Manage apps

Astra Control Center

NetApp
February 12, 2024

Table of Contents

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.

App management requirements

Astra Control has the following app management requirements:

- **Licensing**: To manage apps using Astra Control Center, you need an Astra Control Center license.
- **Namespaces**: Astra Control requires that an app not span more than a single namespace, but a namespace can contain more than one app.
- **StorageClass**: If you install an app with a StorageClass explicitly set and you need to clone the app, the target cluster for the clone operation must have the originally specified StorageClass. Cloning an application with an explicitly set StorageClass to a cluster that does not have the same StorageClass will fail.
- **Kubernetes resources**: Apps that use Kubernetes Resources not collected by Astra Control might not have full app data management capabilities. Astra Control collects the following Kubernetes resources:
  - ClusterRole
  - ClusterRoleBinding
  - ConfigMap
  - CustomResourceDefinition
  - CustomResource
  - DaemonSet
  - Deployment
  - DeploymentConfig
  - Ingress
  - MutatingWebhook
  - PersistentVolumeClaim
  - Pod
  - ReplicaSet
  - RoleBinding
  - Role
  - Route
  - Secret
  - Service
  - ServiceAccount
  - StatefulSet
  - ValidatingWebhook

Supported app installation methods

Astra Control supports the following application installation methods:

- **Manifest file**: Astra Control supports apps installed from a manifest file using kubectl. For example:

```
kubectl apply -f myapp.yaml
```

- **Helm 3**: If you use Helm to install apps, Astra Control requires Helm version 3. Managing and cloning apps installed with Helm 3 (or upgraded from Helm 2 to Helm 3) are fully supported. Managing apps installed with Helm 2 is not supported.
- **Operator-deployed apps**: Astra Control supports apps installed with namespace-scoped operators. These operators are generally designed with a "pass-by-value" rather than "pass-by-reference" architecture. The following are some operator apps that follow these patterns:
  - Apache K8ssandra
  - Jenkins CI
  - Percona XtraDB Cluster

Note that Astra Control might not be able to clone an operator that is designed with a “pass-by-reference” architecture (for example, the CockroachDB operator). During these types of cloning operations, the cloned operator attempts to reference Kubernetes secrets from the source operator despite having its own new secret as part of the cloning process. The clone operation might fail because Astra Control is unaware of the Kubernetes secrets in the source operator.

An operator and the app it installs must use the same namespace; you might need to modify the deployment .yaml file for the operator to ensure this is the case.

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 installed 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 Control 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

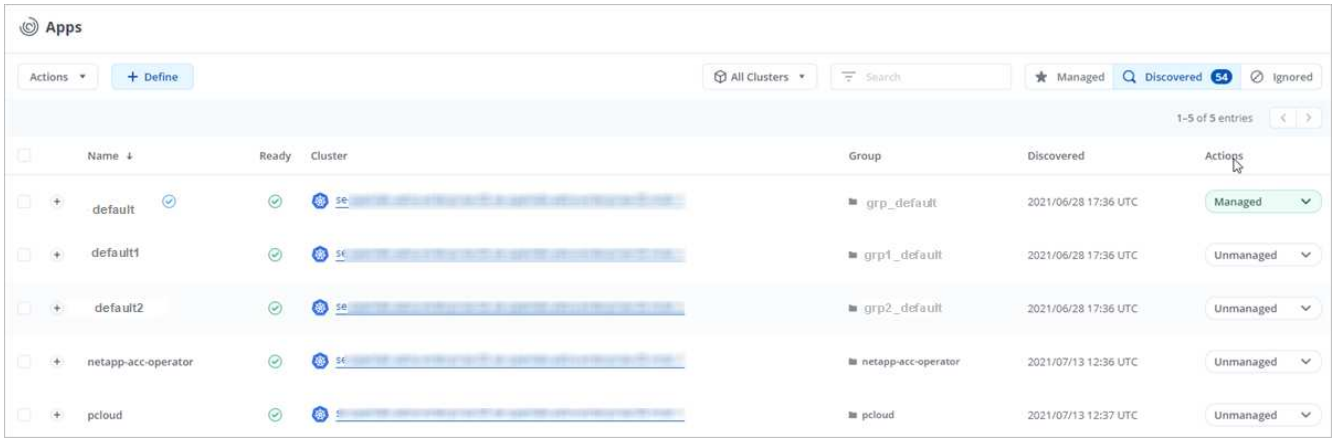
The **Discovered** section of the Apps page shows namespaces and any Helm-installed apps or custom-labeled apps in those namespaces. You can choose to manage each app individually or at the namespace level. It all comes down to the level of granularity that you need for data protection operations.

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 **Applications**.
2. Select **Discovered**.



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

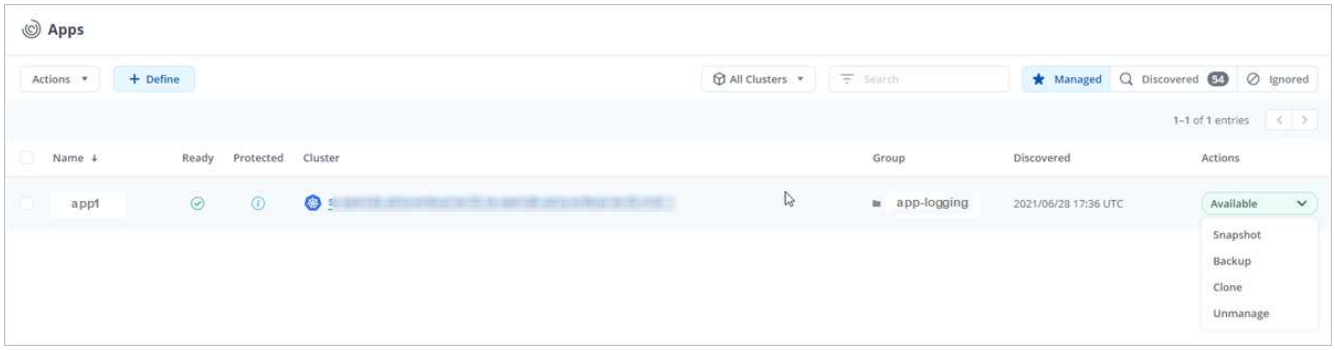
resources.

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

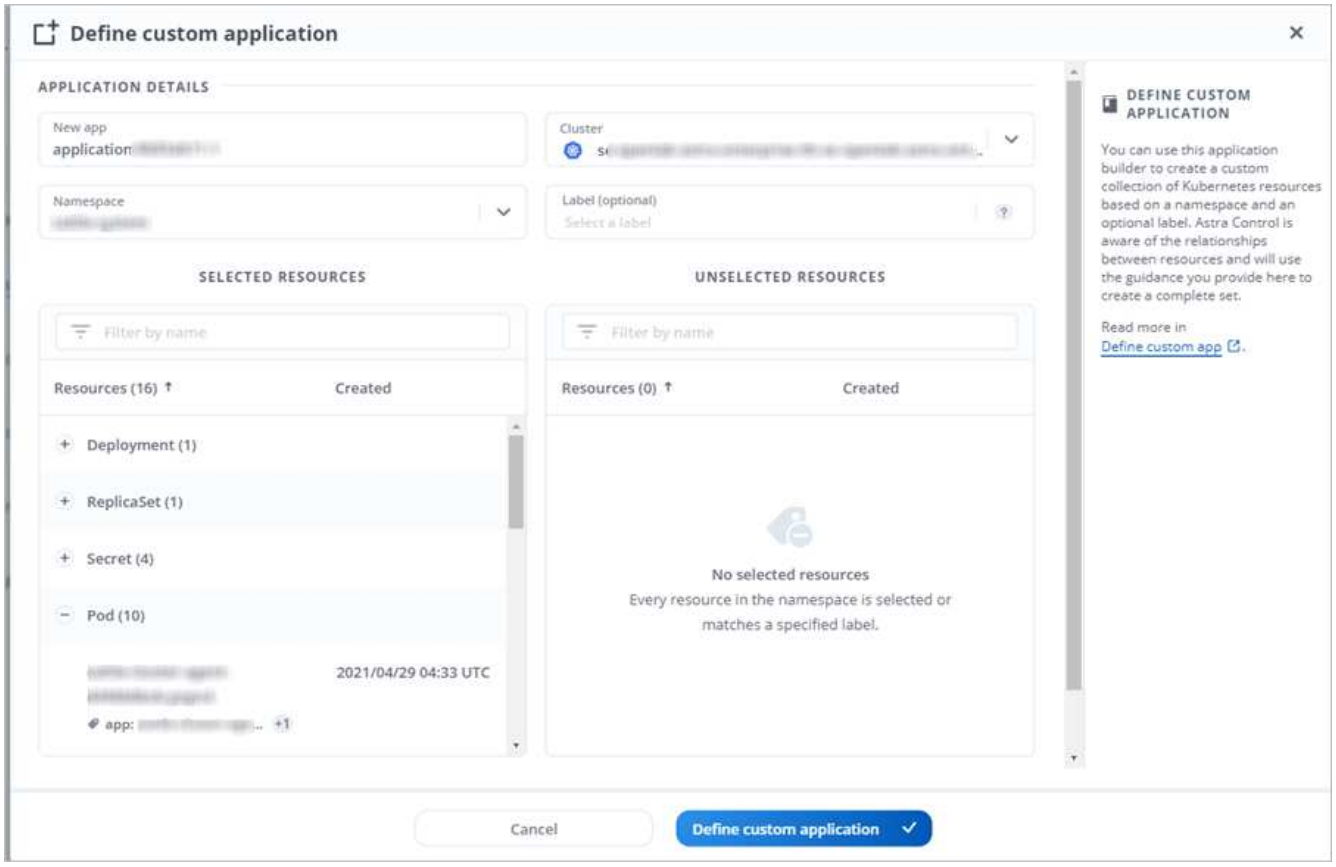
Apps that you chose to manage are now available from the **Managed** tab. Any ignored apps will move to the **Ignored** tab. Ideally, the Discovered tab will show zero apps, so that as new apps are installed, they are easier to find and manage.

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 **Applications**.
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 selecting 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. Select **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 **Applications**.
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.

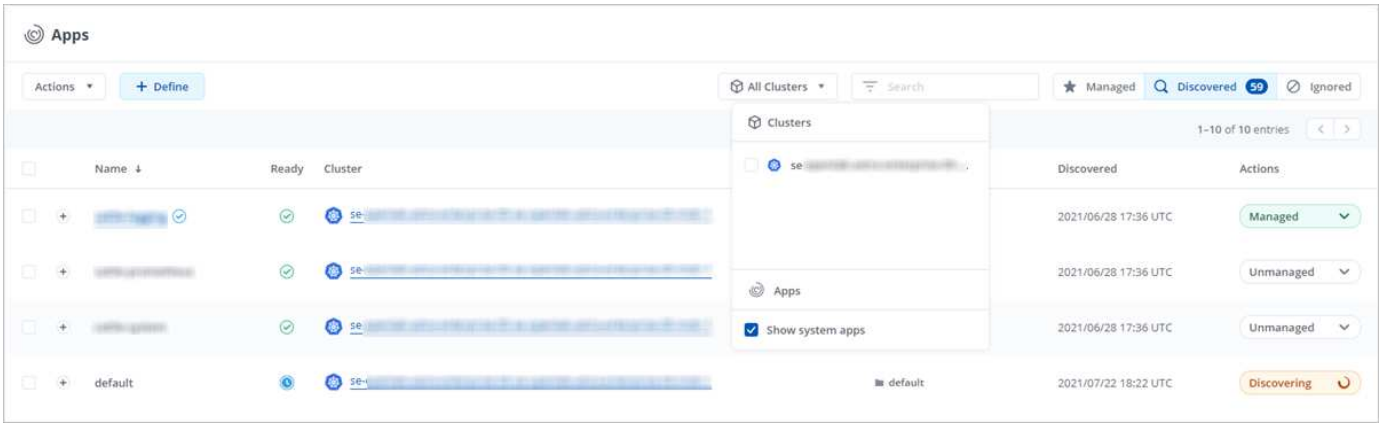
If you unmanage an app, any backups or snapshots that were created earlier will be lost.

Steps

1. From the left navigation bar, select **Applications**.
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.



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 Control 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 select **+ 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 selects 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.

Copyright information

Trademark information