Use Astra Control Service

Astra

NetApp
August 10, 2021

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

Table of Contents

Use Astra Control Service . . . 1
- Log in to Astra Control Service . . . 1
- Manage and protect apps . . . 1
- View app and compute health . . . 14
- Manage buckets . . . 18
- Manage your account . . . 21
- Unmanage apps and compute . . . 29

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

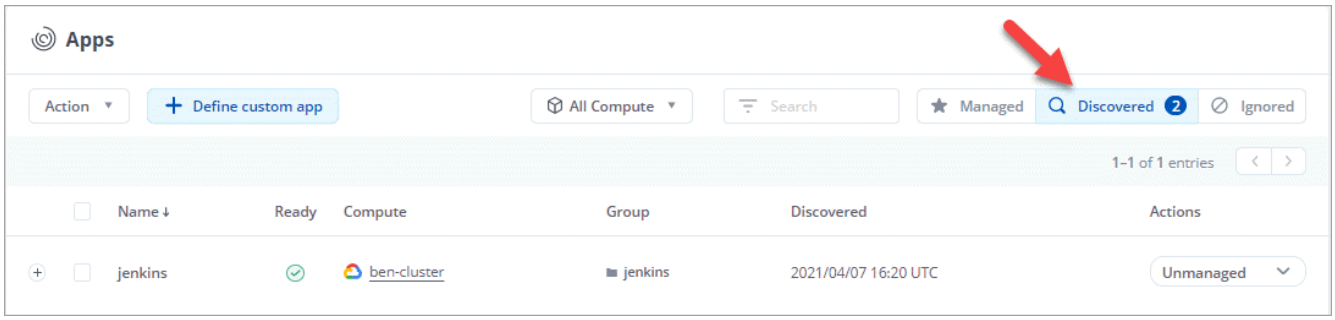
The **Discovered** section of the Apps page shows namespaces and the Helm-installed apps or custom-labeled apps in those namespaces. You can choose to manage each app individually or at the namespace level. It all comes down to the level of granularity that you need for data protection operations.

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

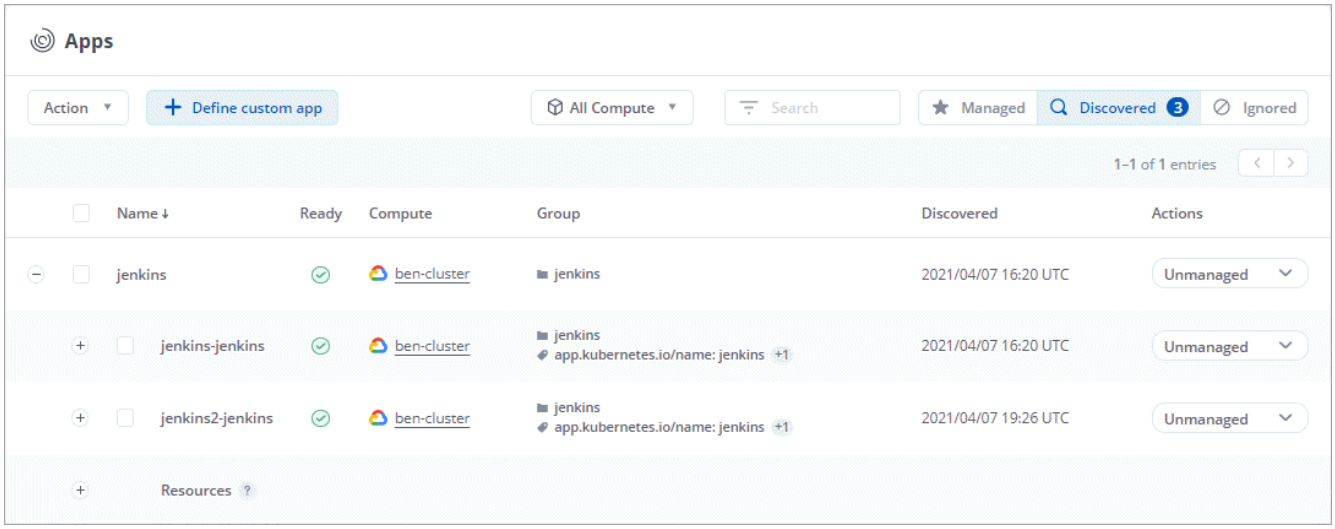
1. Click **Apps** and then click **Discovered**.



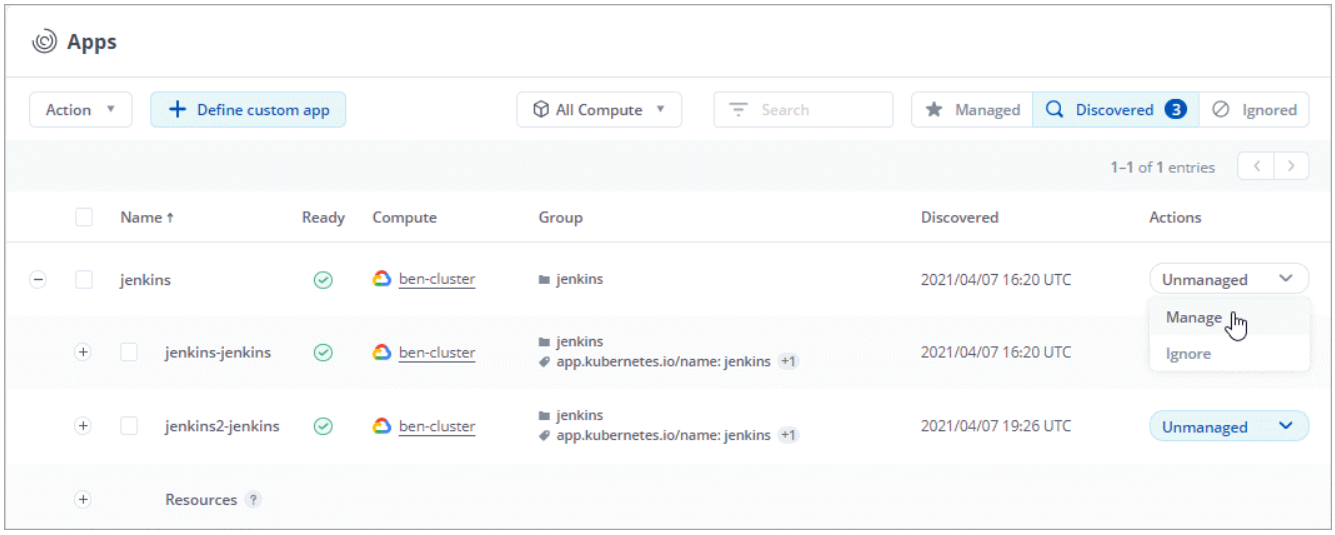
2. View the list of discovered namespaces and expand a namespace to view the apps and associated resources.

   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:

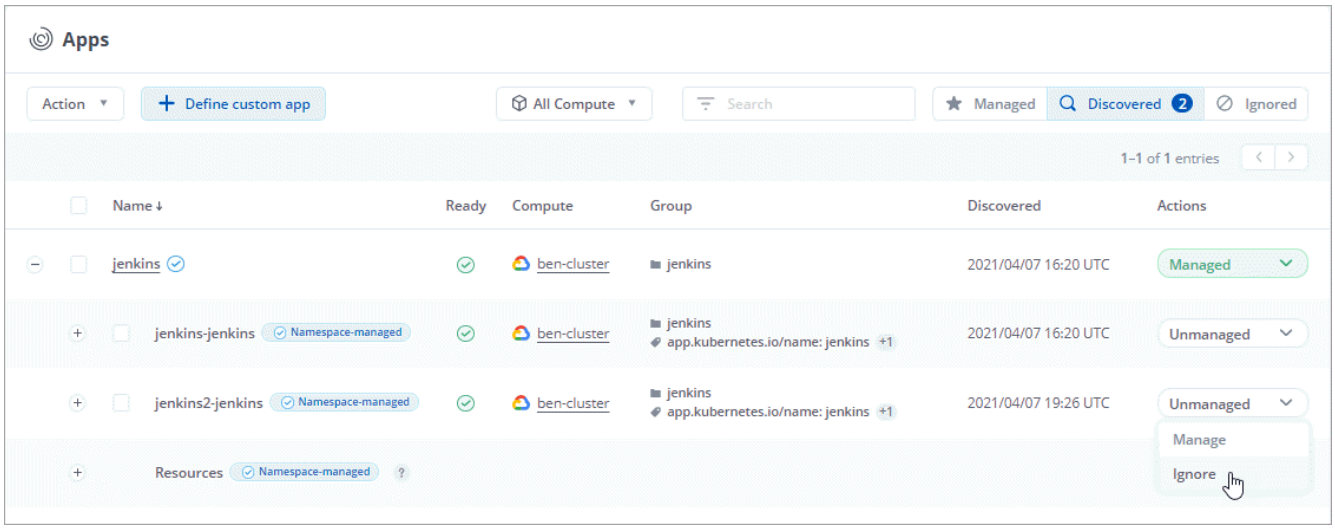


3. Decide whether you want to manage each app individually or at the namespace level.
4. At the desired level in the hierarchy, click the drop-down list in the **Actions** column and click **Manage**.



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.

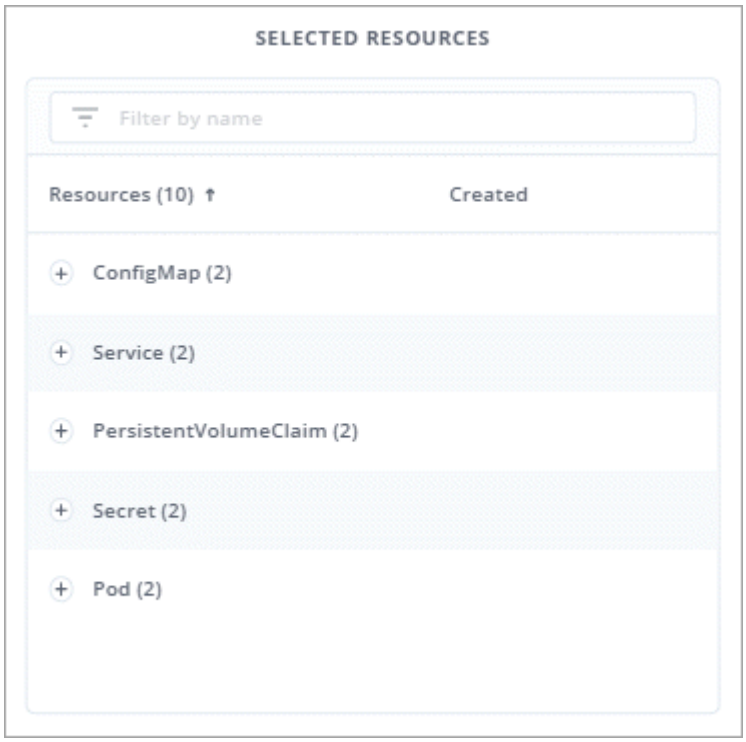
Manage apps by Kubernetes label

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.

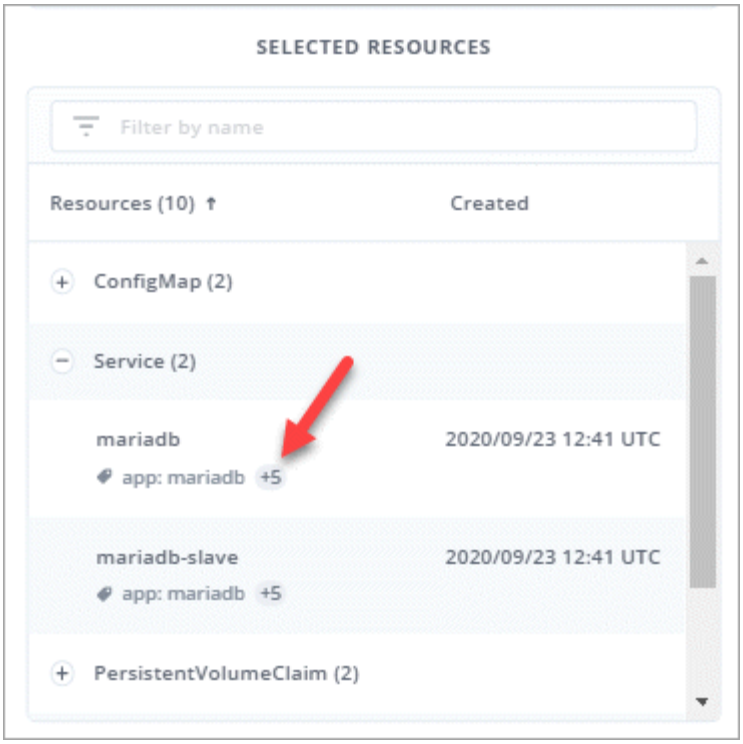
Steps

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).

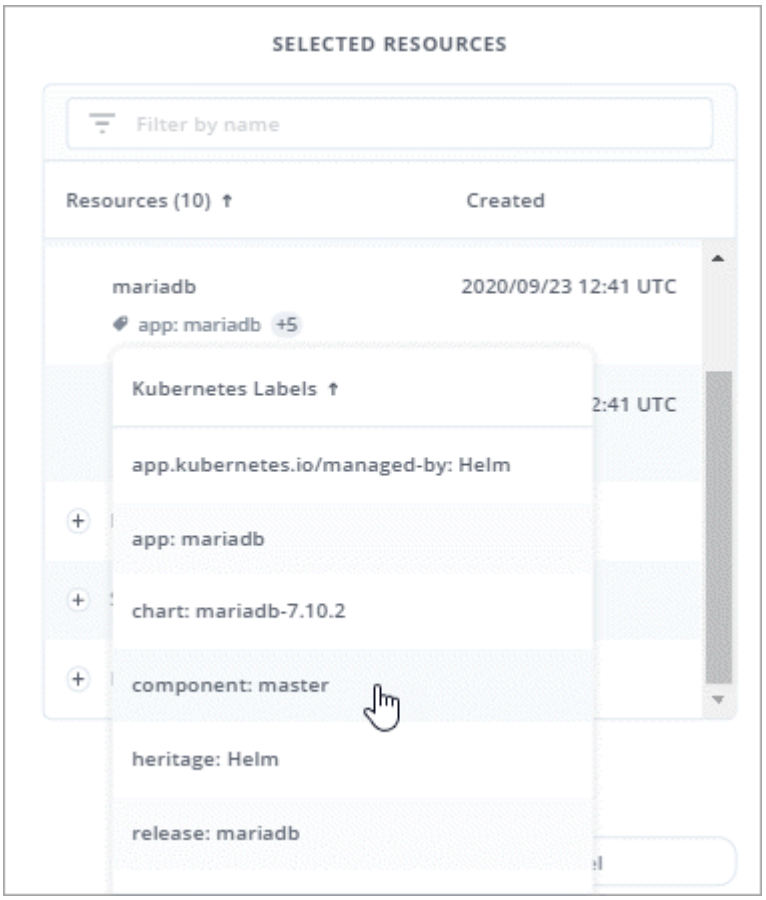
      Here's an example:



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

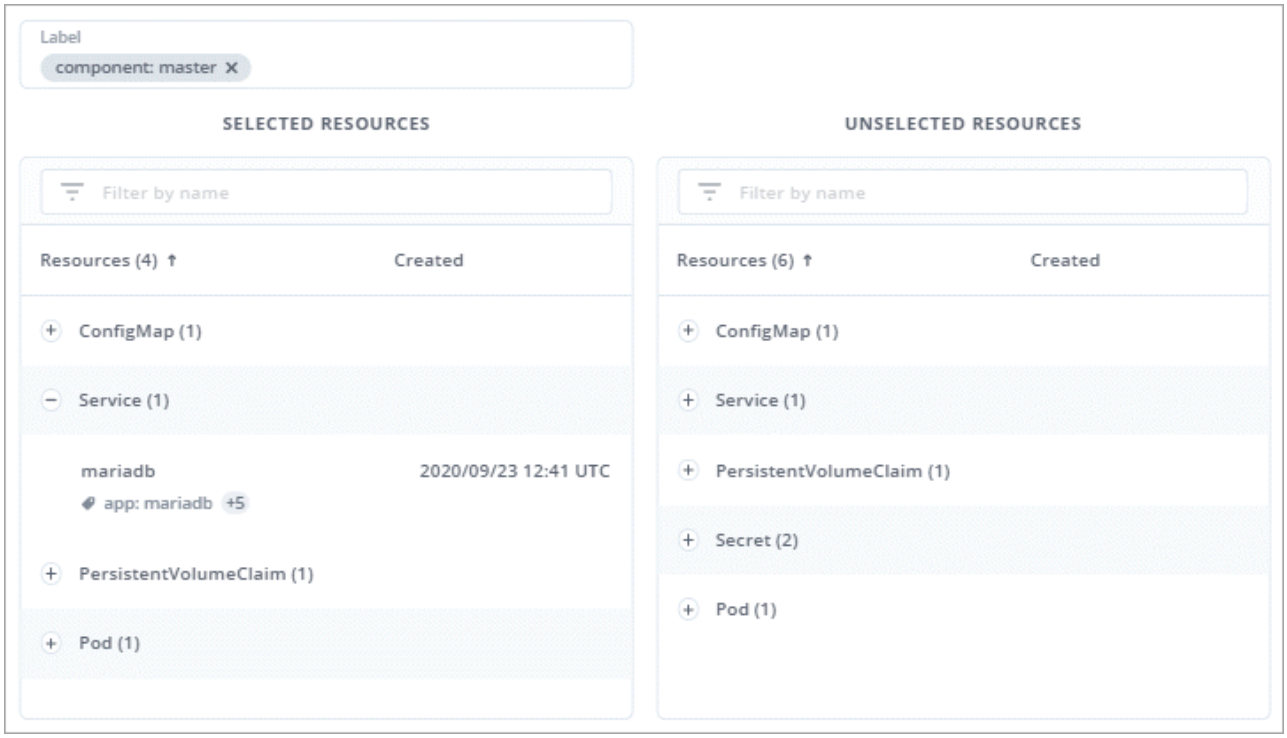


- Select one of the labels.



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.



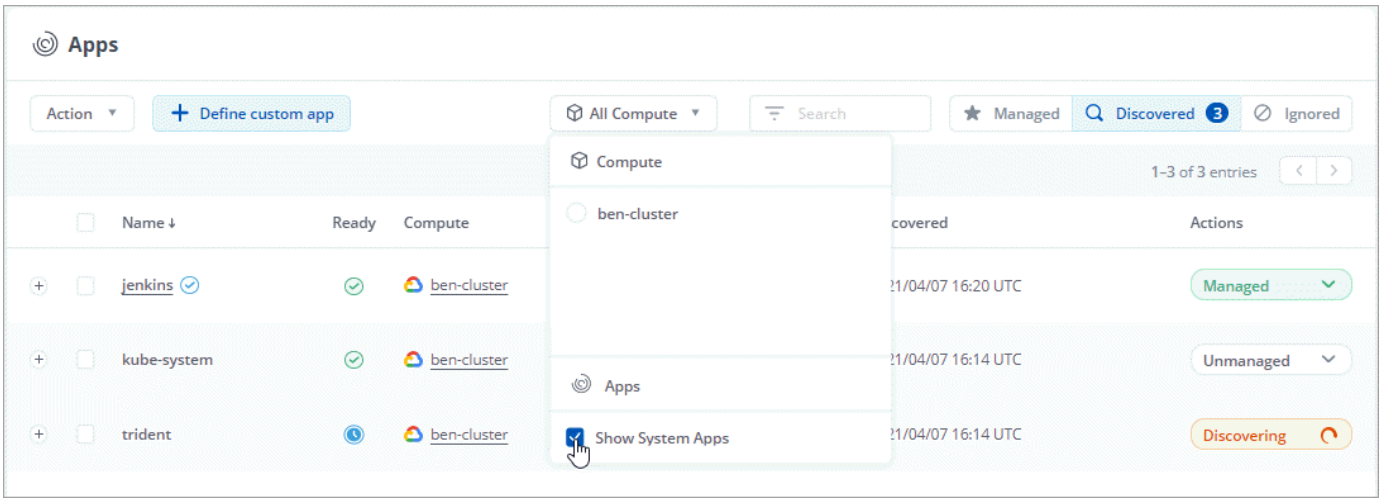
3. Click **Define Custom App**.

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.

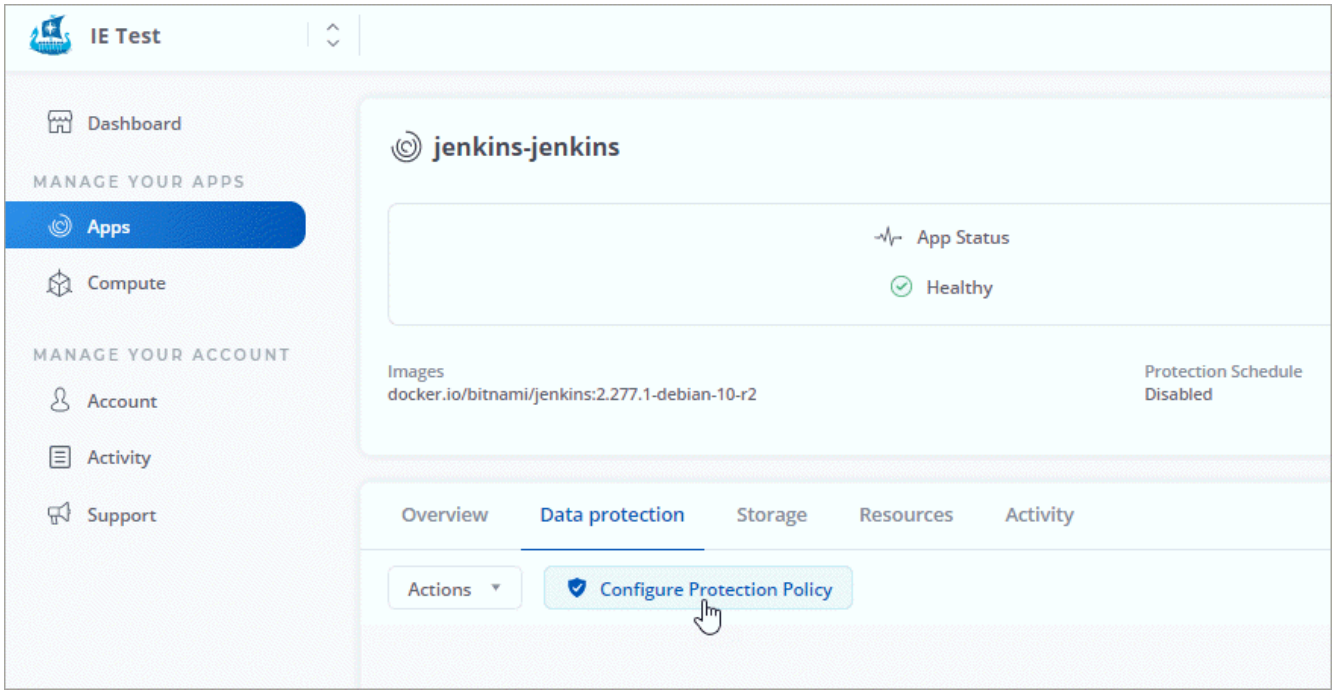
> *You can't be fully protected until you have a recent backup*. This is important because backups are stored in an object store away from the persistent volumes. If a failure or accident wipes out the cluster and it's persistent storage, then you need a backup to recover. A snapshot wouldn't enable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

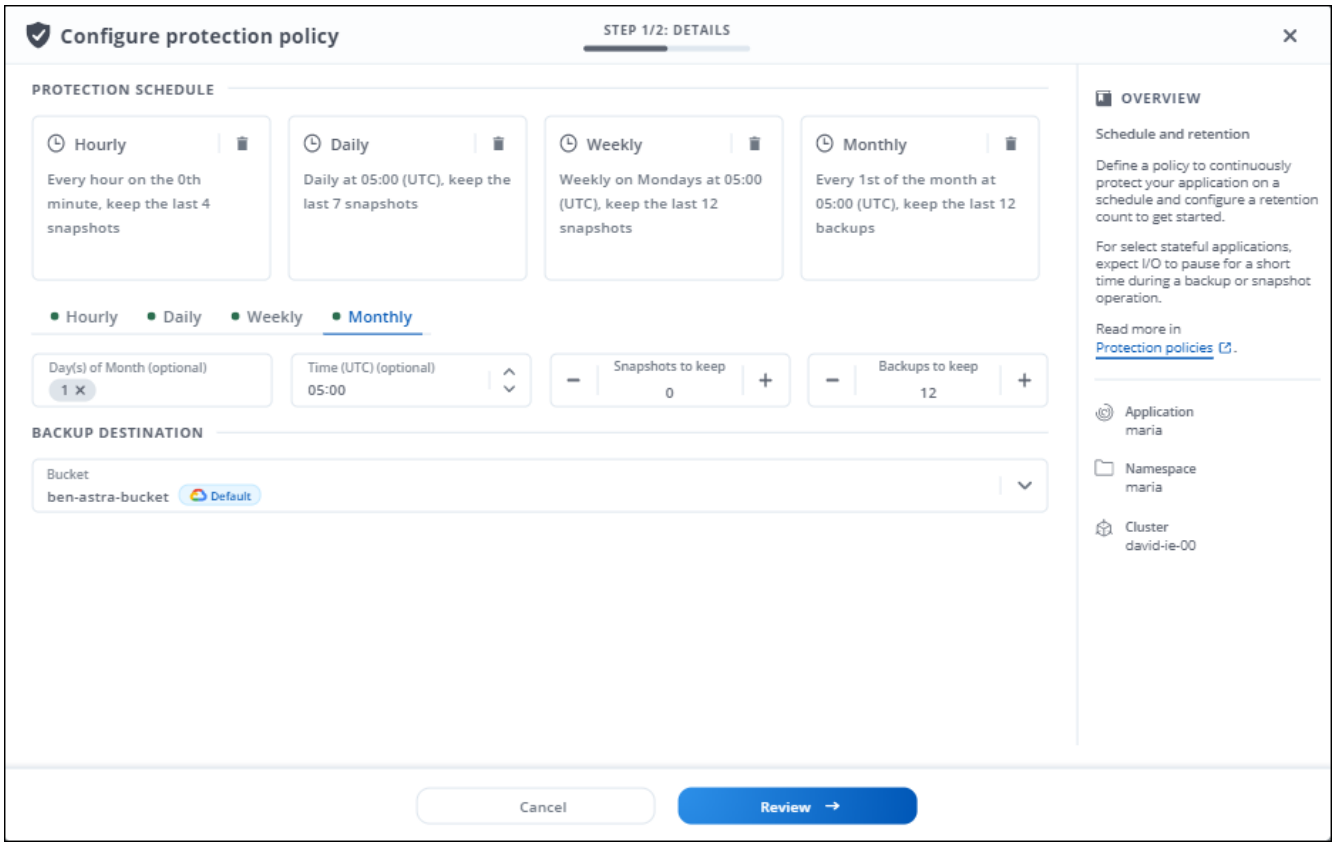


4. Define a protection schedule by choosing the number of snapshots and backups to keep for the hourly, daily, weekly, and monthly schedules.

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.

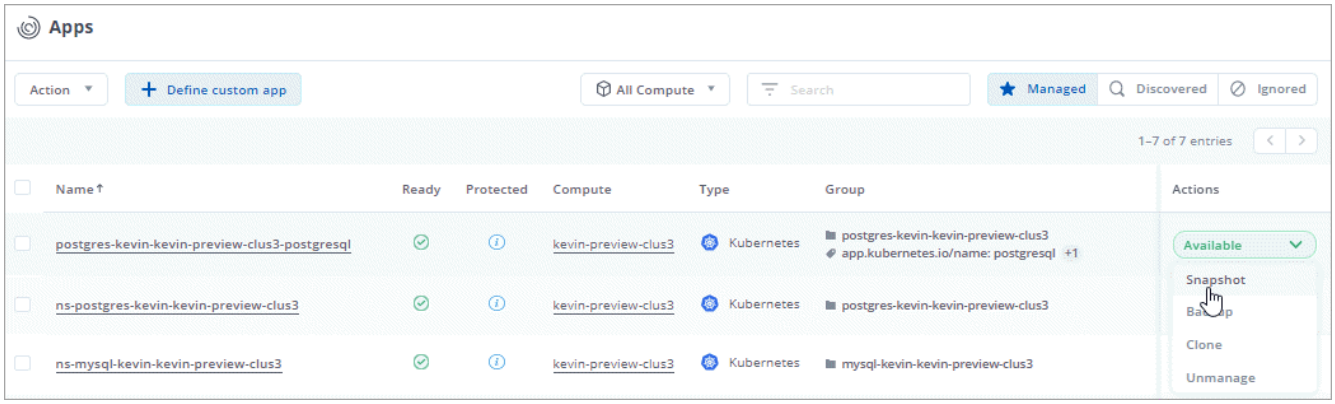
Create a snapshot

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

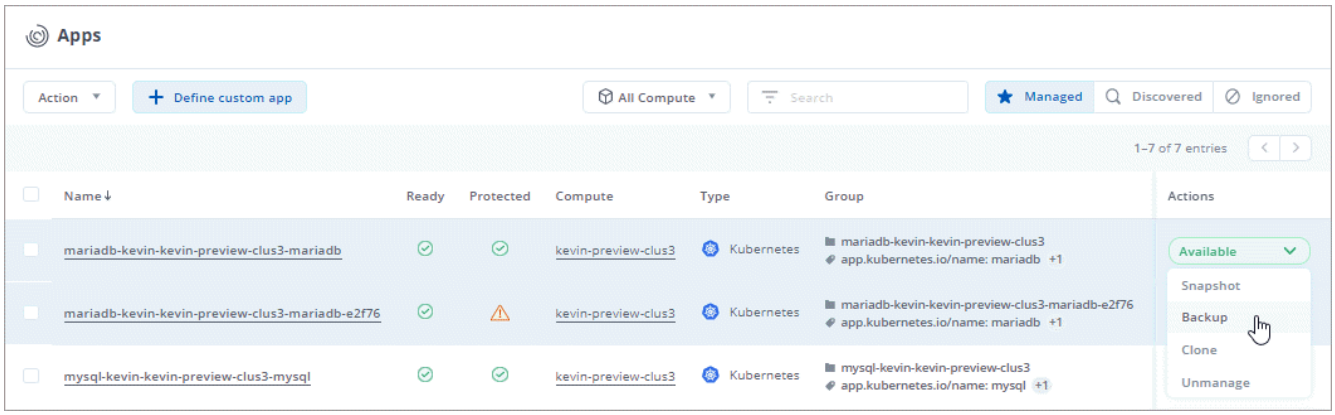
Astra Control creates a snapshot of the apps.

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.

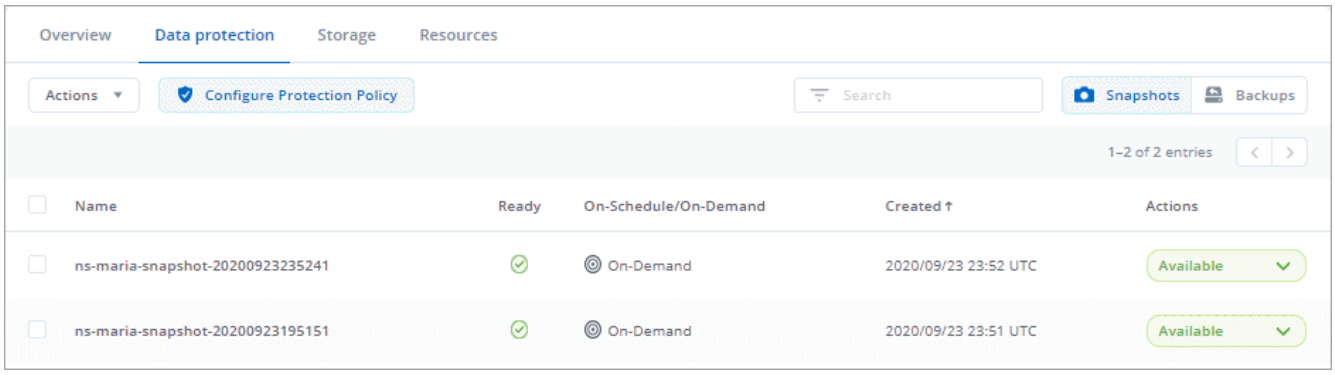
View snapshots and backups

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.



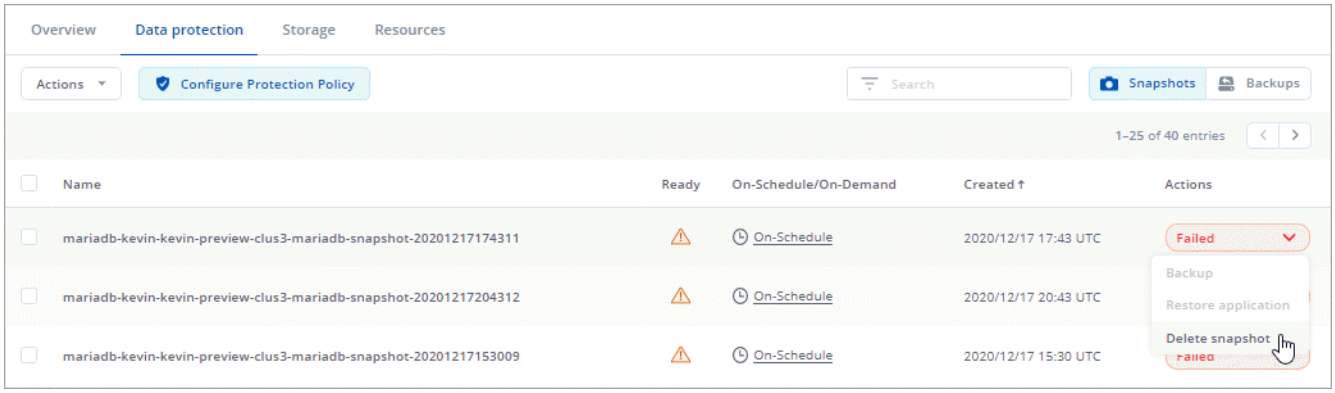
3. Click **Backups** to see the list of backups.

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**.

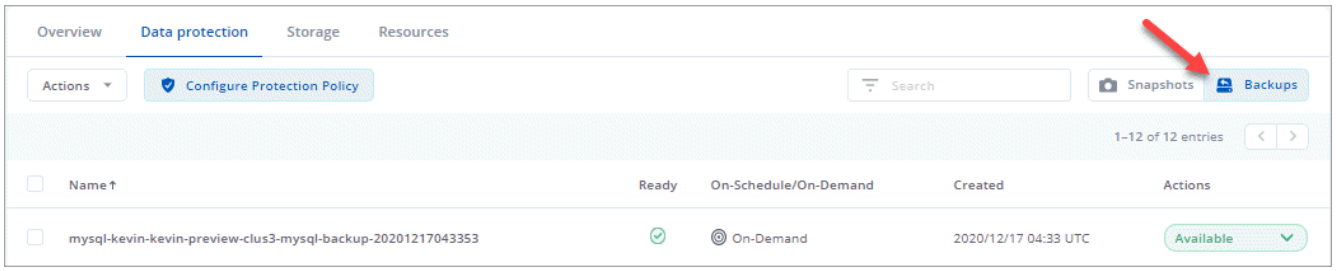
Result

Astra Control deletes the snapshot.

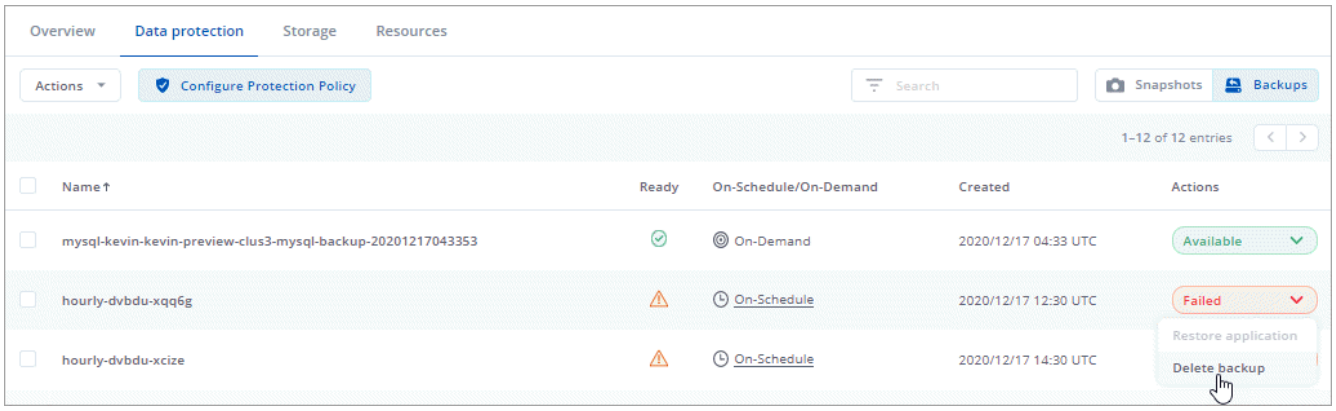
Delete backups

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

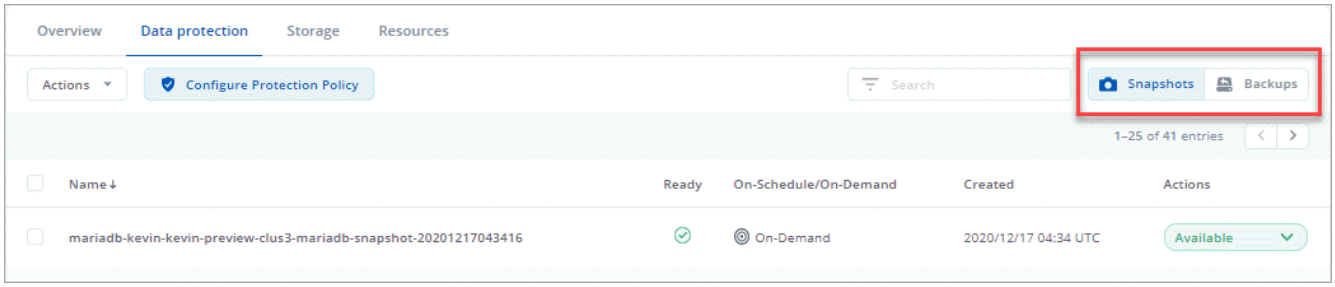
Astra Control deletes the backup.

Restore apps

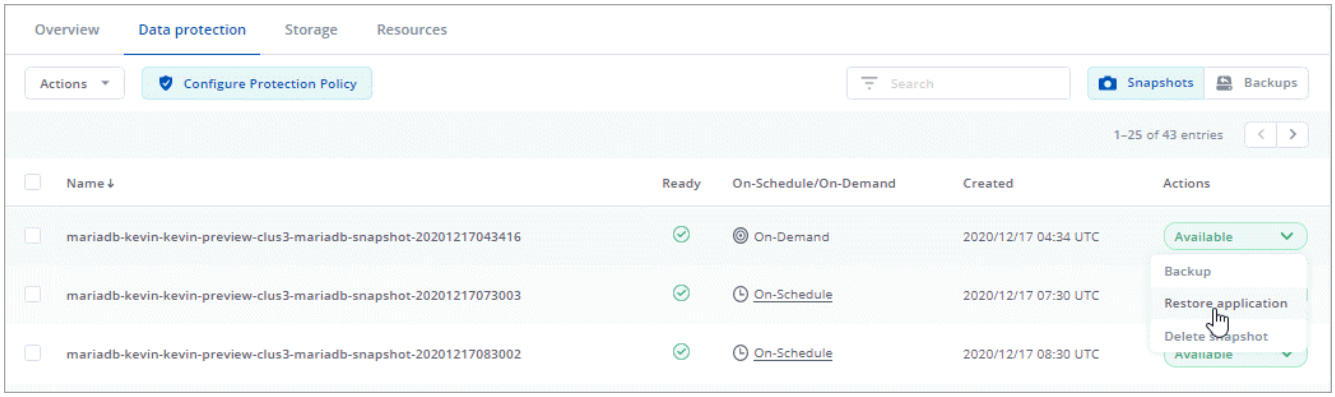
Astra Control can restore your application configuration and persistent storage from a snapshot or backup. Persistent storage backups are transferred from your object store, so restoring from an existing backup will complete the fastest.

Steps

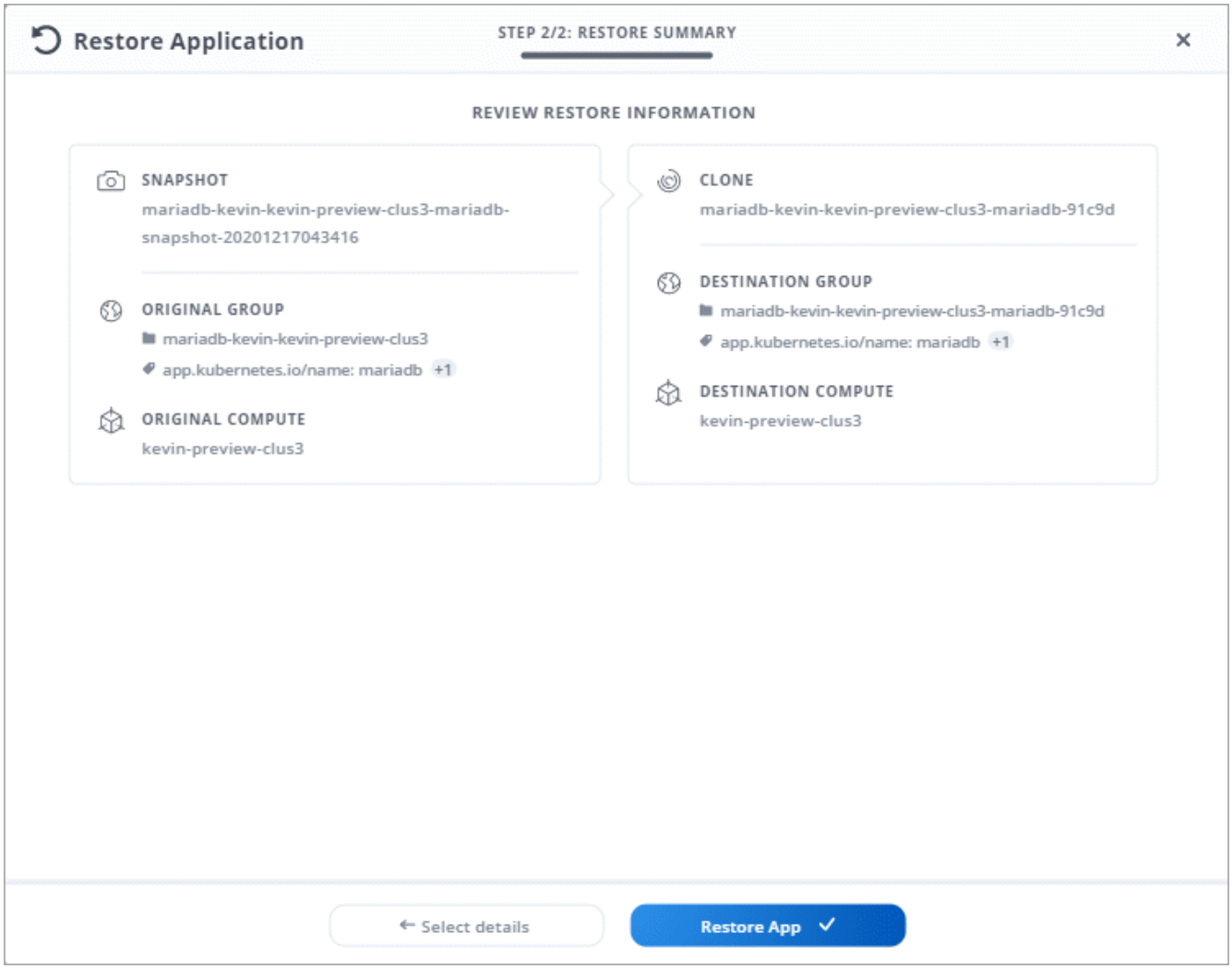
1. Click **Apps** and then click the name of a managed app.
2. Click **Data protection**.
3. If you want to restore from a snapshot, keep **Snapshots** selected. Otherwise, click **Backups** to restore from a backup.



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.

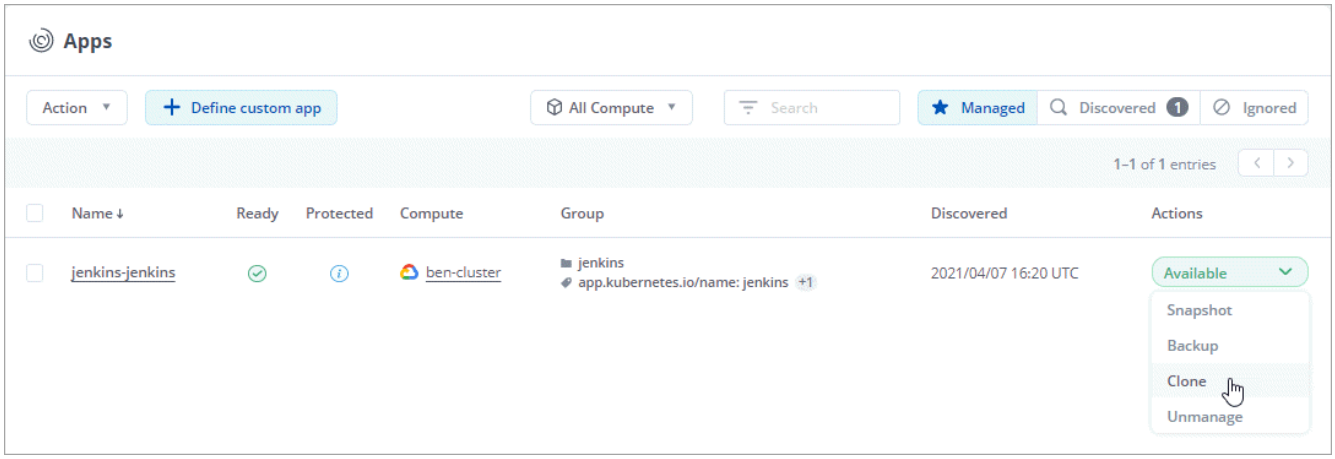
Clone and migrate apps

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**.

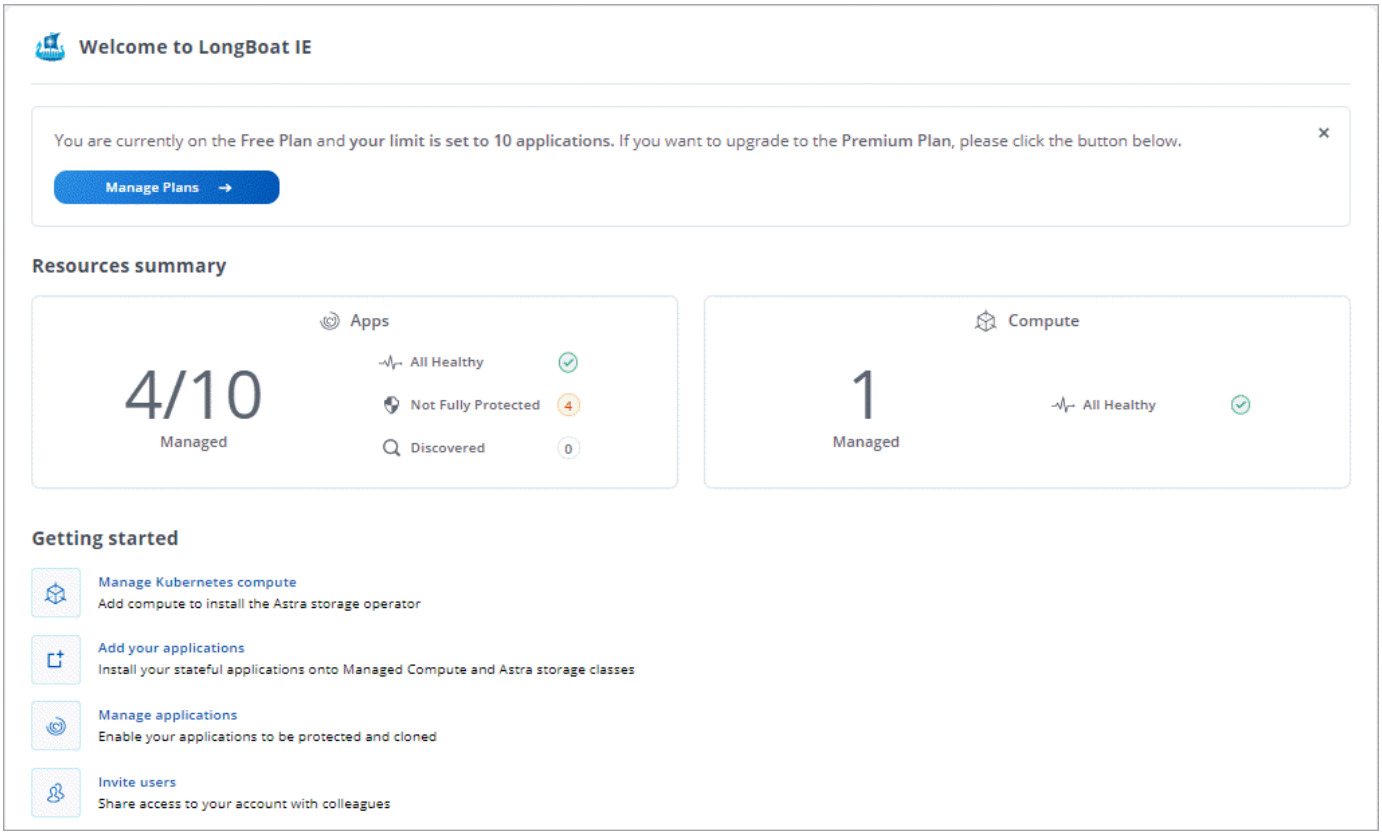
Result

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.

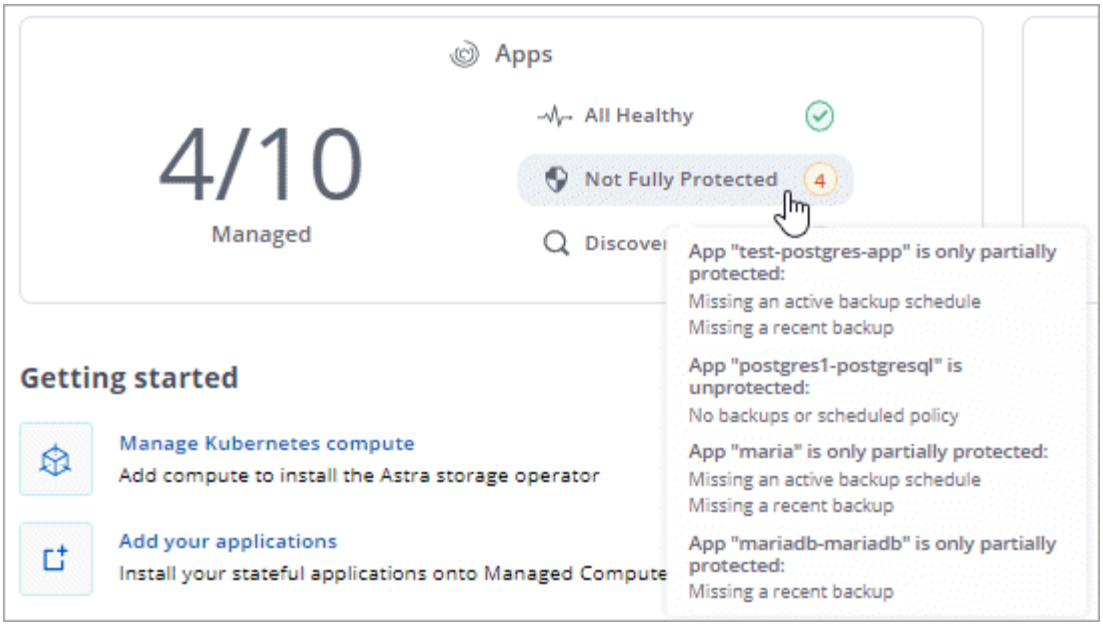


The Apps tile helps you identify the following:

- 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.



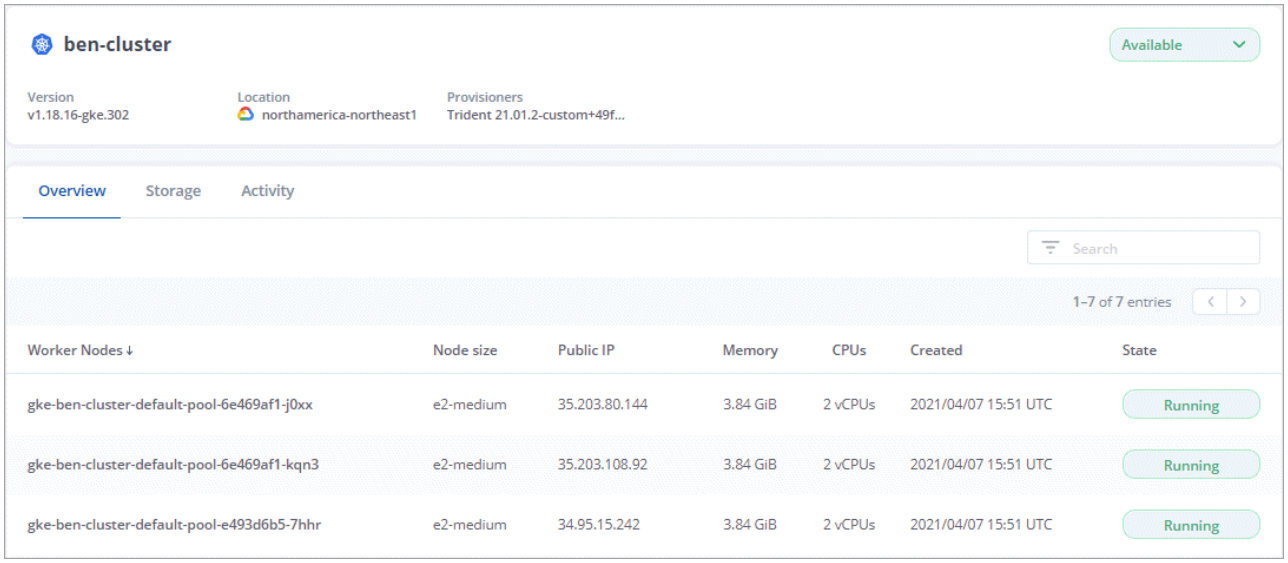
The Compute tile provides similar details about the health of the compute and you can drill down to get more details just like you can with an app.

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.

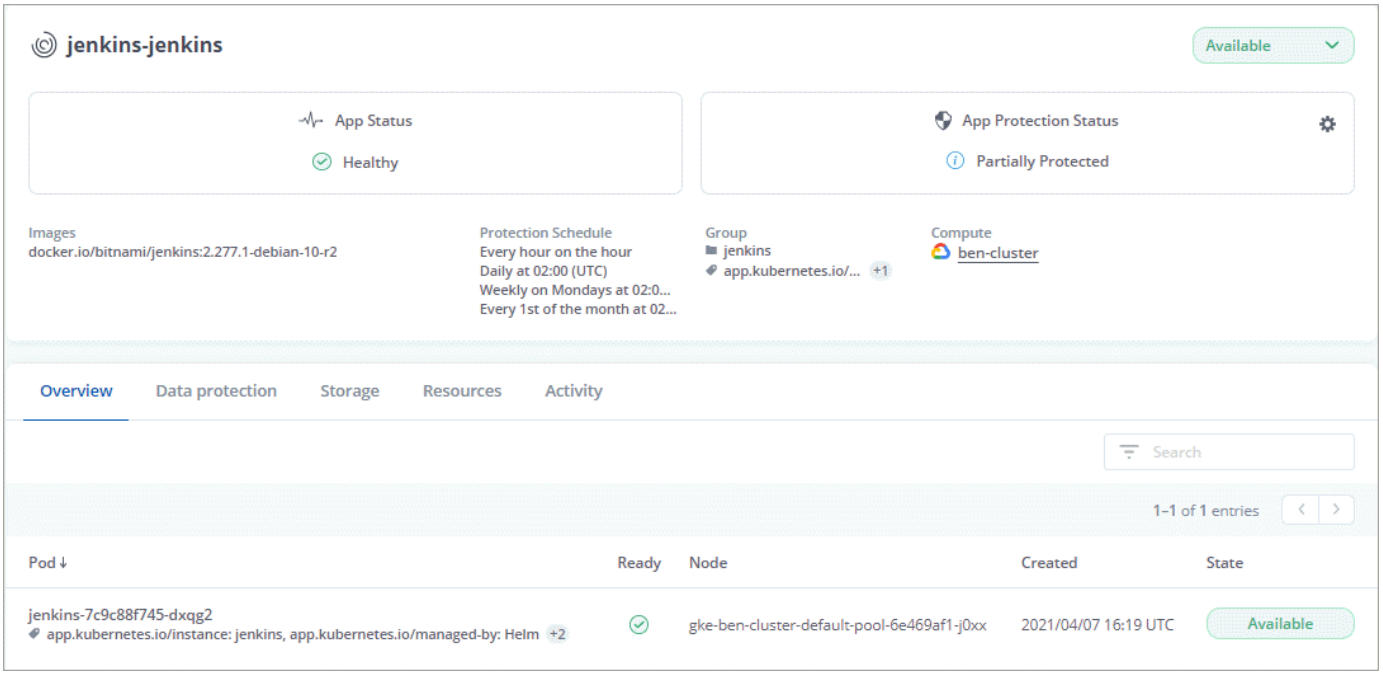
Steps

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.

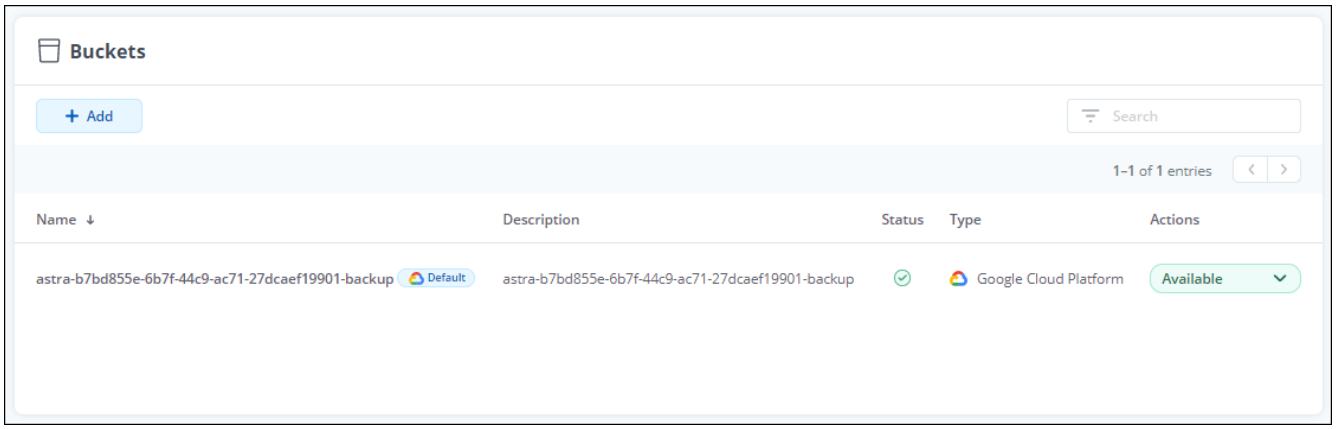
If a bucket is in the Removed state, you can still set it as the default bucket and assign it to a protection schedule. But if the bucket isn't in the Available state by the time a data protection operation starts, then that operation will fail.

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*.

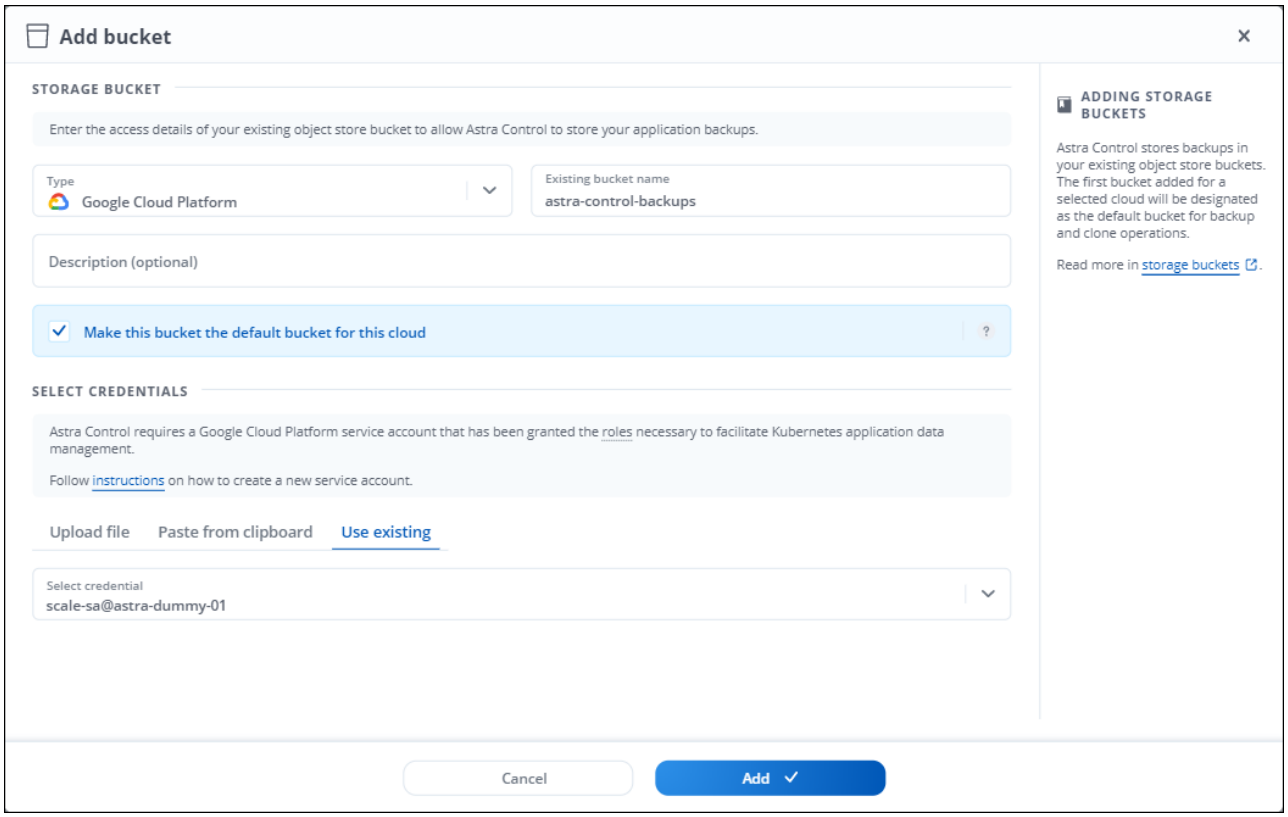
Steps

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:

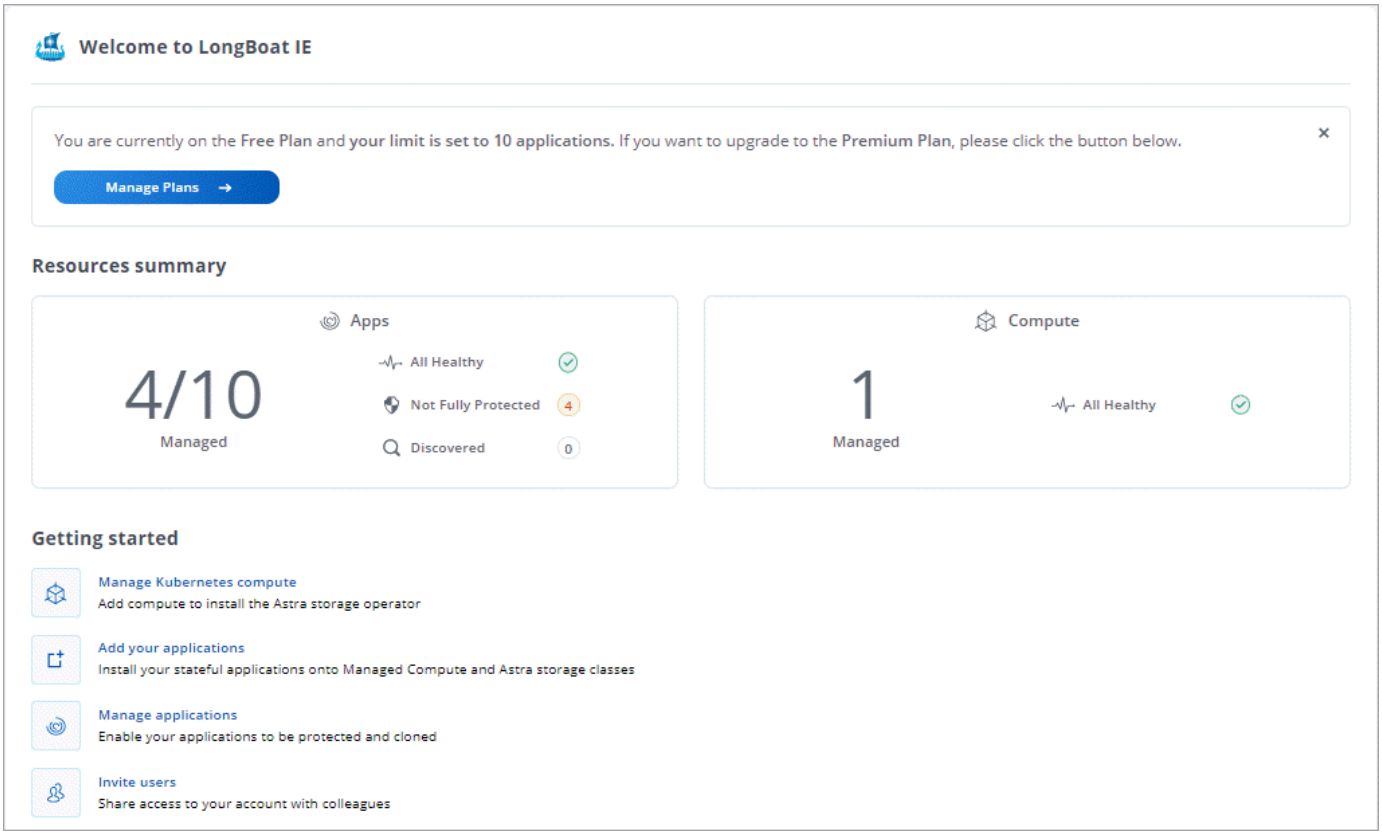
Free Plan
: Manage up to 10 apps for free.

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

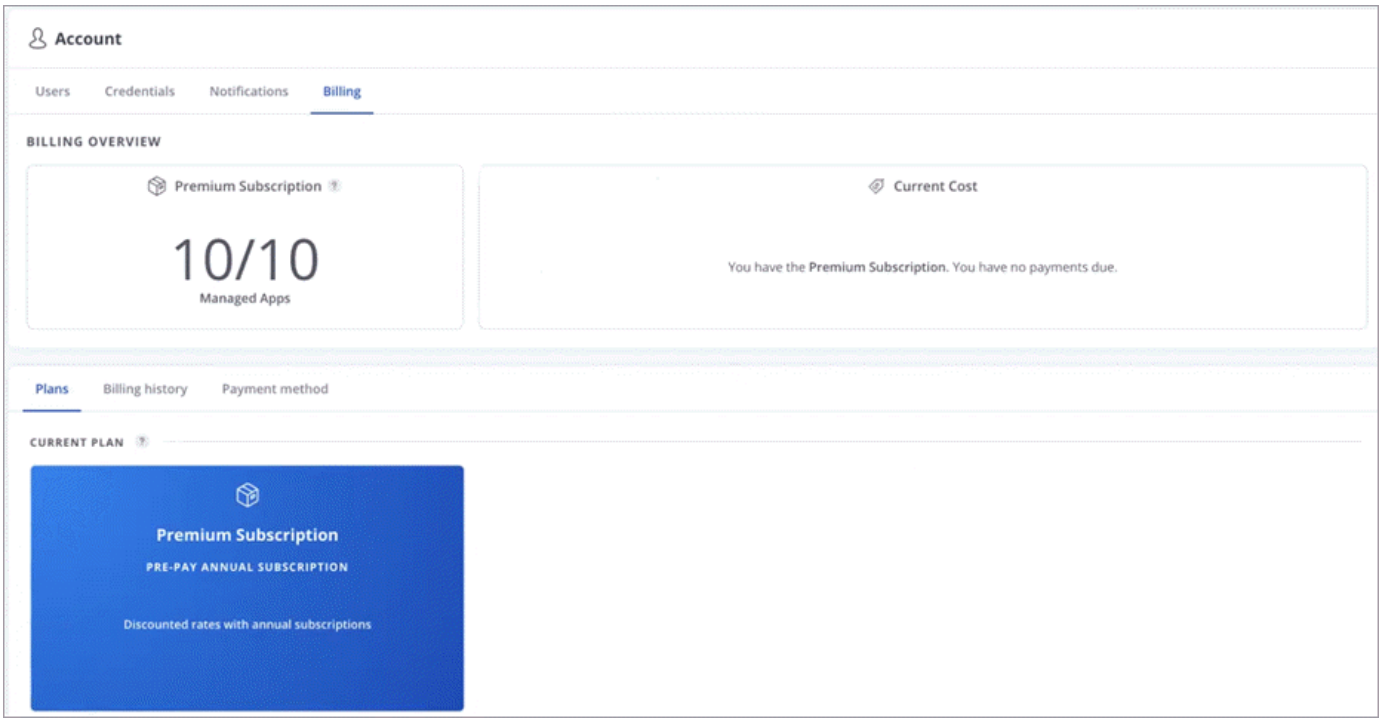
Contact NetApp Sales to pre-pay at a discounted rate with an annual subscription.

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.

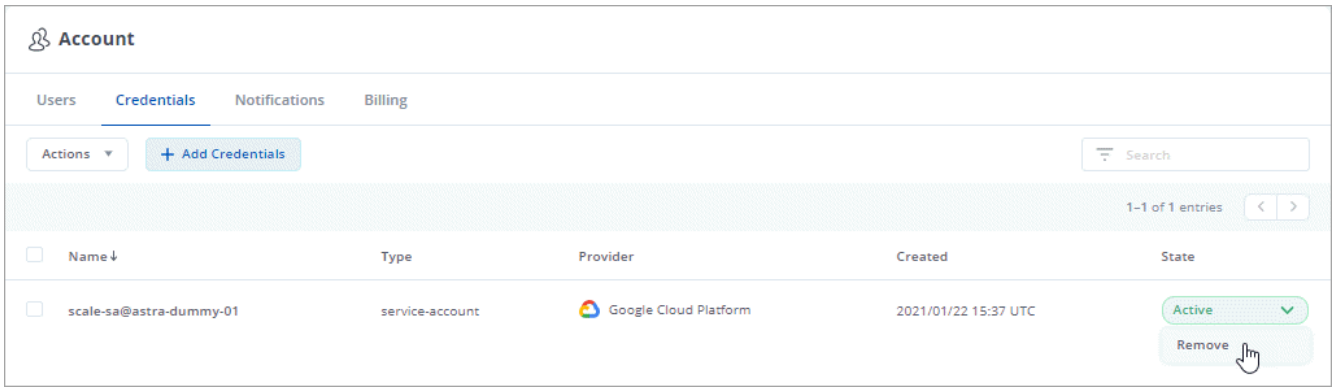
Remove credentials

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**.

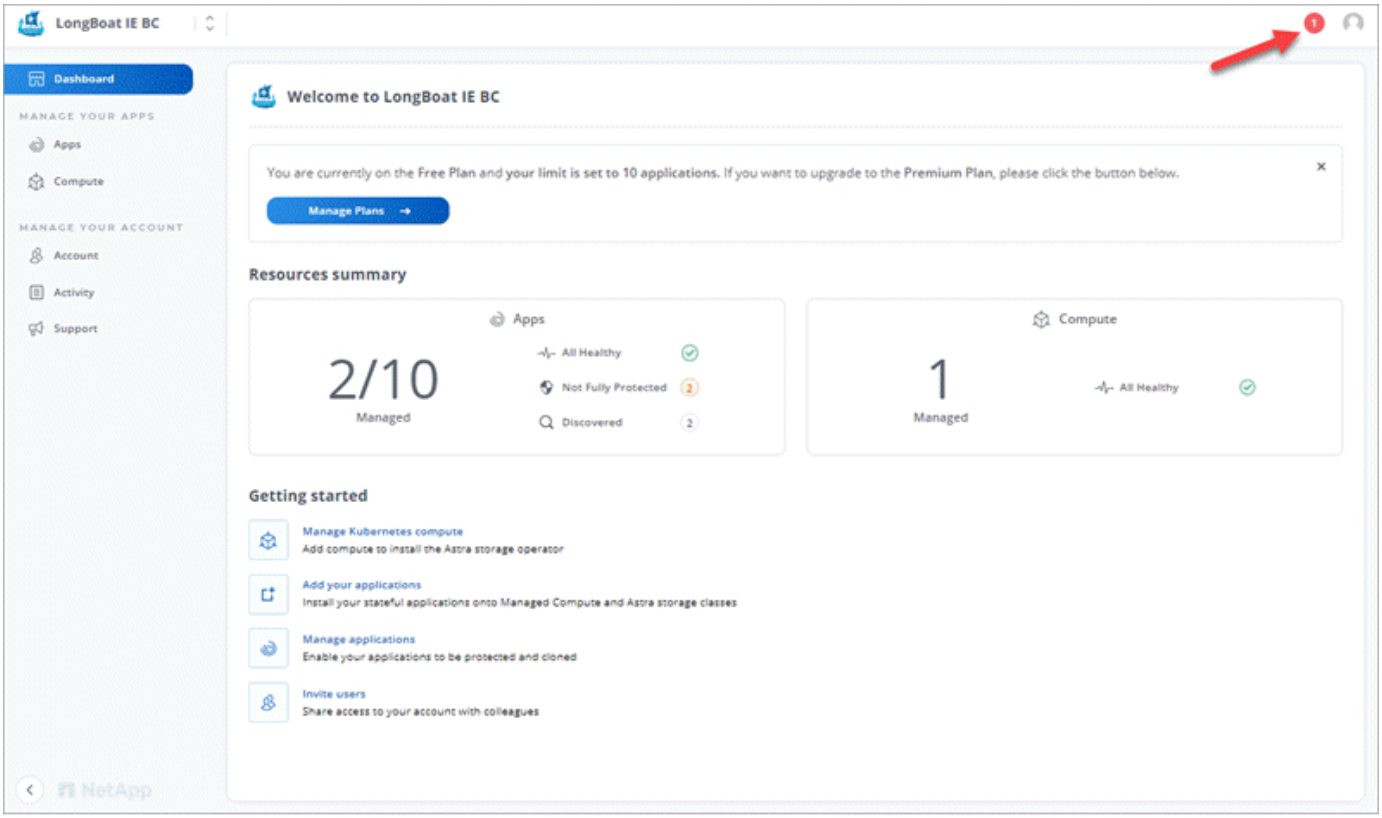
Steps to view account activity for compute

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.

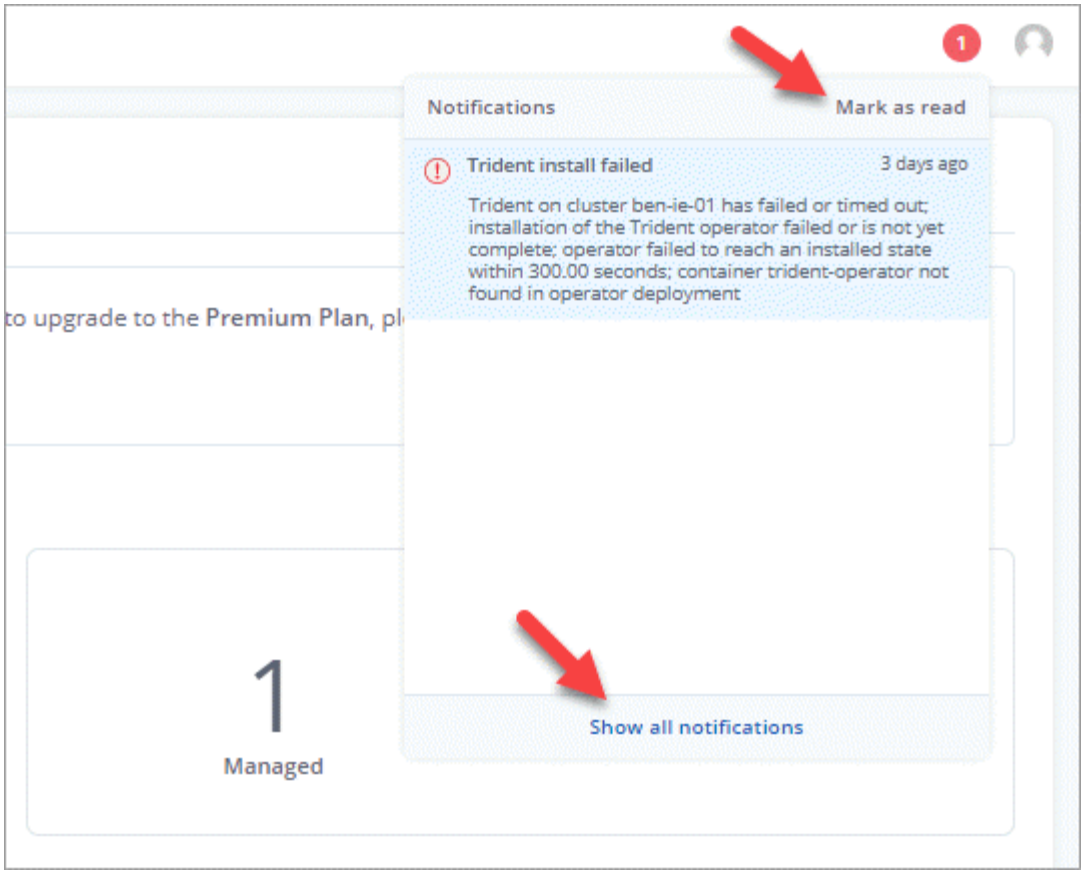
The number of unread notifications is available in the top right of the interface:



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.

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.