



## **Use Astra**

### **Astra Control Center**

NetApp

February 12, 2024

# Table of Contents

- Use Astra ..... 1
  - Manage apps ..... 1
  - Protect apps ..... 7
  - View app and cluster health ..... 12
  - Manage your account. .... 15
  - Manage buckets. .... 20
  - Manage the storage backend. .... 21
  - Monitor and protect infrastructure ..... 23
  - Update an existing license ..... 29
  - Unmanage apps and clusters ..... 30
  - Uninstall Astra Control Center ..... 31

# Use Astra

## Manage apps

### Start managing apps

After you [add a cluster to Astra Control management](#), 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 and their resources.

### Install apps on your cluster

Now that you've added your cluster to Astra Control, you can install apps or manage existing apps on the cluster. Any app that is scoped to a namespace can be managed. After the pods are online, you can manage the app with Astra Control.

For help with deploying validated apps 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.



Apps deployed with Helm 2 are not supported.

You can perform the following activities to manage apps:

- Manage apps
  - [Manage apps by namespace](#)
  - [Manage apps by Kubernetes label](#)
- [Ignore apps](#)
- [Unmanage apps](#)



Astra Control itself is not a standard app; it is a "system app." You should not try to manage Astra Control itself. Astra Control itself isn't shown by default for management. To see system apps, use the "Show system apps" filter.

For instructions on how to manage apps using the Astra API, see the [Astra Automation and API information](#).



After a data protection operation (clone, backup, restore) and subsequent persistent volume resize, there is up to a twenty-minute delay before the new volume size is shown in the UI. The data protection operation is successful within minutes, and you can use the management software for the storage backend to confirm the change in volume size.

## Manage apps by namespace

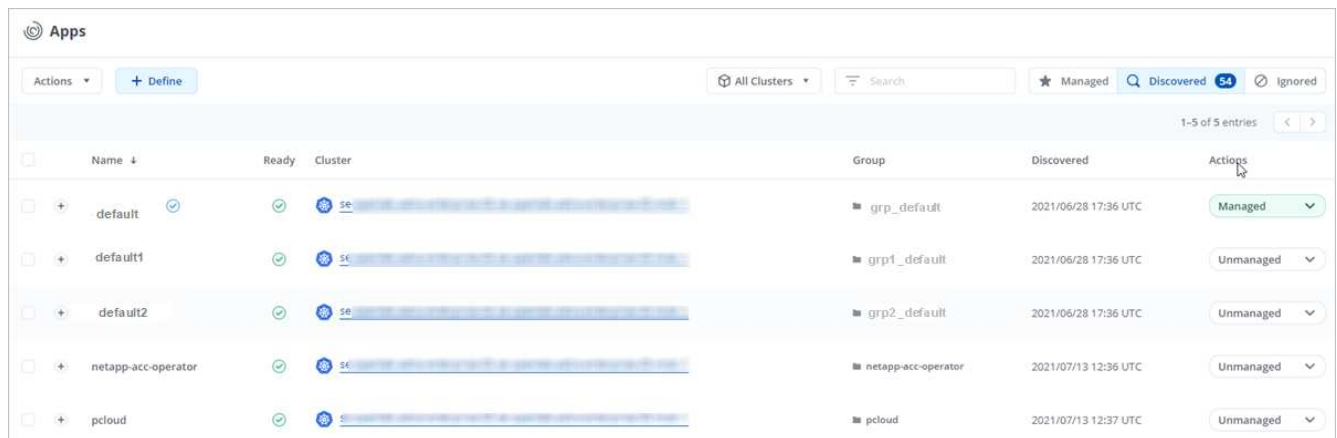
The **Discovered** section of the Apps page shows namespaces and any Helm-installed apps or custom-labeled apps in those namespaces. You can choose to manage each app individually or at the namespace level. It all comes down to the level of granularity that you need for data protection operations.

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 enables 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. From the left navigation bar, select **Apps**.
2. Select **Discovered**.



The screenshot shows the 'Apps' page in Astra Control. At the top, there's a navigation bar with 'Actions' and '+ Define' buttons. Below that, a filter bar shows 'All Clusters', a search bar, and tabs for 'Managed', 'Discovered' (54), and 'Ignored'. The main table lists discovered namespaces and their apps. The columns are: Name, Ready, Cluster, Group, Discovered, and Actions. The 'Name' column has expandable rows for 'default', 'default1', and 'default2'. The 'Group' column shows the namespace for each app. The 'Discovered' column shows the discovery timestamp. The 'Actions' column has a dropdown menu for each app, with options like 'Managed' and 'Unmanaged'.

Name	Ready	Cluster	Group	Discovered	Actions
default	✓	se...	grp_default	2021/06/28 17:36 UTC	Managed
default1	✓	se...	grp1_default	2021/06/28 17:36 UTC	Unmanaged
default2	✓	se...	grp2_default	2021/06/28 17:36 UTC	Unmanaged
netapp-acc-operator	✓	se...	netapp-acc-operator	2021/07/13 12:36 UTC	Unmanaged
pcloud	✓	se...	pcloud	2021/07/13 12:37 UTC	Unmanaged

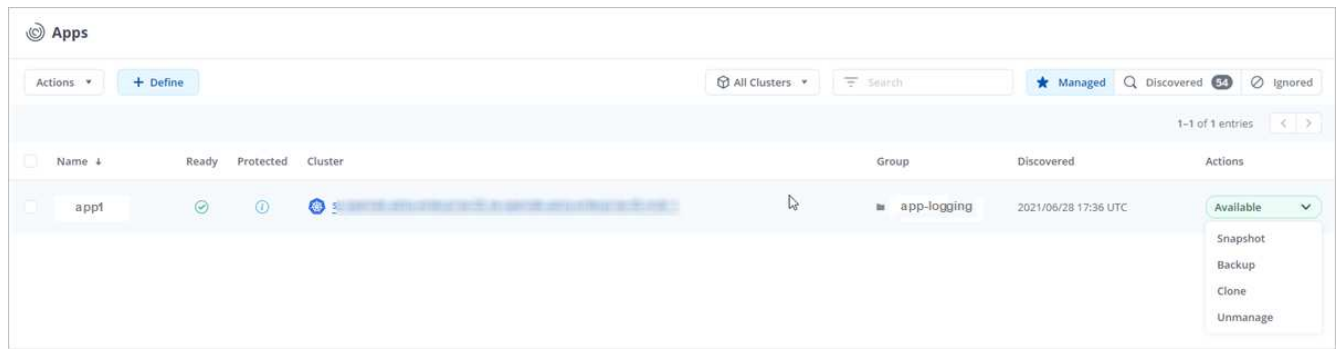
3. View the list of discovered namespaces. Expand the namespace to view the apps and associated resources.

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

4. Look at the **Group** column to see which namespace the application is running in (it's designated with the folder icon).
5. Decide whether you want to manage each app individually or at the namespace level.
6. Find the app you want at the desired level in the hierarchy, and from the Actions menu, select **Manage**.
7. If you don't want to manage an app, from the Actions menu next to the app, select **Ignore**.

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

8. To see the list of managed apps, select **Managed** as the display filter.



Notice the app you just added has a warning icon under the Protected column, indicating that it is not backed up and not scheduled for backups yet.

9. To see details of a particular app, select the app name.

## 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 custom apps by Kubernetes label.](#)

## Steps

1. From the left navigation bar, select **Apps**.
2. Select **Define**.

3. 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. **Cluster:** Select the cluster 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).
    - 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.
4. Click **Define custom application**.

## Result

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

## Ignore apps

If an app has been discovered, it appears in the Discovered list. In this case, you can clean up the Discovered list so that new apps that are newly installed are easier to find. Or, you might have apps that you are managing and later decide you no longer want to manage them. If you don't want to manage these apps, you can indicate that they should be ignored.

Also, you might want to manage apps under one namespace together (Namespace-managed). You can ignore apps that you want to exclude from the namespace.

### Steps

1. From the left navigation bar, select **Apps**.
2. Select **Discovered** as the filter.
3. Select the app.
4. From the Actions menu, select **Ignore**.
5. To unignore, from the Actions menu, select **Unignore**.

### Unmanage apps

When you no longer want to back up, snapshot, or clone an app, you can stop managing it.



If you unmanage an app, any backups or snapshots that were created earlier will be lost.

### Steps

1. From the left navigation bar, select **Apps**.
2. Select **Managed** as the filter.
3. Select the app.
4. From the Actions menu, select **Unmanage**.
5. Review the information.
6. Type "unmanage" to confirm.
7. Select **Yes, Unmanage Application**.

### What about system apps?

Astra Control also discovers the system apps running on a Kubernetes cluster. You can display system apps by selecting the **Show system apps** checkbox under the Cluster filter in the toolbar.

The screenshot shows the 'Apps' management interface. At the top, there's a toolbar with 'Actions' and '+ Define'. Below it, a table lists discovered apps. The table has columns: Name, Ready, Cluster, and Actions. A 'Clusters' filter dropdown is open, showing a 'Show system apps' checkbox which is checked. The table lists several apps, including 'default', which is in a 'Discovering' state.

Name	Ready	Cluster	Actions
...	...	...	...
...	...	...	...
...	...	...	...
default	...	...	Discovering

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



Astra Control itself is not a standard app; it is a "system app." You should not try to manage Astra Control itself. Astra Control itself isn't shown by default for management. To see system apps, use the "Show system apps" filter.

## Find more information

- [Use the Astra API](#)

## Define a custom app example

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**.

As you make your selections, the Custom App window shows 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.



Custom apps can be created only 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 devops team's Kubernetes admin adds the label `deployment=stable` to the stable release pods. The team adds the label `deployment=canary` to the canary release pod.

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 will create 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.



## Steps

1. After the team adds the cluster to Astra Control, the next step is to define a custom app. To do this, the team clicks the **+ Define** button on the Apps page.
2. In the pop-up window which appears, the team sets `devops-canary-deployment` as the app name. The team chooses the cluster in the **Cluster** drop-down, then the app's namespace from the **Namespace** drop-down.
3. The team can either type `deployment=canary` in the **Labels** field, or select that label from the resources listed below.
4. After defining the custom app for the canary deployment, the team repeats the process for the stable deployment.

When the team has finished creating the two custom apps, they can treat these resources as any other Astra Control application. They can clone them, create backups and snapshots, and create a custom Protection Policy for each group of resources based on the Kubernetes labels.

## Protect apps

### 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. You can use the Astra UI or [the Astra API](#) to protect apps.



If you use Helm to deploy apps, Astra Control Center requires Helm version 3. Managing and cloning apps deployed with Helm 3 (or upgraded from Helm 2 to Helm 3) are fully supported. Apps deployed with Helm 2 are not supported.



When you create a project for hosting an app on an OpenShift cluster, the project (or Kubernetes namespace) is assigned a SecurityContext UID. To enable Astra Control Center to protect your app and move the app to another cluster or project in OpenShift, you need to add policies that enable the app to run as any UID. As an example, the following OpenShift CLI commands grant the appropriate policies to a WordPress app.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

### 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. Snapshots are useful for fast clones; snapshots include all of the Kubernetes objects for the app, including configuration files.

A *backup* is stored in the external object store. A backup can be slower to take compared to local snapshots. You can migrate an app by restoring its backup to a different cluster. 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 its 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 an 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 hourly, daily, weekly, and monthly.

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

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

5. Click **Review**.
6. Click **Set Protection Policy**.

### Result

Astra Control Center 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**.
5. Review the snapshot summary and click **Snapshot**.

### Result

The snapshot process begins. A snapshot is successful when the status is **Available** in the **Actions** column on the **Data protection > Snapshots** page.

## Create a backup

You can also back up an app at any time.



S3 buckets in Astra Control Center do not report available capacity. Before backing up or cloning apps managed by Astra Control Center, check bucket information in the ONTAP or StorageGRID management system.

## 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.
5. Choose whether to back up the app from an existing snapshot. If you select this option, you can choose from a list of existing snapshots.
6. Choose a destination for the backup by selecting from the list of storage buckets.
7. Click **Review**.
8. Review the backup summary and click **Backup**.

## Result

Astra Control Center creates a backup of the app.



If your network has an outage or is abnormally slow, a backup operation might time out. This causes the backup to fail.



There is no way to stop a running backup. If you need to delete the backup, wait until it has completed and then use the instructions in [Delete backups](#). To delete a failed backup, [use the Astra API](#).



After a data protection operation (clone, backup, restore) and subsequent persistent volume resize, there is up to a twenty-minute delay before the new volume size is shown in the UI. The data protection operation is successful within minutes, and you can use the management software for the storage backend to confirm the change in volume size.

## 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 an 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 an 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 word "delete" to confirm deletion and then click **Yes, Delete snapshot**.

## Result

Astra Control Center deletes the snapshot.

## Delete backups

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



There is no way to stop a running backup. If you need to delete the backup, wait until it has completed and then use these instructions. To delete a failed backup, [use the Astra API](#).

1. Click **Apps** and then click the name of an 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 word "delete" to confirm deletion and then click **Yes, Delete backup**.

## Result

Astra Control Center deletes the backup.

## Restore apps

Astra Control Center can restore your application from a snapshot or backup. Persistent storage backups and snapshots are transferred from your object store, so restoring from an existing snapshot to the same cluster will be faster than other methods. You can use the Astra UI or [the Astra API](#) to restore apps.



If you use Helm to deploy apps, Astra Control Center requires Helm version 3. Managing and cloning apps deployed with Helm 3 (or upgraded from Helm 2 to Helm 3) are fully supported. Apps deployed with Helm 2 are not supported.



If you restore to a different cluster, ensure that the cluster is using the same persistent volume access mode (for example, ReadWriteMany). The restore operation will fail if the destination persistent volume access mode is different.



When you create a project for hosting an app on an OpenShift cluster, the project (or Kubernetes namespace) is assigned a SecurityContext UID. To enable Astra Control Center to protect your app and move the app to another cluster or project in OpenShift, you need to add policies that enable the app to run as any UID. As an example, the following OpenShift CLI commands grant the appropriate policies to a WordPress app.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

## Steps

1. Click **Apps** and then click the name of an app.
2. Click **Data protection**.
3. If you want to restore from a snapshot, keep the **Snapshots** icon selected. Otherwise, click the **Backups** icon 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 restore:
  - Enter a name and namespace for the app.



If you are restoring an app that has been deleted, choose a different name and namespace for the app than the original name. If the name for the restored app is the same as the deleted app, the restore operation will fail.

- Choose the destination cluster for the app.
  - Click **Review**.
7. **Restore Summary**: Review details about the restore action and click **Restore**.

## Result

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



After a data protection operation (clone, backup, restore) and subsequent persistent volume resize, there is up to a twenty-minute delay before the new volume size is shown in the UI. The data protection operation is successful within minutes, and you can use the management software for the storage backend to confirm the change in volume size.

## 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. You can use the Astra UI or [the Astra API](#) to clone and migrate apps.



If you clone an app between clusters, the source and destination clusters must be the same distribution of OpenShift. For example, if you clone an app from an OpenShift 4.7 cluster, use a destination cluster that is also OpenShift 4.7.

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



S3 buckets in Astra Control Center do not report available capacity. Before backing up or cloning apps managed by Astra Control Center, check bucket information in the ONTAP or StorageGRID management system.



When you create a project for hosting an app on an OpenShift cluster, the project (or Kubernetes namespace) is assigned a SecurityContext UID. To enable Astra Control Center to protect your app and move the app to another cluster or project in OpenShift, you need to add policies that enable the app to run as any UID. As an example, the following OpenShift CLI commands grant the appropriate policies to a WordPress app.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

## What you'll need

To clone apps to a different cluster, you need a default bucket. When you add your first bucket, it becomes the default bucket.

## Steps

1. Click **Apps**.
2. Do one of the following:
  - Click the drop-down list in the **Actions** column for the desired app.
  - Click the name of the desired app, and select the status drop-down list at the top right of the page.
3. Click **Clone**.
4. **Clone details**: Specify details for the clone:
  - Enter a name.
  - Enter a namespace for the clone.
  - Choose a destination cluster 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 Center creates the clone from the app's current state.
5. **Source**: If you chose to clone from an existing snapshot or backup, choose the snapshot or backup that you'd like to use.
6. Click **Review**.
7. **Clone Summary**: Review the details about the clone and click **Clone**.

## Result

Astra Control Center clones that app based on the information that you provided. The clone operation is successful when the new app clone is in the `Available` state on the **Apps** page.



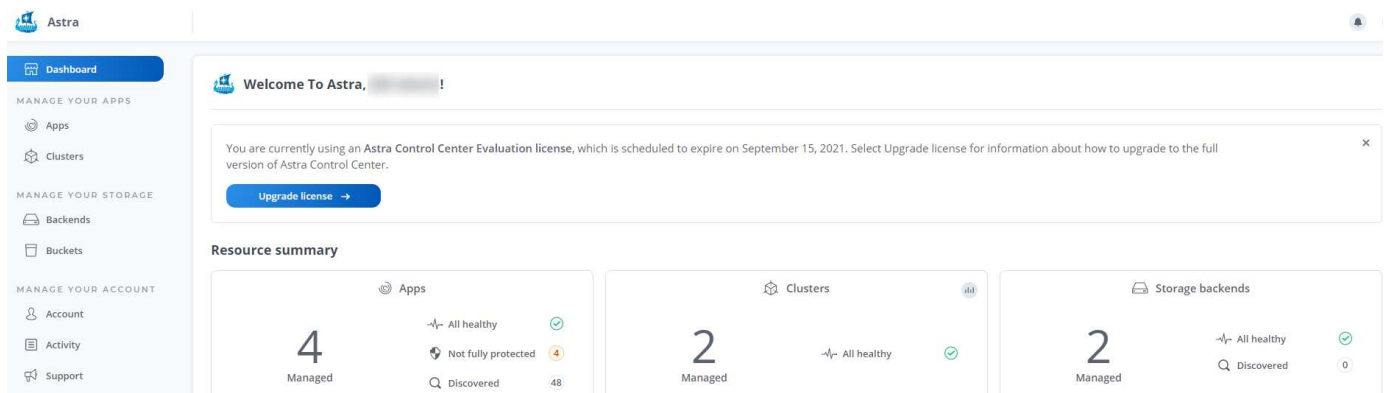
After a data protection operation (clone, backup, restore) and subsequent persistent volume resize, there is up to a twenty-minute delay before the new volume size is shown in the UI. The data protection operation is successful within minutes, and you can use the management software for the storage backend to confirm the change in volume size.

# View app and cluster health

## View a summary of app and cluster health

Select the **Dashboard** to see a high-level view of your apps, clusters, storage backends,

and their health.



These aren't just static 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.

## Apps tile

The **Apps** tile helps you identify the following:

- How many apps you're currently managing with Astra.
- 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.

## Clusters tile

The **Clusters** tile provides similar details about the health of the clusters that you are managing by using Astra Control Center, and you can drill down to get more details just like you can with an app.

## Storage backends tile

The **Storage backends** tile provides information to help you identify the health of storage backends including:

- How many storage backends are managed
- Whether these managed backends are healthy
- Whether the backends are fully protected
- The number of backends that are discovered, but are not yet managed.

## View the health and details of clusters

After you add clusters to be managed by Astra Control Center, you can view details about the cluster, such as its location, the worker nodes, persistent volumes, and storage classes.

## Steps

1. In the Astra Control Center UI, select **Clusters**.
2. On the **Clusters** page, select the cluster whose details you want to view.
3. View the information on the **Overview**, **Storage**, and **Activity** 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**: Shows the activities related to the cluster.



You can also view cluster information starting from the Astra Control Center **Dashboard**. On the **Clusters** tab under **Resource summary**, you can select the managed clusters, which takes you to the **Clusters** page. After you get to the **Clusters** page, follow the steps outlined above.

## View the health and details of an app

After you start managing an app, Astra 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. In the Astra Control Center UI, select **Apps** and then select 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 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 its 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

Shows the activities related to the app.



You can also view app information starting from the Astra Control Center **Dashboard**. On the **Apps** tab under **Resource summary**, you can select the managed apps, which takes you to the **Apps** page. After you get to the **Apps** page, follow the steps outlined above.

# Manage your account

## Manage users

You can add, remove, and edit users of your Astra Control Center installation using the Astra Control Center UI. You can use the Astra UI or [the Astra API](#) to manage users.

### Add users

Account Owners and Admins can add more users to the Astra Control Center installation.

### Steps

1. In the **Manage Your Account** navigation area, click **Account**.
2. Select the **Users** tab.
3. Select **Add User**.
4. Enter the user's name, email address, and a temporary password.

The user will need to change the password upon first login.

5. Select a user role with the appropriate system permissions.

Each role provides the following permissions:

- A **Viewer** can view resources.
- A **Member** has Viewer role permissions and can manage apps and clusters, but cannot unmanage apps or clusters, or delete snapshots or backups.
- An **Admin** has Member role permissions and can add and remove any other users except the Owner.
- An **Owner** has Admin role permissions and can add and remove any user accounts.

6. Click **Add**.

## Manage passwords

You can manage passwords for user accounts in Astra Control Center.

## Change your password

You can change the password of your user account at any time.

### Steps

1. Click the User icon at the top right of the screen.
2. Select **Profile**.
3. Click the **Actions** drop-down list, and select **Change Password**.
4. Enter a password that conforms to the password requirements.
5. Enter the password again to confirm.
6. Click **Change password**.

## Reset another user's password

If your account has Admin or Owner role permissions, you can reset passwords for other user accounts as well as your own. When you reset a password, you assign a temporary password that the user will have to change upon logging in.

### Steps

1. In the **Manage Your Account** navigation area, click **Account**.
2. In the **Users** tab, select the drop-down list in the **State** column for the user.
3. Select **Reset Password**.
4. Enter a temporary password that conforms to the password requirements.
5. Enter the password again to confirm.



Next time the user logs in, the user will be prompted to change the password.

6. Click **Reset password**.

## Change a user's role

Users with the Owner role can change the role of all users, while users with the Admin role can change the role of users who have the Admin, Member, or Viewer role.

### Steps

1. In the **Manage Your Account** navigation area, 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 Center updates the user's permissions based on the new role that you selected.

## Remove users

Users with the Owner or Admin role can remove other users from the account at any time.

### Steps

1. In the **Manage Your Account** navigation area, click **Account**.

2. In the **Users** tab, select the checkbox in the row of each user that you want to remove.
3. Click **Actions** and select **Remove user/s**.
4. When you're prompted, confirm deletion by typing the word "remove" and then click **Yes, Remove User**.

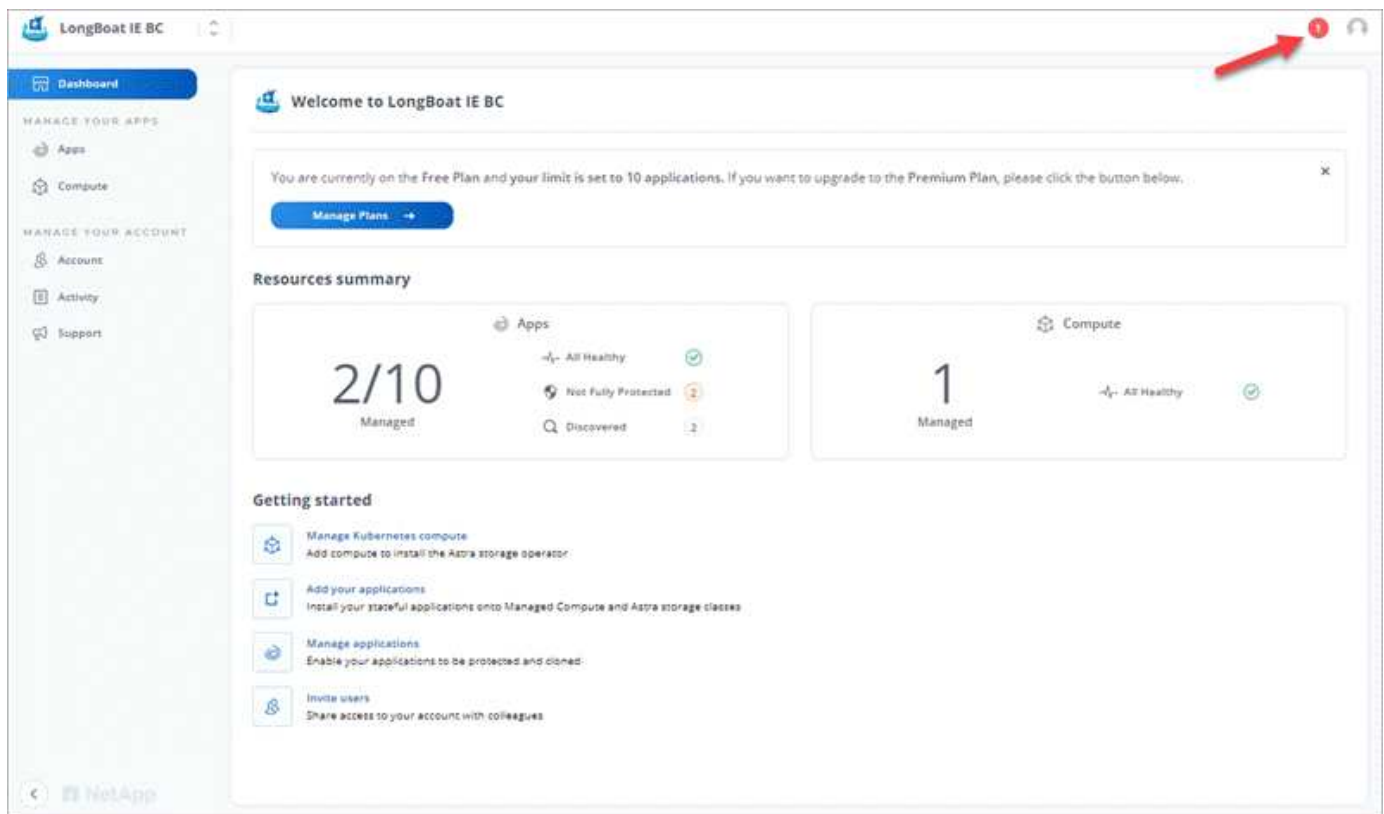
## Result

Astra Control Center removes the user from the account.

## View and manage notifications

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

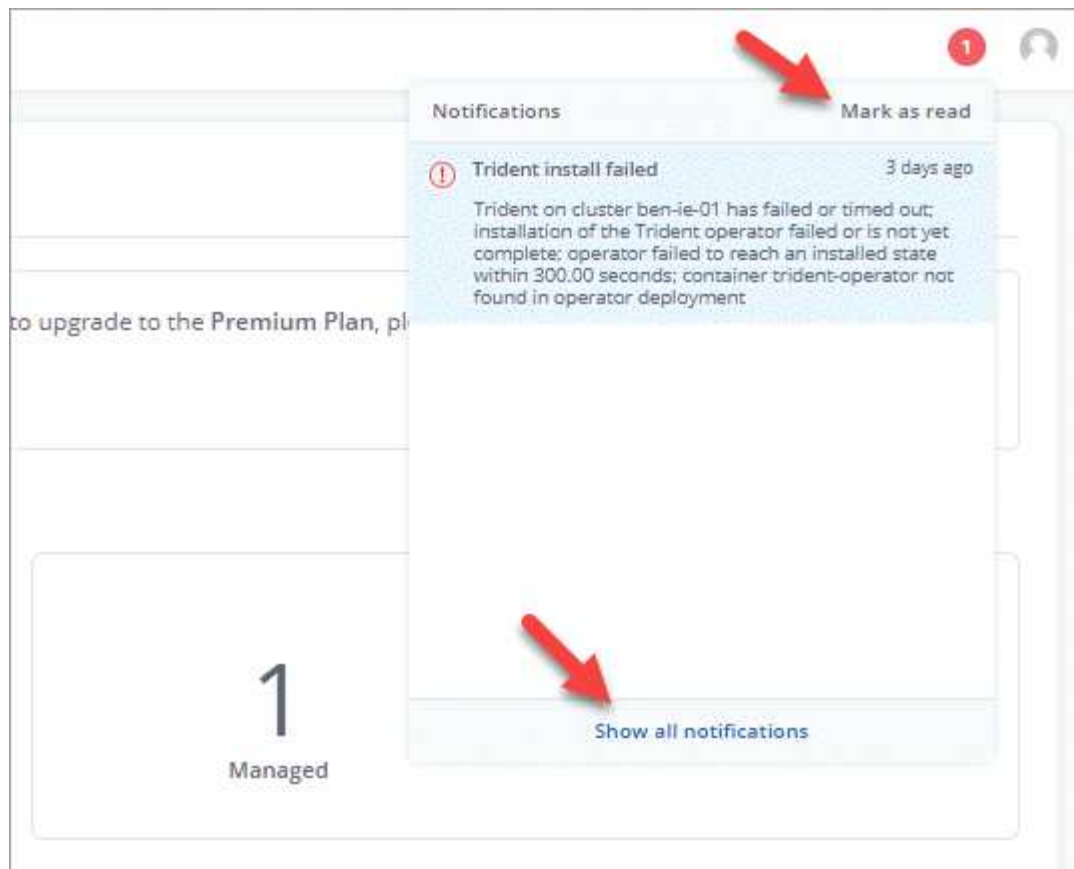
The number of unread notifications is available in the top right of the interface:



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**.

## Add and remove credentials

Add and remove credentials for local private cloud providers such as ONTAP S3, Kubernetes clusters managed with OpenShift, or unmanaged Kubernetes clusters from your account at any time. Astra Control Center uses these credentials to discover Kubernetes clusters and the apps on the clusters, and to provision resources on your behalf.

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

### Add credentials

You can add credentials to Astra Control Center when you manage clusters. To add credentials by adding a new cluster, see [Add a Kubernetes cluster](#).



If you create your own `kubeconfig` file, you should define only **one** context element in it. See [Kubernetes documentation](#) for information about creating `kubeconfig` files.

### Remove credentials

Remove credentials from an account at any time. You should only remove credentials after [unmanaging all](#)

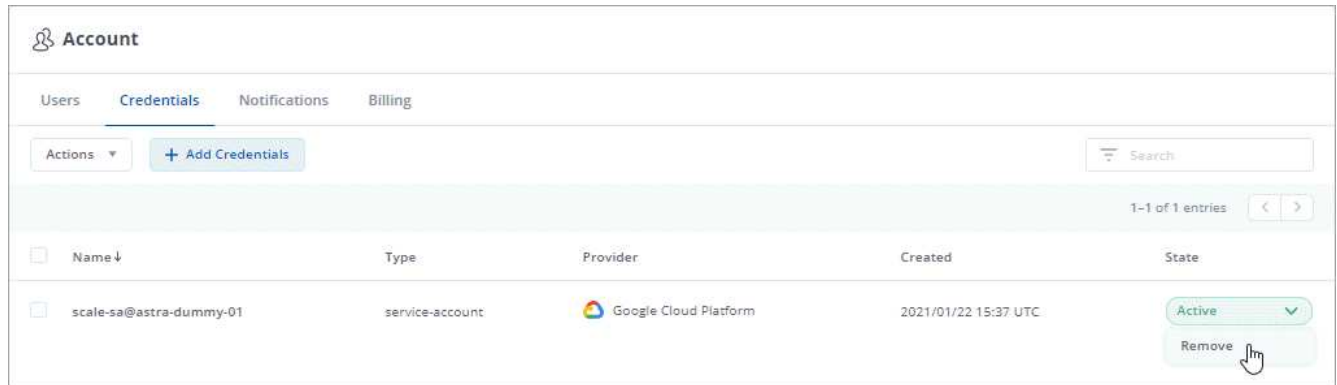
associated clusters.



The first set of credentials that you add to Astra Control Center is always in use because Astra Control Center 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 word "remove" to confirm deletion and then click **Yes, Remove Credential**.

### Result

Astra Control Center removes the credentials from the account.

## Update an existing license

You can convert an evaluation license to a full license, or you can update an existing evaluation or full license with a new license. If you don't have a full license, work with your NetApp sales contact to obtain a full license and serial number. You can use the Astra UI or [the Astra API](#) to update an existing license.

### Steps

1. Log in to the NetApp Support Site.
2. Access the Astra Control Center Download page, enter the serial number, and download the full NetApp license file (NLF).
3. Log in to the Astra Control Center UI.
4. From the left navigation, select **Account > License**.
5. In the **Account > License** page, click the status drop-down menu for the existing license and select **Replace**.
6. Browse to the license file that you downloaded.
7. Select **Add**.

The **Account > Licenses** page displays the license information, expiration date, license serial number, account ID, and CPU units used.

# Manage buckets

An object store bucket provider is essential if you want to back up your applications and persistent storage or if you want to clone applications across clusters. Using Astra Control Center, add an object store provider as your off-cluster, backup destination for your apps.

You don't need a bucket if you are cloning your application configuration and persistent storage to the same cluster.

Use any of the following bucket providers:

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Generic S3



Although Astra Control Center supports Amazon S3 as a Generic S3 bucket provider, Astra Control Center might not support all object store vendors that claim Amazon's S3 support.

You cannot delete a bucket; however, you can edit it.

A bucket can be in one of these states:

- pending: The bucket is scheduled for discovery.
- available: The bucket is available for use.
- removed: The bucket is not currently accessible.

For instructions on how to manage buckets using the Astra API, see the [Astra Automation and API information](#).

You can do these tasks related to managing buckets:

- [Add a bucket](#)
- [Edit a bucket](#)



S3 buckets in Astra Control Center do not report available capacity. Before backing up or cloning apps managed by Astra Control Center, check bucket information in the ONTAP or StorageGRID management system.

## Remove credentials

Remove S3 credentials from an account at any time using the Astra Control API.

For details, see [Use the Astra Control API](#).



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

## Edit a bucket

You can change the access credential information for a bucket and change whether a selected bucket is the default bucket.



When you add a bucket, select the correct bucket provider type with credentials that are correct for that provider. For example, the UI accepts NetApp ONTAP S3 as the type with StorageGRID credentials; however, this will cause all future app backups and restores using this bucket to fail. See the [Release Notes](#).

### Steps

1. From left navigation, select **Buckets**.
2. From the Actions menu, select **Edit**.
3. Change any information other than the bucket type.



You can't modify the bucket type.

4. Select **Update**.

## Find more information

- [Use the Astra API](#)

## Manage the storage backend

Managing storage clusters in Astra Control as a storage backend enables you to get linkages between persistent volumes (PVs) and the storage backend as well as additional storage metrics. You can monitor storage capacity and health details, including performance if Astra Control Center is connected to Cloud Insights.

For instructions on how to manage storage backends using the Astra API, see the [Astra Automation and API information](#).

You can complete the following tasks related to managing a storage backend:

- [Add a storage backend](#)
- [View storage backend details](#)
- [Unmanage a storage backend](#)

## View storage backend details

You can view storage backend information from the Dashboard or from the Backends option.

### View storage backend details from the Dashboard

#### Steps

1. From the left navigation, select **Dashboard**.
2. Review the Storage backend section that shows the state:
  - **Unhealthy**: The storage is not in an optimal state. This could be due to a latency issue or an app is degraded due to a container issue, for example.
  - **All healthy**: The storage has been managed and is in an optimal state.
  - **Discovered**: The storage has been discovered, but not managed by Astra Control.

## View storage backend details from the Backends option

View information about the backend health, capacity, and performance (IOPS throughput and/or latency).

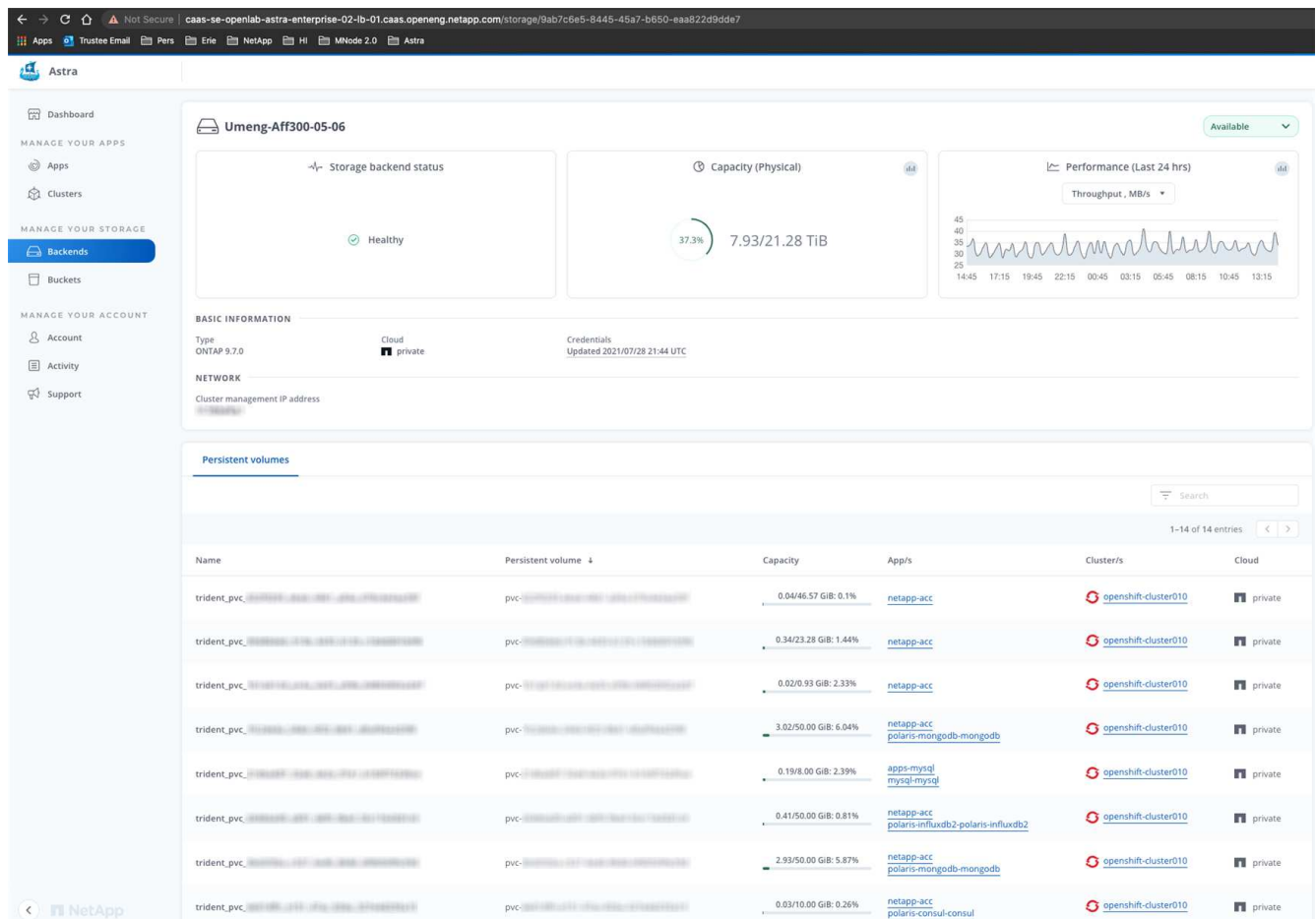
With a connection to Cloud Insights, you can see the volumes that the Kubernetes apps are using, which are stored on a selected storage backend.

### Steps

1. In the left navigation area, select **Backends**.
2. Select the storage backend.



If you connected to NetApp Cloud Insights, excerpts of data from Cloud Insights appear on the Backends page.



3. To go directly to Cloud Insights, click the **Cloud Insights** icon next to the metrics image.

## Unmanage a storage backend

You can unmanage the backend.

### Steps

1. From left navigation, select **Backends**.
2. Select the backend storage.
3. From the Actions menu, select **Unmanage**.



4. Type "unmanage" to confirm the removal.
5. Select **Yes, remove storage backend**.

## Find more information

- [Use the Astra API](#)

## Monitor and protect infrastructure

You can configure several optional settings to enhance your Astra Control Center experience. If the network where you're running Astra Control Center requires a proxy for connecting to the Internet (to upload support bundles to NetApp Support Site or establish a connection to Cloud Insights), you should configure a proxy server in Astra Control Center. To monitor and gain insight into your complete infrastructure, create a connection to NetApp Cloud Insights. To collect Kubernetes events from systems monitored by Astra Control Center, add a Fluentd connection.



After you enable the Cloud Insights connection, you can view throughput information on the **Backends** page as well as connect to Cloud Insights from here after selecting a storage backend. You can also find the information on the **Dashboard** in the Cluster section, and also connect to Cloud Insights from here.

## Add a proxy server

If the network where you're running Astra Control Center requires a proxy for connecting to the Internet (to upload support bundles to NetApp Support Site or establish a connection to Cloud Insights), you should configure a proxy server in Astra Control Center.



Astra Control Center does not validate the details you enter for your proxy server. Ensure that you enter the correct values.

### Steps

1. Log in to Astra Control Center using an account with **admin/owner** privilege.
2. Select **Account > Connections**.
3. Select **Connect** from the drop-down list to add a proxy server.



#### HTTP PROXY

Configure Astra Control to send traffic through a proxy server.

Disconnected



Connect

4. Enter the proxy server name or IP address and the proxy port number.
5. If your proxy server requires authentication, select the checkbox, and enter the username and password.
6. Select **Connect**.

### Result

If the proxy information you entered was saved, the **HTTP Proxy** section of the **Account > Connections** page indicates that it is connected, and displays the server name.



Connected



## HTTP PROXY ?

Server: proxy.example.com:8888

Authentication: Enabled

### Edit proxy server settings

You can edit the proxy server settings.

#### Steps

1. Log in to Astra Control Center using an account with **admin/owner** privilege.
2. Select **Account > Connections**.
3. Select **Edit** from the drop-down list to edit the connection.
4. Edit the server details and authentication information.
5. Select **Save**.

### Disable proxy server connection

You can disable the proxy server connection. You will be warned before you disable that potential disruption to other connections might occur.

#### Steps

1. Log in to Astra Control Center using an account with **admin/owner** privilege.
2. Select **Account > Connections**.
3. Select **Disconnect** from the drop-down list to disable the connection.
4. In the dialog box that opens, confirm the operation.

### Connect to Cloud Insights

To monitor and gain insight into your complete infrastructure, connect NetApp Cloud Insights with your Astra Control Center instance. Cloud Insights is included in your Astra Control Center license.



Cloud Insights should be accessible from the network that Astra Control Center uses, or indirectly via a proxy server.



When Astra Control Center is connected to Cloud Insights, an Acquisition Unit pod gets created. This pod collects data from the storage backends that are managed by Astra Control Center and pushes it to Cloud Insights. This pod requires 8 GB RAM and 2 CPU cores.

#### What you'll need

- An Astra Control Center account with **admin/owner** privileges.
- A valid Astra Control Center license.

- A proxy server if the network where you're running Astra Control Center requires a proxy for connecting to the Internet.



If you are new to Cloud Insights, familiarize yourself with the features and capabilities [here](#).

## Steps

1. Log in to Astra Control Center using an account with **admin/owner** privilege.
2. Select **Account > Connections**.
3. Select **Connect** where it shows **Disconnected** in the drop-down list to add the connection.

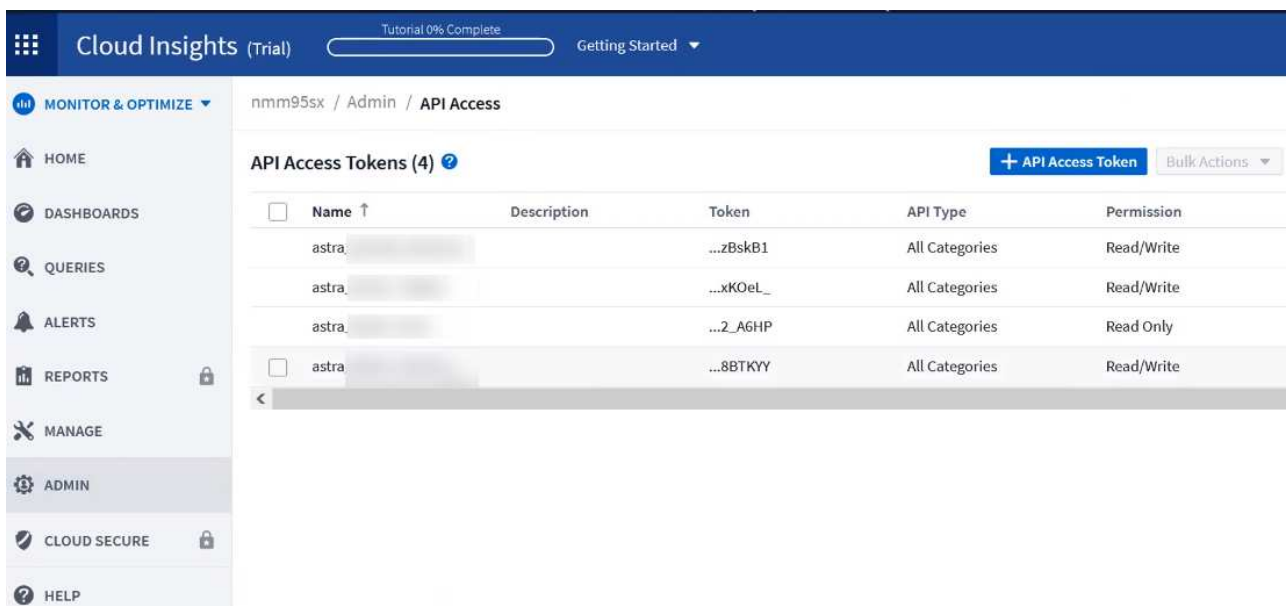


4. Enter the Cloud Insights API tokens and the tenant URL. The tenant URL has the following format, as an example:

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

You get the tenant URL when you get the Cloud Insights license. If you do not have the tenant URL, see the [Cloud Insights documentation](#).

- a. To get the [API token](#), log in to your Cloud Insights tenant URL.
- b. In Cloud Insights, generate a **Read only** type API token.



- c. Copy the **Read only** key. You will need to paste it into the Astra Control Center window for enabling the Cloud Insights connection.

- d. In Cloud Insights, generate a **Read/Write** type API token.
- e. Copy the **Read/Write** key. You will need to paste it into the Astra Control Center **Connect Cloud Insights** window.



We recommend that you generate a **Read only** key and a **Read/Write** key, and not use the same key for both purposes. By default, the token expiry period is set to one year. We recommend that you keep the default selection to give the token the maximum duration before it expires. If your token expires, the telemetry will stop.

- f. Paste the keys that you copied from Cloud Insights into Astra Control Center.

## 5. Select **Connect**.



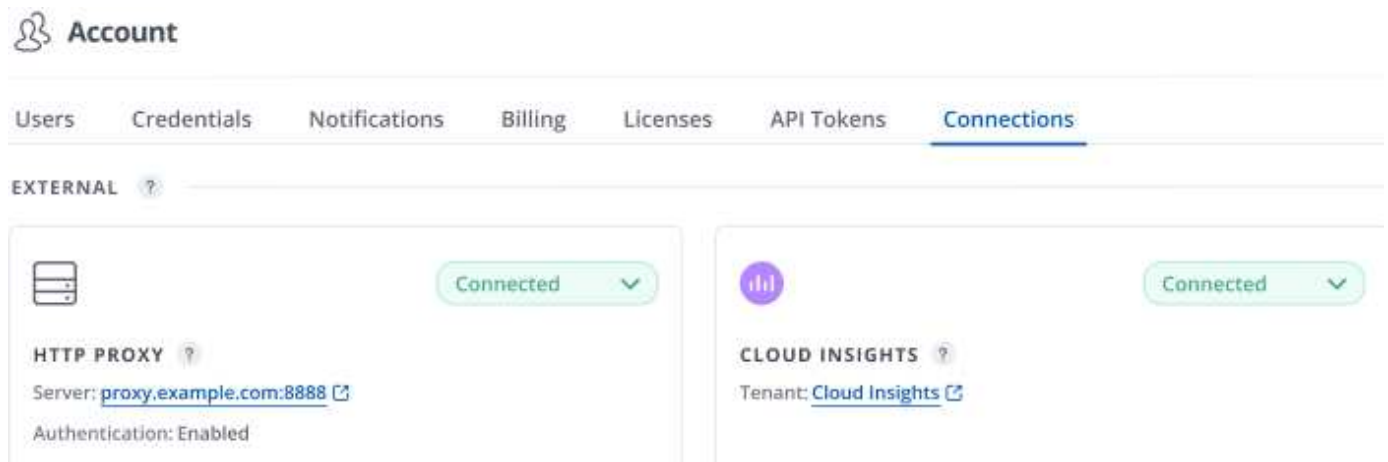
After you select **Connect**, the status of the connection changes to **Pending** in the **Cloud Insights** section of the **Account > Connections** page. It can a few minutes for the connection to be enabled and the status to change to **Connected**.



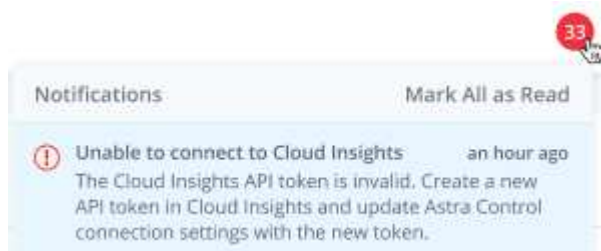
To go back and forth easily between the Astra Control Center and Cloud Insights UIs, ensure that you are logged into both.

## View data in Cloud Insights

If the connection was successful, the **Cloud Insights** section of the **Account > Connections** page indicates that it is connected, and displays the tenant URL. You can visit Cloud Insights to see data being successfully received and displayed.

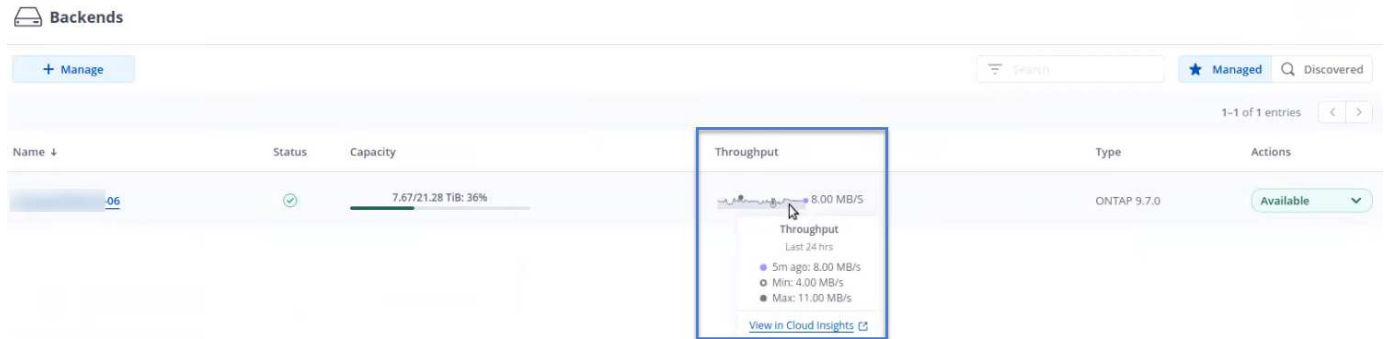


If the connection failed for some reason, the status shows **Failed**. You can find the reason for failure under **Notifications** at the top-right side of the UI.



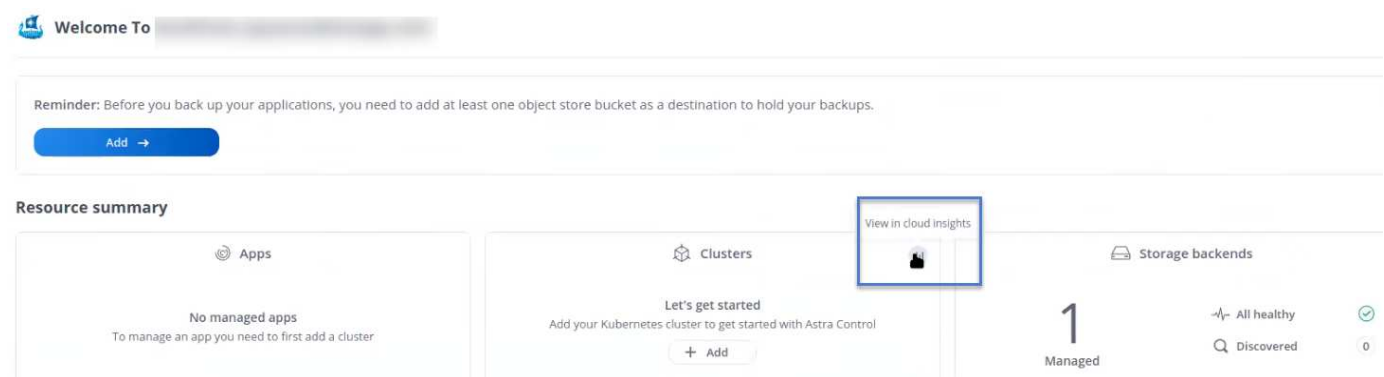
You can also find the same information under **Account > Notifications**.

From Astra Control Center, you can view throughput information on the **Backends** page as well as connect to Cloud Insights from here after selecting a storage backend.



To go directly to Cloud Insights, select the **Cloud Insights** icon next to the metrics image.

You can also find the information on the **Dashboard**.



After enabling the Cloud Insights connection, if you remove the backends that you added in Astra Control Center, the backends stop reporting to Cloud Insights.

## Edit Cloud Insights connection

You can edit the Cloud Insights connection.



You can only edit the API keys. To change the Cloud Insights tenant URL, we recommended that you disconnect the Cloud Insights connection, and connect with the new URL.

## Steps

1. Log in to Astra Control Center using an account with **admin/owner** privilege.
2. Select **Account > Connections**.
3. Select **Edit** from the drop-down list to edit the connection.
4. Edit the Cloud Insights connection settings.
5. Select **Save**.

## Disable Cloud Insights connection

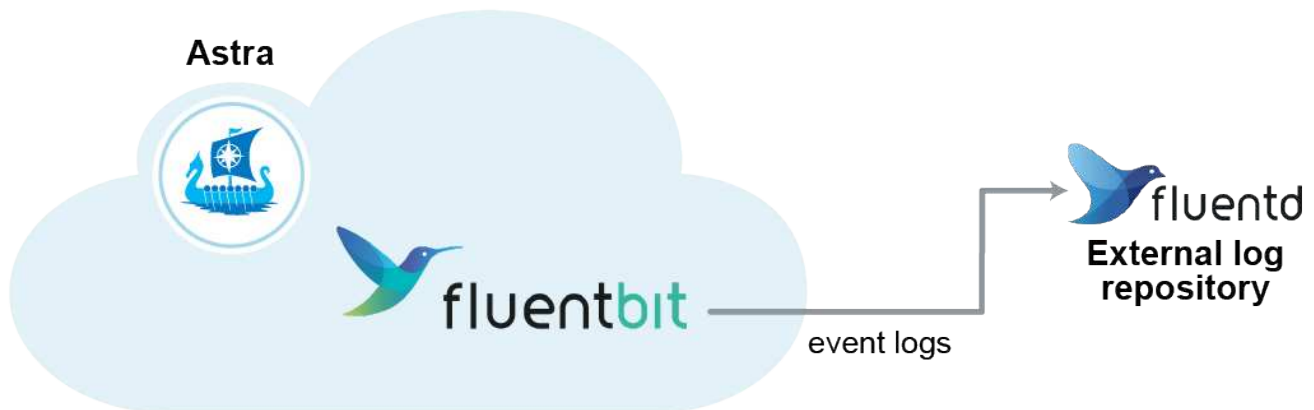
You can disable the Cloud Insights connection for a Kubernetes cluster managed by Astra Control Center. Disabling the Cloud Insights connection does not delete the telemetry data already uploaded to Cloud Insights.

## Steps

1. Log in to Astra Control Center using an account with **admin/owner** privilege.
2. Select **Account > Connections**.
3. Select **Disconnect** from the drop-down list to disable the connection.
4. In the dialog box that opens, confirm the operation.  
After you confirm the operation, on the **Account > Connections** page, the Cloud Insights status changes to **Pending**. It take a few minutes for the status to change to **Disconnected**.

## Connect to Fluentd

You can send logs (Kubernetes events) from Astra Control Center to your Fluentd endpoint. The Fluentd connection is disabled by default.



Only the event logs from managed clusters are forwarded to Fluentd.

## What you'll need

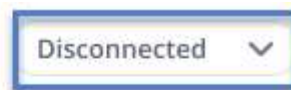
- An Astra Control Center account with **admin/owner** privileges.
- Astra Control Center installed and running on a Kubernetes cluster.



Astra Control Center does not validate the details you enter for your Fluentd server. Ensure that you enter the correct values.

## Steps

1. Log in to Astra Control Center using an account with **admin/owner** privilege.
2. Select **Account > Connections**.
3. Select **Connect** from the drop-down list where it shows **Disconnected** to add the connection.



### FLUENTD

Connect Astra Control logs to Fluentd for use by your log analysis software.

4. Enter the host IP address, the port number, and shared key for your Fluentd server.
5. Select **Connect**.

## Result

If the details you entered for your Fluentd server were saved, the **Fluentd** section of the **Account > Connections** page indicates that it is connected. Now you can visit the Fluentd server that you connected and view the event logs.

If the connection failed for some reason, the status shows **Failed**. You can find the reason for failure under **Notifications** at the top-right side of the UI.

You can also find the same information under **Account > Notifications**.



If you are having trouble with log collection, you should log in to your worker node and ensure that your logs are available in `/var/log/containers/`.

## Edit the Fluentd connection

You can edit the Fluentd connection to your Astra Control Center instance.

### Steps

1. Log in to Astra Control Center using an account with **admin/owner** privilege.
2. Select **Account > Connections**.
3. Select **Edit** from the drop-down list to edit the connection.
4. Change the Fluentd endpoint settings.
5. Select **Save**.

## Disable the Fluentd connection

You can disable the Fluentd connection to your Astra Control Center instance.

### Steps

1. Log in to Astra Control Center using an account with **admin/owner** privilege.
2. Select **Account > Connections**.
3. Select **Disconnect** from the drop-down list to disable the connection.
4. In the dialog box that opens, confirm the operation.

# Update an existing license

You can convert an evaluation license to a full license, or you can update an existing evaluation or full license with a new license. If you don't have a full license, work with your NetApp sales contact to obtain a full license and serial number. You can use the Astra UI or [the Astra API](#) to update an existing license.

### Steps

1. Log in to the NetApp Support Site.
2. Access the Astra Control Center Download page, enter the serial number, and download the full NetApp license file (NLF).

3. Log in to the Astra Control Center UI.
4. From the left navigation, select **Account > License**.
5. In the **Account > License** page, click the status drop-down menu for the existing license and select **Replace**.
6. Browse to the license file that you downloaded.
7. Select **Add**.

The **Account > Licenses** page displays the license information, expiration date, license serial number, account ID, and CPU units used.

## Unmanage apps and clusters

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

### Unmanage an app

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

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

#### Steps

1. From the left navigation bar, select **Apps**.
2. Select the checkbox for the apps that you no longer want to manage.
3. From the **Action** menu, select **Unmanage**.
4. Type "unmanage" to confirm.
5. Confirm that you want to unmanage the apps and then select **Yes, unmanage Application**.

#### Result

Astra Control Center stops managing the app.

### Unmanage a cluster

Unmanage the cluster that you no longer want to manage from Astra Control Center.

- This action stops your cluster from being managed by Astra Control Center. 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](#).



Before you unmanage the cluster, you should unmanage the apps associated with the cluster.

#### Steps

1. From the left navigation bar, select **Clusters**.
2. Select the checkbox for the cluster that you no longer want to manage in Astra Control Center.
3. From the **Actions** menu, select **Unmanage**.
4. Confirm that you want to unmanage the cluster and then select **Yes, unmanage cluster**.



## Result

The status of the cluster changes to **Removing** and after that the cluster will be removed from the **Clusters** page, and it is no longer managed by Astra Control Center.



**If Astra Control Center and Cloud Insights are not connected**, unmanaging the cluster removes all the resources that were installed for sending telemetry data. **If Astra Control Center and Cloud Insights are connected**, unmanaging the cluster deletes only the `fluentbit` and `event-exporter` pods.

## Uninstall Astra Control Center

You might need to remove Astra Control Center components if you are upgrading from a trial to a full version of the product. To remove Astra Control Center and the Astra Control Center Operator, run the commands described in this procedure in sequence.

### What you'll need

- Use Astra Control Center UI to unmanage all [clusters](#).

### Steps

1. Delete Astra Control Center. The following sample command is based upon a default installation. Modify the command if you made custom configurations.

```
kubectl delete -f astra_control_center_min.yaml -n netapp-acc
```

Result:

```
astracontrolcenter.astra.netapp.io "astra" deleted
```

2. Use the following command to delete the `netapp-acc` namespace:

```
kubectl delete ns netapp-acc
```

Result:

```
namespace "netapp-acc" deleted
```

3. Use the following command to delete Astra Control Center operator system components:

```
kubectl delete -f astra_control_center_operator_deploy.yaml
```

Result:

```
namespace "netapp-acc-operator" deleted
customresourcedefinition.apiextensions.k8s.io
"astracontrolcenters.astra.netapp.io" deleted
role.rbac.authorization.k8s.io "acc-operator-leader-election-role"
deleted
clusterrole.rbac.authorization.k8s.io "acc-operator-manager-role"
deleted
clusterrole.rbac.authorization.k8s.io "acc-operator-metrics-reader"
deleted
clusterrole.rbac.authorization.k8s.io "acc-operator-proxy-role" deleted
rolebinding.rbac.authorization.k8s.io "acc-operator-leader-election-
rolebinding" deleted
clusterrolebinding.rbac.authorization.k8s.io "acc-operator-manager-
rolebinding" deleted
clusterrolebinding.rbac.authorization.k8s.io "acc-operator-proxy-
rolebinding" deleted
configmap "acc-operator-manager-config" deleted
service "acc-operator-controller-manager-metrics-service" deleted
deployment.apps "acc-operator-controller-manager" deleted
```

## Find more information

- [Known issues for uninstall](#)

## Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## 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.