



# **Manage and protect apps**

Astra

NetApp  
July 12, 2021

# Table of Contents

- Manage and protect apps. . . . . 1
  - Start managing apps . . . . . 1
  - Protect apps with snapshots and backups. . . . . 6
  - Restore apps . . . . . 11
  - Clone and migrate apps . . . . . 13

# 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

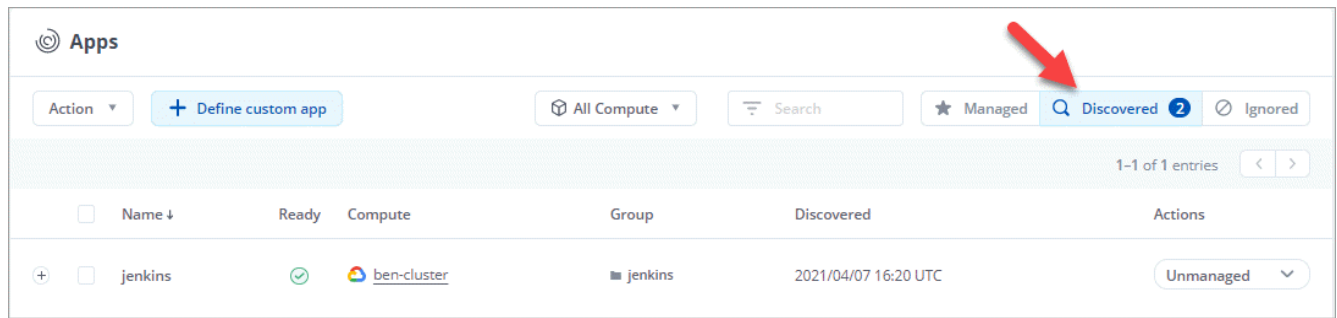
The **Discovered** section of the Apps page shows namespaces and the Helm-installed apps or custom-labeled apps in those namespaces. You can choose to manage each app individually or at the namespace level. It all comes down to the level of granularity that you need for data protection operations.

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

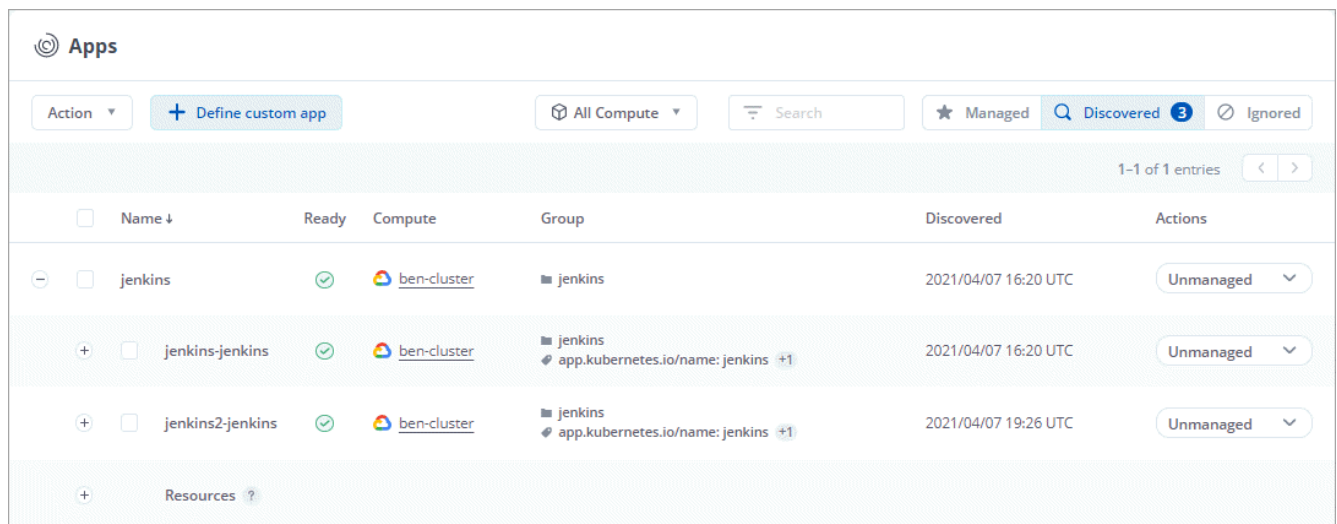
1. Click **Apps** and then click **Discovered**.



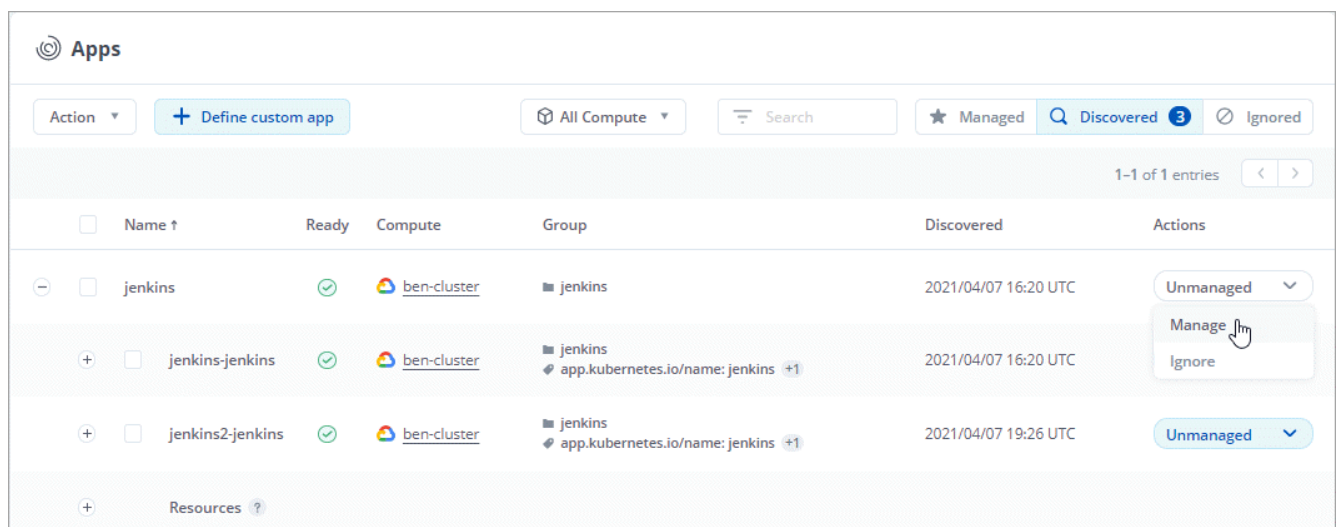
2. View the list of discovered namespaces and expand a namespace to view the apps and associated resources.

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:

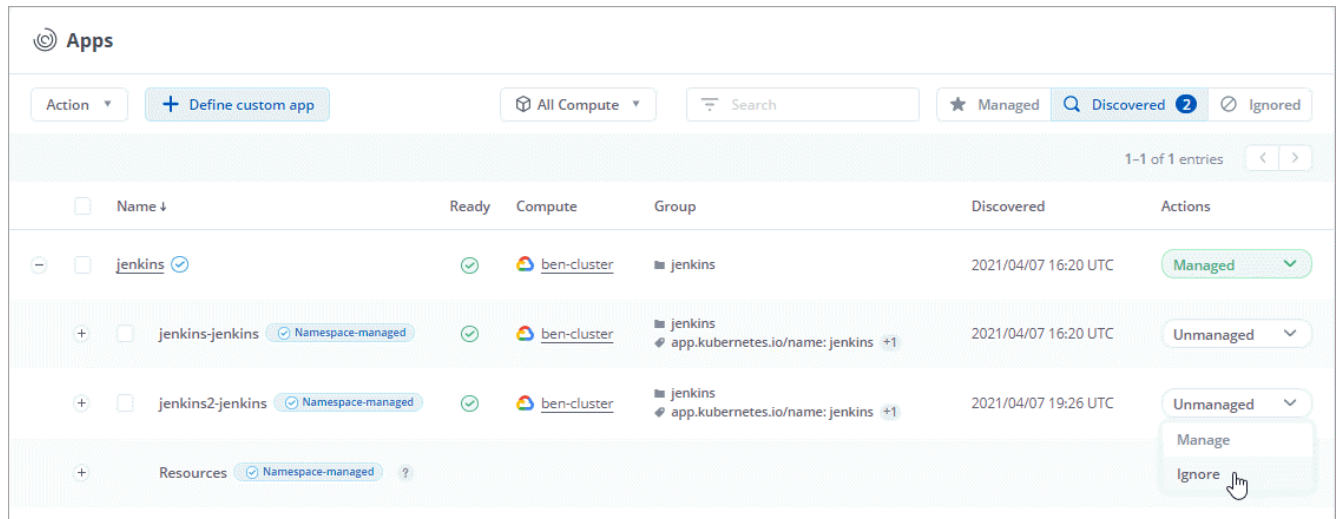


3. Decide whether you want to manage each app individually or at the namespace level.
4. At the desired level in the hierarchy, click the drop-down list in the **Actions** column and click **Manage**.



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.

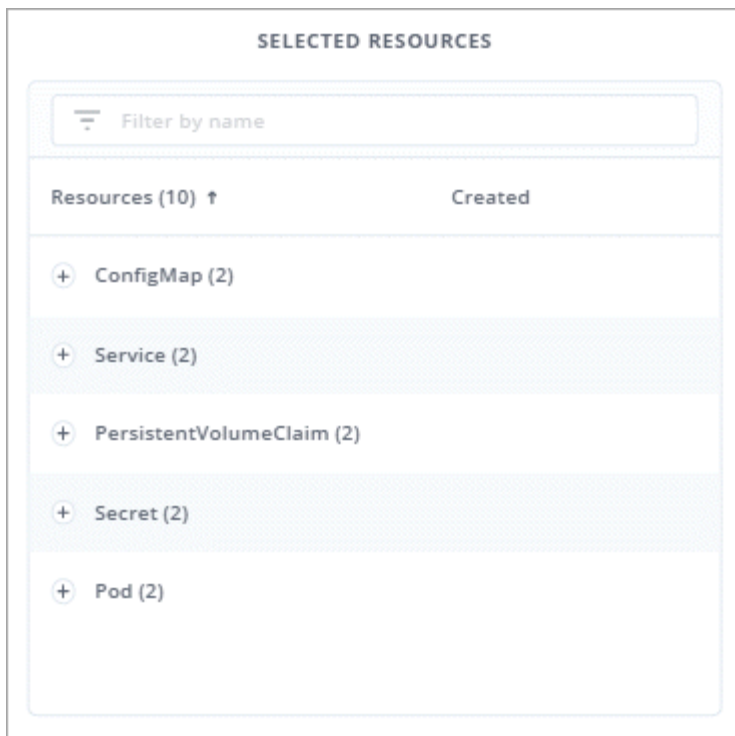
## Manage apps by Kubernetes label

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](#).

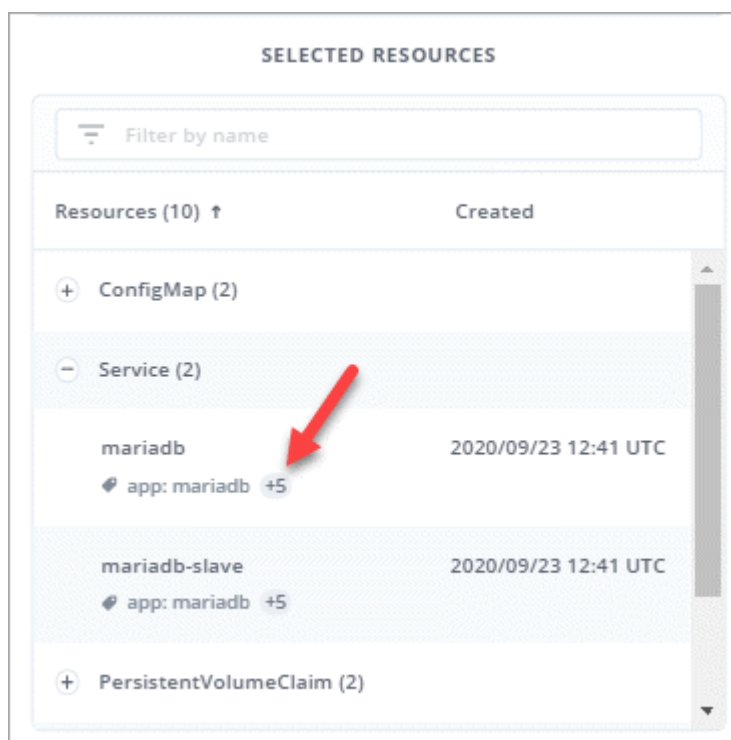
## Steps

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).

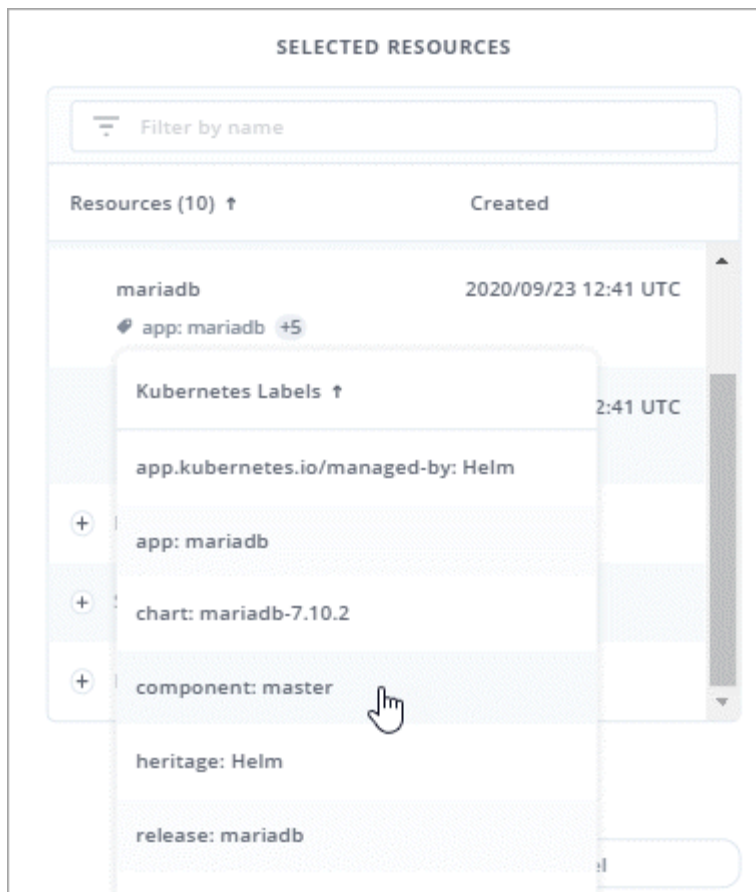
Here's an example:



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

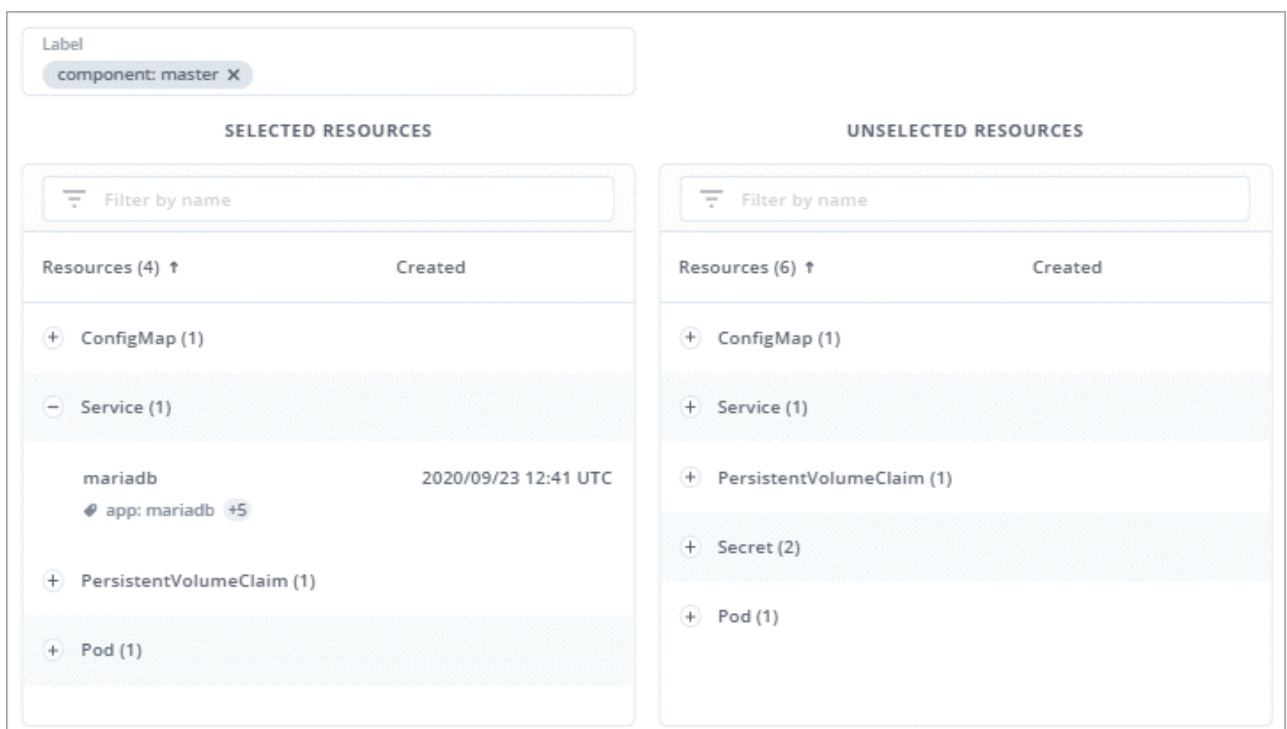


- Select one of the labels.



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.



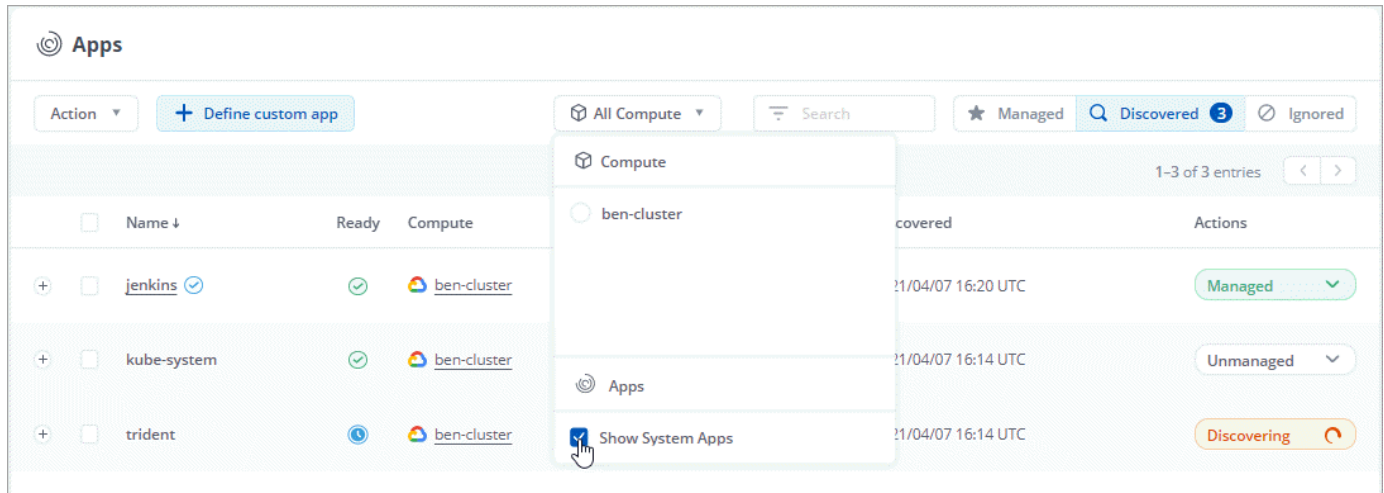
3. Click **Define Custom App**.

## 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 its persistent storage, then you need a backup to recover. A snapshot wouldn't enable you to recover.

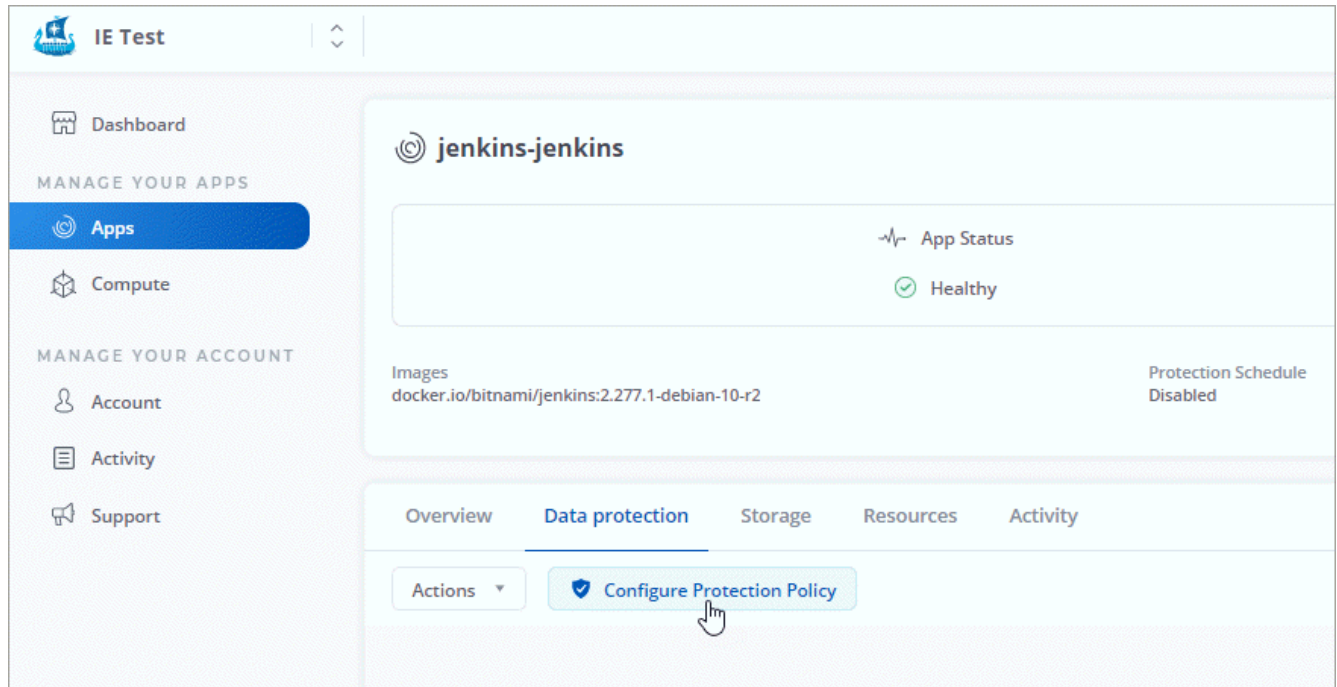
### Configure a protection policy

A protection policy protects an app by creating snapshots, backups, or both at a defined schedule. You can choose to create snapshots and backups hourly, daily, weekly, and monthly, and you can specify the number of copies to retain.



## Steps

1. Click **Apps** and then click the name of 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 hourly, daily, weekly, and monthly.

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

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

**Configure Protection Policy**

STEP 1/2: DETAILS

×

**PROTECTION SCHEDULE**

**Hourly**

Every hour on the 0th minute, keep the last 4 snapshots

**Daily**

Daily at 02:00 (UTC), keep the last 15 snapshots

**Weekly**

Weekly on Mondays at 02:00 (UTC), keep the last 26 snapshots

**Monthly**

Every 1st of the month at 02:00 (UTC), keep the last 12 backups

● Hourly

● Daily

● Weekly

● **Monthly**

Day(s) of Month

1 X

Time (UTC)

02:00

^

v

−

Snapshots to keep

0

+

−

Backups to keep

12

+

**OVERVIEW**

**Schedule and Retention**

Define a policy to continuously protect your application on a schedule and configure a retention count to get started.

For select stateful applications expect IO to pause for a short period of time during a backup or snapshot operation.

Read more in [Protection Policies](#).

Application  
jenkins-jenkins

Namespace  
jenkins

Labels  
app.kubernetes.io/name: jenkins,  
app.kubernetes.io/instance: jenkins

Compute  
ben-cluster

Cancel

Review Information →

- Click **Review Information**.
- Click **Set Protection Policy**.

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

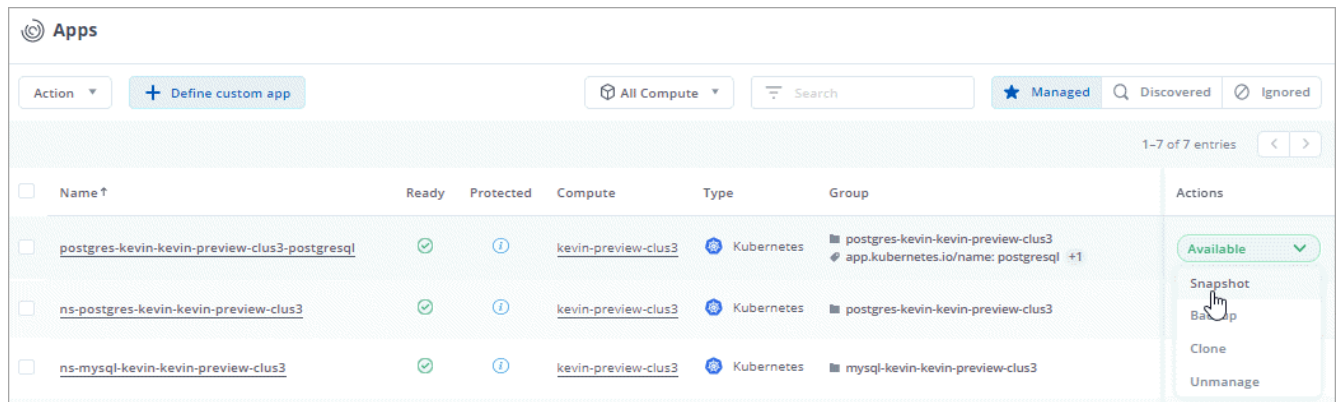
Astra Control implements the data protection policy by creating and retaining snapshots and backups using the schedule and retention policy that you defined.

## Create a snapshot

You can create an on-demand snapshot at any time.

### Steps

- Click **Apps**.
- Click the drop-down list in the **Actions** column for the desired app.
- Click **Snapshot**.



4. Customize the name of the snapshot and then click **Review Information**.

5. Review the snapshot summary and click **Snapshot App**.

## Result

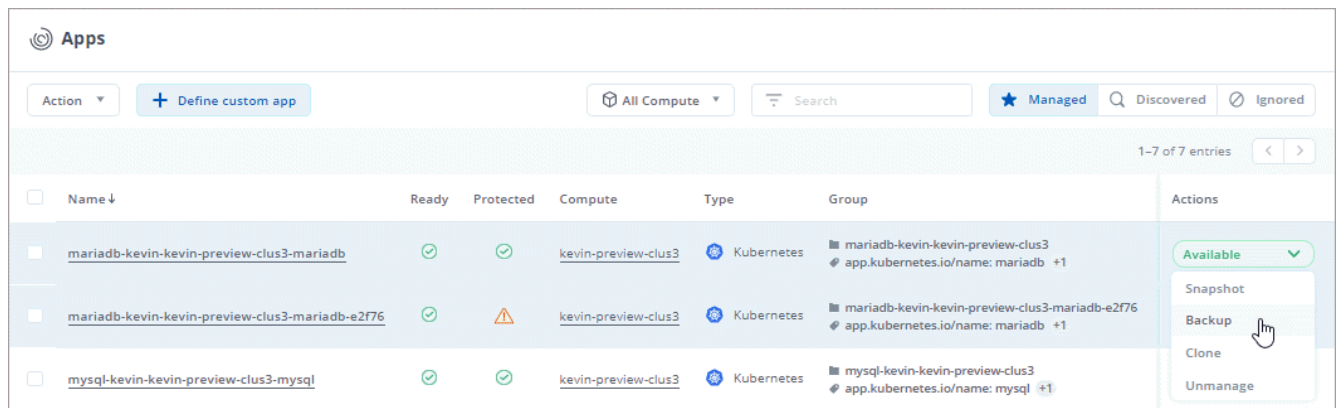
Astra Control creates a snapshot of the apps.

## 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.

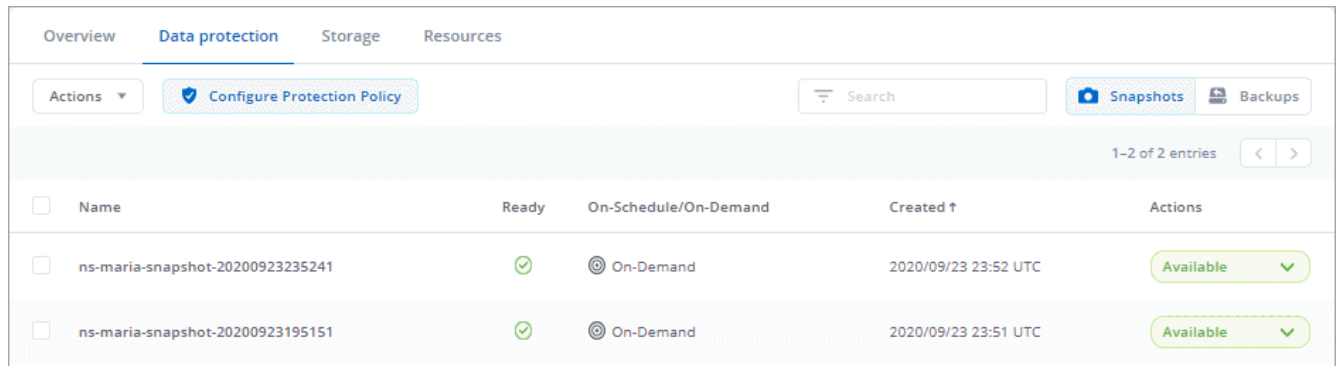
## View snapshots and backups

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.



The screenshot shows the 'Data protection' tab in the Astra Control interface. It displays a table of snapshots for a managed application. The table has columns for Name, Ready status, On-Schedule/On-Demand status, Created time, and Actions. Two snapshots are listed, both with a 'Ready' status of 'Available' and an 'On-Demand' schedule.

<input type="checkbox"/>	Name	Ready	On-Schedule/On-Demand	Created ↑	Actions
<input type="checkbox"/>	ns-maria-snapshot-20200923235241	✓	⌚ On-Demand	2020/09/23 23:52 UTC	Available ✓
<input type="checkbox"/>	ns-maria-snapshot-20200923195151	✓	⌚ On-Demand	2020/09/23 23:51 UTC	Available ✓

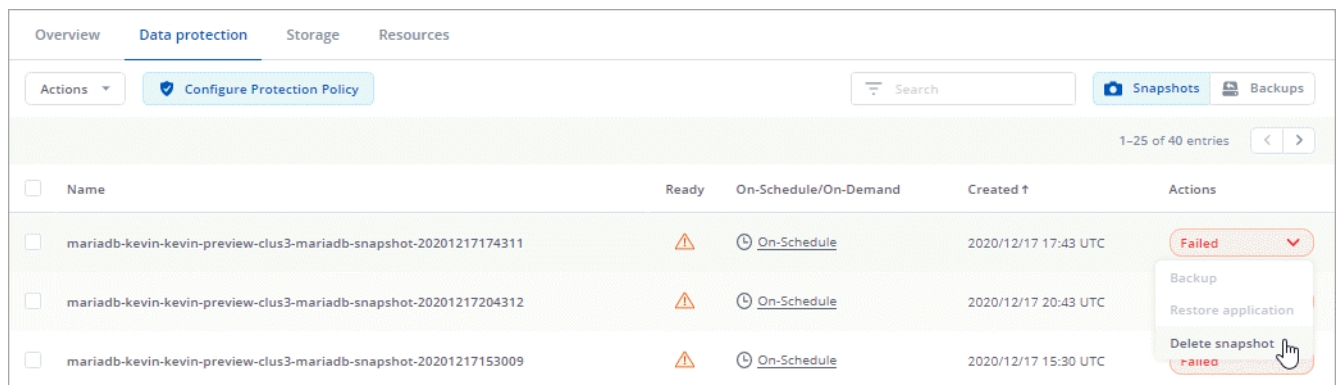
3. Click **Backups** to see the list of backups.

## 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**.



The screenshot shows the 'Data protection' tab with a table of snapshots. The 'Actions' column for the first snapshot is open, showing options: 'Backup', 'Restore application', and 'Delete snapshot'. The 'Delete snapshot' option is highlighted with a mouse cursor.

<input type="checkbox"/>	Name	Ready	On-Schedule/On-Demand	Created ↑	Actions
<input type="checkbox"/>	mariadb-kevin-kevin-preview-clus3-mariadb-snapshot-20201217174311	⚠	⌚ On-Schedule	2020/12/17 17:43 UTC	Failed ✓ Backup Restore application Delete snapshot (highlighted)
<input type="checkbox"/>	mariadb-kevin-kevin-preview-clus3-mariadb-snapshot-20201217204312	⚠	⌚ On-Schedule	2020/12/17 20:43 UTC	
<input type="checkbox"/>	mariadb-kevin-kevin-preview-clus3-mariadb-snapshot-20201217153009	⚠	⌚ On-Schedule	2020/12/17 15:30 UTC	

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

## Result

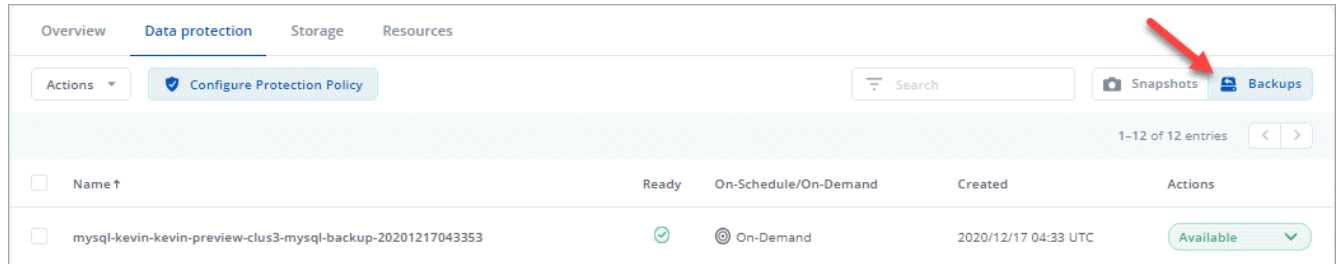
Astra Control deletes the snapshot.

## Delete backups

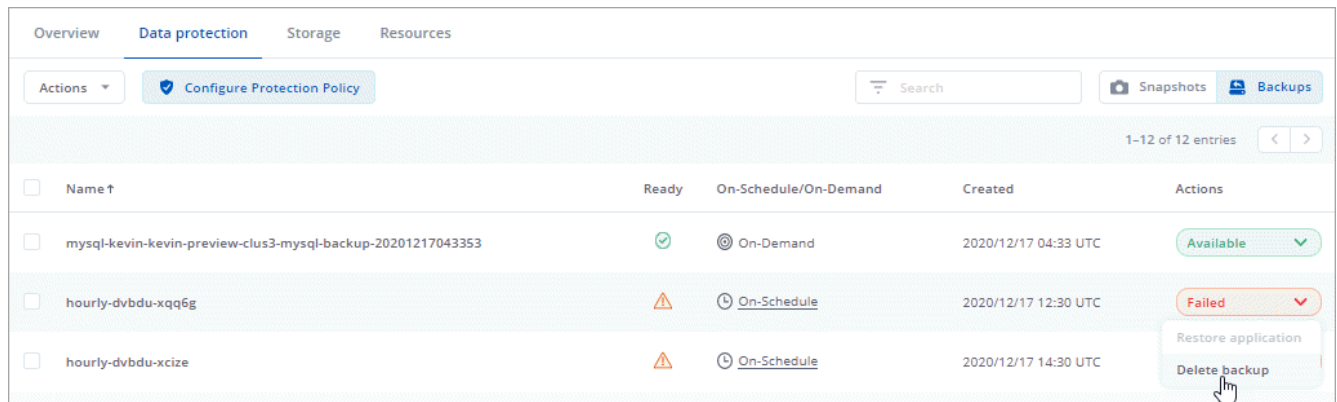
Delete the scheduled or on-demand backups that you no longer need.

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

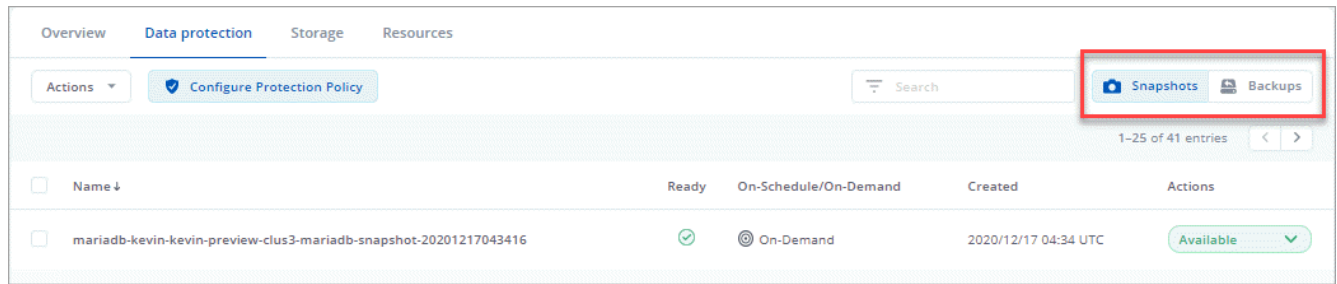
Astra Control deletes the backup.

## Restore apps

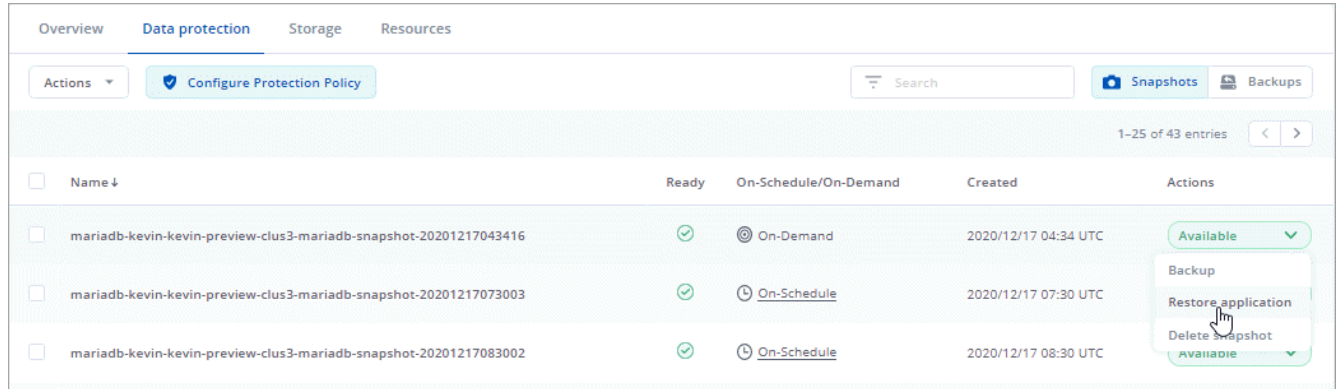
Astra Control can restore your application configuration and persistent storage from a snapshot or backup. Persistent storage backups are transferred from your object store, so restoring from an existing backup will complete the fastest.

### 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**.

Restore Application

STEP 2/2: RESTORE SUMMARY

×

REVIEW RESTORE INFORMATION

**SNAPSHOT**  
mariadb-kevin-kevin-preview-clus3-mariadb-snapshot-20201217043416

**ORIGINAL GROUP**  
mariadb-kevin-kevin-preview-clus3  
app.kubernetes.io/name: mariadb +1

**ORIGINAL COMPUTE**  
kevin-preview-clus3

**CLONE**  
mariadb-kevin-kevin-preview-clus3-mariadb-91c9d

**DESTINATION GROUP**  
mariadb-kevin-kevin-preview-clus3-mariadb-91c9d  
app.kubernetes.io/name: mariadb +1

**DESTINATION COMPUTE**  
kevin-preview-clus3

← Select details

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**.

<div> <div>Apps</div> <div> <div>Action</div> <div> <div>+ Define custom app</div> <div>All Compute</div> <div>Search</div> <div>Managed</div> <div>Discovered 1</div> <div>Ignored</div> </div> </div> </div>							
<div>1-1 of 1 entries</div>							
<input type="checkbox"/>	Name ↓	Ready	Protected	Compute	Group	Discovered	Actions
<input type="checkbox"/>	<a href="#">jenkins-jenkins</a>				jenkins app.kubernetes.io/name: jenkins +1	2021/04/07 16:20 UTC	<div>Available</div> <div> <div>Snapshot</div> <div>Backup</div> <div>Clone</div> <div>Unmanage</div> </div>

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**.

Clone Application

STEP 2/2: CLONE SUMMARY

REVIEW CLONE INFORMATION

APP

jenkins-jenkins

ORIGINAL GROUP

jenkins

app.kubernetes.io/name: jenkins +1

ORIGINAL COMPUTE

ben-cluster

CLONE

jenkins-jenkins-e8ae1

DESTINATION GROUP

jenkins-jenkins-e8ae1

app.kubernetes.io/name: jenkins +1

DESTINATION COMPUTE

ben-cluster

## Result

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



## 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.