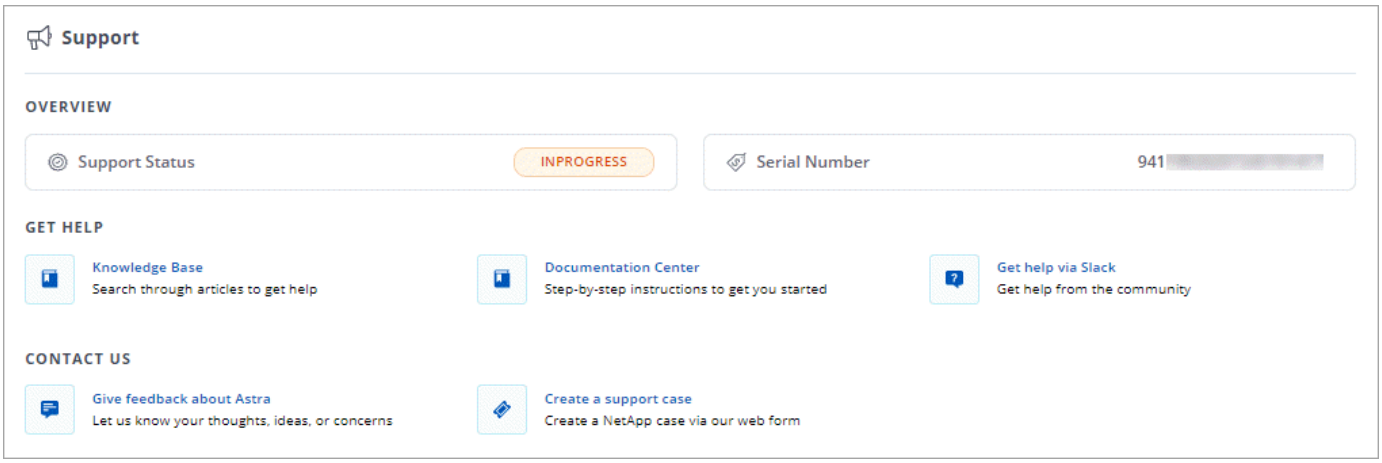
   Go to the NetApp Support Registration site to perform this task. You can provide your newly registered Astra Control serial number to expedite the process.

Get help

NetApp provides support for Astra Control in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a Slack channel. Your Astra Control account includes remote technical support via web ticketing.

You must first activate support for your NetApp serial number in order to use these non self-service support options. A NetApp Support Site (NSS) SSO account is required for chat and web ticketing along with case management.

You can access support options from the Astra Control UI by selecting the **Support** tab from the main menu.



Self support

These options are available for free 24x7:

- Knowledge base

  Search for articles, FAQ's, or Break Fix information related to Astra Control.

- Documentation

  This is the doc site that you're currently viewing.

- Slack

  Go to the containers channel in thePub workspace to connect with peers and experts.

- Feedback email

  Send an email to astra.feedback@netapp.com to let us know your thoughts, ideas, or concerns.

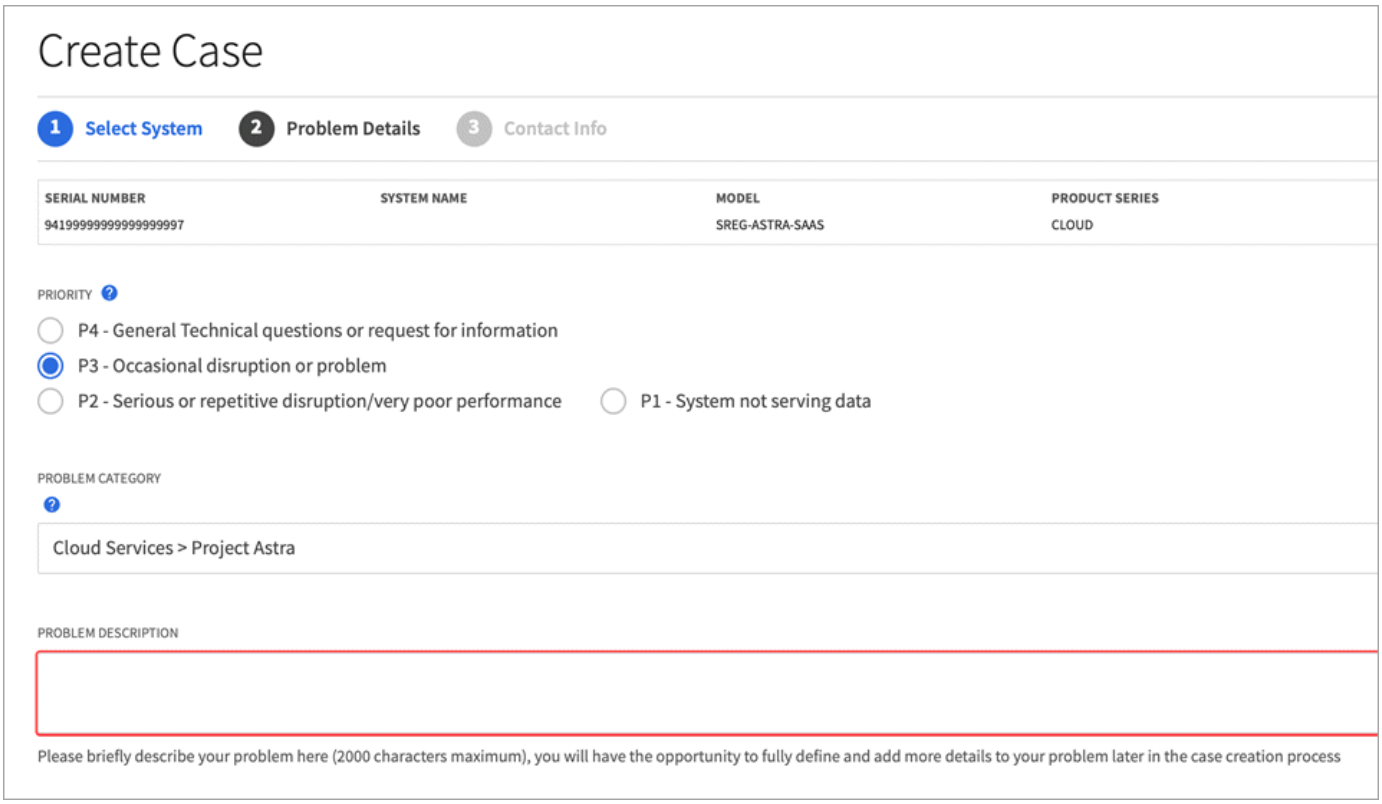
Subscription support

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

Once your Astra Control serial number is activated, you can access NetApp technical support resources by creating a Support ticket.

Select **Cloud Data Services > Astra**.

Use your "941" serial number to open the web ticket. Learn more about your serial number.



Legal notices

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

Copyright

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

Trademarks

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

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

Patents

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

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

Privacy policy

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

Astra Control API license

https://docs.netapp.com/us-en/astra-automation/media/astra-api-license.pdf

Open source

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

Notice for Astra

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

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

Trademark Information

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