



Manage and protect apps

Project Astra

NetApp

November 17, 2020

This PDF was generated from <https://docs.netapp.com/us-en/project-astra/use/use/manage-apps.html> on November 17, 2020. Always check docs.netapp.com for the latest.

Table of Contents

- Manage and protect apps 1
 - Start managing apps 1
 - Protect apps with snapshots and backups 3
 - Restore apps..... 6
 - Clone and migrate apps 7

Manage and protect apps

Start managing apps

After you add [a Kubernetes cluster to the 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 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 Astra is still in the process of discovering the app. Hovering over the Ready column shows the current status.

[screenshot app discovery status]

After 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. 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

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 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

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

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, 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

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

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

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

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

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

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 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, 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

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

Copyright Information

Copyright © 2020 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.