Use Project Astra

Project Astra

NetApp
October 18, 2020

Table of Contents

Use Project Astra

Manage and protect apps

Start managing apps

After you add a Kubernetes cluster to the Project Astra beta program, go to the Apps page to start managing the apps that run on the cluster.

Start managing an app

View the apps that you can discover from the **Discovered** section of the Apps page and then click **Manage**.

Steps

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

   If you just added the cluster to Project Astra, you'll notice that some apps are in the process of being discovered.

   [screenshot app discovery]

   If there are any issues with discovery, you can hover over the icon in the Ready column to view details about the issue.

   In the following image, you can see that Project Astra is still in the process of discovering the app. Hovering over the Ready column shows the current status.

   [screenshot app discovery status]

   After Project Astra discovers an app, you have the option to either manage the app or ignore it.

2. Look at the **Group** column to see which namespace the application is running in (it's designated with the folder icon) and whether any Kubernetes labels are available (those are designated with a tag icon).

   Here's an example:

   [screenshot group]

   This information can be helpful because you might want to manage everything in the namespace, or you might want to manage the app using labels that you've already set up. You'll see how to use these labels in a few steps.

3. Click the drop-down list in the **Actions** column for the desired app and click **Manage**.

[screenshot app manage]

4. In the **Manage Application** dialog box, provide the required information to manage the app:
   a. **New App**: Customize the name of the app.
   b. **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:

      [screenshot selected resources]

      There are two primary ways to use the Selected Resources field:

      - View the resources to validate that the Kubernetes resources that you want to protect are listed.
      - If a namespace contains multiple discrete applications and you use Kubernetes labels to split apart the apps, then you can choose a label to register the app with, based on that label.
        - View the available labels by expanding a resource and clicking the number of labels.

          [screenshot view labels]

        - Select one of the labels.

          [screenshot select label]

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

        - View **Unselected Resources** to verify the app resources that you don't want to protect.

          [screenshot selected label]

5. Click **Manage App**.

The following video shows how to start managing an app.

▶ https://docs.netapp.com/us-en/project-astra/use/media/video-manage-app.mp4 *(video)*

Result

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

[screenshot app managed]

What's next?

Repeat these steps for additional apps. Choose **Ignore** for any of the apps that you don't want to manage from Project Astra. Those apps will move to the **Ignored** tab. Ideally, you'd have zero clusters listed in the Discovered tab after you're done.

Manage an app using a custom label

Project Astra includes an action at the top of the Apps page named **Manage new app**. You can use this action to manage an app by using a *custom* label. For example, you might not want to use one of the discovered Helm labels to manage the app.

Steps

1. Click **Apps** > **Manage new app**.
2. In the **Manage Application** dialog box, provide the required information to manage the app:
    a. **New App**: Customize the 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 custom label.
    e. **Selected Resources:** View and manage the Kubernetes resources that you'd like to protect.
    f. **Unselected Resources**: Verify the app resources that you don't want to protect.
3. Click **Manage App**.

Result

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

What about system apps?

When you add a Kubernetes cluster, Project Astra also discovers the system apps running on the cluster. You can view them by filtering the Apps list.

[screenshot system apps]

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. A backup can be slower to take compared to the local snapshots. However, they can be accessed across regions in the cloud. Backups are used for migrating applications across cloud regions. Also, you can choose to have a longer retention period for backups.

Configure a protection policy

Configure a protection policy to protect an app by creating snapshots, backups, or both at a defined schedule and with a specified 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**.

   [A screenshot of the Data protection tab for an app which enables you to configure a 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 a schedule to take snapshots daily and weekly, while retaining the last 14 hourly snapshots and the last 26 weekly snapshots. It also takes monthly backups and retains the last 12 copies. Because 0 copies were selected for hourly, no hourly snapshots or backups are taken.

   [A screenshot of a sample configuration policy where you can choose to take snapshots and backups on an hourly, daily, weekly, or monthly basis.]

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

Result

Project Astra 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**.

   [A screenshot of the app page where you can click the drop-down list in the actions column and select Snapshot.]

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

Result

Project Astra 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**.

   [A screenshot of the app page where you can click the drop-down list in the actions column and select 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

Project Astra 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 an app.
2. Click **Data Protection**.

   The snapshots display by default.

   [A screenshot of the data protection tab for an app where you can view the list of the current snapshots and backups.]

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**.

   [A screenshot of the Data protection tab for an app where you can delete a snapshot.]

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

Result

Project Astra 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 an app.
2. Click **Data Protection**.
3. Click **Backups**.

   [A screenshot of the Backups option that's available in the far right of the data protection tab.]

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

   [A screenshot of the Data protection tab for an app where you can delete a snapshot.]

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

Result

Project Astra deletes the backup.

Restore apps

You can restore an app by creating a clone from a point-in-time snapshot or from a backup.

Steps

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

   [A screenshot of the app page where you can click the drop-down list in the actions column and

select Clone.]

4. **Clone details**: Specify details for the clone:
   - Enter a name.
   - Choose whether to restore the app to the same cluster or to a different cluster.
   - Choose to create the clone from an existing snapshot or backup.
5. **Source**: Choose the snapshot or backup that you'd like to use.

   [screenshot clone source]

6. **Clone Summary**: Review the details about the clone and click **Clone App**.

   [screenshot clone summary]

Result

Project Astra 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 Project Astra 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**.

   [A screenshot of the app page where you can click the drop-down list in the actions column and select Clone.]

4. **Clone details**: Specify details for the clone:
   - Enter a name.
   - 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, Project Astra 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.

[screenshot clone source]

6. **Clone Summary**: Review the details about the clone and click **Clone App**.

   [screenshot clone summary]

Result

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

View app and cluster health

View a summary of app and cluster health

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

[screenshot dashboard]

The Apps tile helps you identify the following:

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

Note that these aren't just numbers or statuses—you can drill down from each of these. For example, if you have an unhealthy app, you can hover over the icon to identify which app has an issue and what the issue is. You can then go to the cluster to correct the issue.

[screenshot dashboard healthy]

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

View the health and details of a cluster

After you add a cluster to the Project Astra beta program, you can view details about the cluster, such as its location, the worker nodes, persistent volumes, and

storage classes.

Steps

1. Click **Compute**.
2. Click the name of a cluster.
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 cluster, including the storage class and state.

     [A screenshot of the Overview tab for a cluster.]

View the health and details of an app

After you start managing an app, Project 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.

[screenshot app overview]

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. Project 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. An app is either Fully Protected (it has a recent backup), Partially Protected (it has a data protection schedule or active snapshots, but no recently successful backup), or it's Unprotected.

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.

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.

Manage your account

Invite and remove users

Invite users to join your Project Astra beta program account and remove users that should no longer have access to your account.

Invite users

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

Steps

1. Click **Account**.
2. In the **Users** tab, click + **Invite users**.
3. 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 clusters.
     - A **Viewer** can view resources.

     [A screenshot of the Invite Users screen where you enter a name]
4. Click **Send invite/s**.

Result

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

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

Project Astra removes the user from the account.

Add and remove credentials

Add and remove cloud provider credentials from your account at any time. The Project Astra beta program uses these credentials to discover clusters, apps on a cluster, and to provision resources on your behalf.

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

Add credentials

The most common way to add credentials to Project Astra is when you add a cluster, but you can also add credentials from the Account page. The credentials will then be available to choose when you add your next Kubernetes cluster.

What you'll need

You should have the service account key file for a service account that has the required permissions. Learn more.

Steps

1. Click **Account** > **Credentials**.
2. Click **Add Credentials**.
3. Enter a name for the credentials that distinguishes them from other credentials in Project Astra.
4. Provide the Google Cloud service account key file either by uploading the file or by pasting the contents from your clipboard.
5. Click **Add credentials**.

Result

The credentials are now available to select when you add a Kubernetes cluster to Project Astra.

Remove credentials

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

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**.

   [A screenshot of the Credentials tab in the Account page where you can click the state column and select the Remove action.]

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

Result

Project Astra removes the credentials from the account.

View and manage notifications

Project 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:

[A screenshot that shows the Project Astra interface where you can view the number of unread notifications.]

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.

   [A screenshot that shows the expanded notifications in the Project Astra interface.]

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**.

Unmanage apps and clusters

Remove any apps or clusters that you no longer want to manage from the Project Astra beta program.

Stop managing an app

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

About this task

- This action stops your app from being managed by Project Astra. It doesn't remove the app from your cluster.
- Existing backups and snapshots aren't deleted, but data management operations aren't available from Project Astra.
- If you remove an app from your cluster, Project Astra will identify that it was removed, but the app remains in a managed state. That means you can still clone the app from a backup until you explicitly unmanage the app.

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

Steps

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

Result

Project Astra stops managing the app.

Stop managing clusters

Stop managing the clusters that you no longer want to manage from Project Astra.

About this task

- This action stops your cluster from being managed by Project Astra. 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.

- Apps associated with this cluster will no longer be managed and will go into a Detached state.
- Any snapshots or backups associated with applications on the cluster aren't deleted, but data

management operations aren't available from Project Astra.

Steps

1. Delete any snapshots or backups and stop managing the cluster's applications before removing the cluster.

   Learn how to delete snapshots and backups.

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

Result

Project Astra stops managing the clusters.

Cleaning up after the Beta

A few things remain after you've removed apps and clusters from Project Astra:

- The object store that was created in your Google Cloud account
- The Admin role that was installed on each managed Kubernetes cluster
- The service account that you created

You'll need to manually remove these.