



# Protect your data

ASA r2

NetApp  
September 26, 2024

# Table of Contents

- Protect your data ..... 1
  - Create snapshots to back up your data on ASA r2 storage systems ..... 1
  - Replicate snapshots to a remote cluster from ASA r2 storage systems ..... 5
  - Protect your Kubernetes applications on ASA r2 storage systems ..... 10
  - Restore data on ASA r2 storage systems ..... 10
  - Manage ONTAP consistency groups on ASA r2 storage systems ..... 11
  - Manage ONTAP data protection policies and schedules on ASA r2 storage systems ..... 14

# Protect your data

## Create snapshots to back up your data on ASA r2 storage systems

To back up data on your ASA r2 system, you need to create a snapshot. You can use ONTAP System Manager to create a manual snapshot of a single storage unit, or to create a consistency group and schedule automatic snapshots of multiple storage units at the same time.

### Step 1: Optionally, create a consistency group

A consistency group is a collection of storage units that are managed as a single unit. Create consistency groups to simplify storage management and data protection for application workloads spanning multiple storage units. For example, suppose you have a database consisting of 10 storage units in a consistency group, and you need to back up the entire database. Instead of backing up each storage unit, you can back up the entire database by simply adding snapshot data protection to the consistency group.

Create a consistency group using new storage units or create a consistency group using existing storage units.

## Use new storage units

### Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Select **+ Add** ; then select **Using new storage units**.
3. Enter a name for the new storage unit, the number of units, and the capacity per unit.

If you create more than one unit, each unit is created with the same capacity and the same host operating system. To assign a different capacity to each unit, select **More options**; then select **Add a different capacity**.

4. Select the host operating system and host mapping.
5. Select **Add**.

### What's next?

You have created a consistency group containing the storage units you want to protect. You are now ready to create a snapshot.

## Use existing storage units

### Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Select **+ Add** ; then select **Using existing storage units**.
3. Enter a name for the consistency group; then search for and select the storage units you want to include in the consistency group.
4. Select **Add**.

### What's next?

You have created a consistency group containing the storage units you want to protect. You are now ready to create a snapshot.

## Step 2: Create a snapshot

A snapshot is a local, read-only copy of your data that you can use to restore storage units to specific points in time.

Snapshots can be created on demand, or they can be created automatically in regular intervals based on a [snapshot policy and schedule](#). The snapshot policy and schedule specifies when to create the snapshots, how many copies to retain, how to name them, and how to label them for replication. For example, a system might create one snapshot every day at 12:10 a.m., retain the two most recent copies, name them “daily” (appended with a timestamp), and label them “daily” for replication.

### Types of snapshots

You can create an on-demand snapshot of a single storage unit or of a consistency group. You can create automated snapshots of a consistency group containing multiple storage units. You cannot create automated snapshots of a single storage unit.

- On-demand snapshots

An on-demand snapshot of a storage unit can be created at any time. The storage unit does not need to be

a member of a consistency group to be protected by an on-demand snapshot. If you create an on-demand snapshot of a storage unit that is a member of a consistency group, the other storage units in the consistency group are not included in the on-demand snapshot. If you create an on-demand snapshot of a consistency group, all the storage units in the consistency group are included in the snapshot.


- Automated snapshots

Automated snapshots are created using snapshot policies. To apply a snapshot policy to a storage unit for automated snapshot creation, the storage unit must be a member of a consistency group. If you apply a snapshot policy to a consistency group, all the storage units in the consistency group are protected with automated snapshots.

Create a snapshot of a consistency group or a storage unit.

## Snapshot of a consistency group

### Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the name of the consistency group you want to protect.
3. Select  ; then select **Protect**.
4. If you want to create an immediate snapshot on-demand, under **Local protection**, select **Add a snapshot now**.



Local protection creates the snapshot on the same cluster containing the storage unit.

- a. Enter a name for the snapshot or accept the default name; then optionally, enter a SnapMirror label.

The SnapMirror label is used by the remote destination.

5. If you want to create automated snapshots using a snapshot policy, select **Schedule snapshots**.
  - a. Select a snapshot policy.

Accept the default snapshot policy, select an existing policy, or create a new policy.

Option	Steps
Select an existing snapshot policy	Select  next to the default policy; then select the existing policy that you want to use.
Create a new snapshot policy	<ol style="list-style-type: none"><li>a. Select  <b>Add</b> ; then enter the snapshot policy parameters.</li><li>b. Select <b>Add policy</b>.</li></ol>


6. If you want to replicate your snapshots to a remote cluster, under **Remote protection**, select **Replicate to a remote cluster**.
  - a. Select the source cluster and storage VM; then select the replication policy.

The initial data transfer for replication starts immediately by default.

7. Select **Save**.

## Snapshot of storage unit

### Steps

1. In System Manager, select **Storage**.
2. Hover over the name of the storage unit you want to protect.
3. Select  ; then select **Protect**. If you want to create an immediate snapshot on-demand, under **Local protection**, select **Add a snapshot now**.

Local protection creates the snapshot on the same cluster containing the storage unit.



4. Enter a name for the snapshot or accept the default name; then optionally, enter a SnapMirror label.

The SnapMirror label is used by the remote destination.

5. If you want to create automated snapshots using a snapshot policy, select **Schedule snapshots**.

a. Select a snapshot policy.

Accept the default snapshot policy, select an existing policy, or create a new policy.

Option	Steps
Select an existing snapshot policy	Select  next to the default policy; then select the existing policy that you want to use.
Create a new snapshot policy	a. Select  <b>Add</b> ; then enter the snapshot policy parameters. b. Select <b>Add policy</b> .

6. If you want to replicate your snapshots to a remote cluster, under **Remote protection**, select **Replicate to a remote cluster**.

a. Select the source cluster and storage VM; then select the replication policy.

The initial data transfer for replication starts immediately by default.

7. Select **Save**.

### What's next?

Now that your data is protected with snapshots, you should [set up snapshot replication](#) to copy your consistency groups to a geographically remote location for backup and disaster recovery.

## Replicate snapshots to a remote cluster from ASA r2 storage systems

Snapshot replication is a process in which consistency groups on your ASA r2 system are copied to a geographically remote location. After the initial replication, changes to consistency groups are copied to the remote location based upon a replication policy. Replicated consistency groups can be used for disaster recovery or data migration.





Snapshot replication from an ASA r2 storage system is supported only to another ASA r2 storage system. You cannot replicate snapshots from an ASA r2 system to a current ASA, AFF or FAS system.

To set up Snapshot replication, you need to establish a replication relationship between your ASA r2 system and the remote location. The replication relationship is governed by a replication policy. A default policy to replicate all snapshots is created during cluster set up. You can use the default policy or optionally, create a new policy.

### Step 1: Create a cluster peer relationship

Before you can protect your data by replicating it to a remote cluster, you need to create a cluster peer relationship between the local and remote cluster.

#### Steps

1. On the local cluster, in System Manager, select **Cluster > Settings**.
2. Under **Intercluster Settings** next to **Cluster peers** select , then select **Add a cluster peer**.
3. Select **Launch remote cluster**; this generates a passphrase you'll use to authenticate with the remote cluster.
4. After the passphrase for the remote cluster is generated, paste it under **Passphrase** on the local cluster.
5. Select  **Add**; then enter the intercluster network interface IP address.
6. Select **Initiate cluster peering**.


### What's next?

You have peered for local ASA r2 cluster with a remote cluster. You can now create a replication relationship.

## Step 2: Optionally, create a replication policy

The snapshot replication policy defines when updates performed on the ASA r2 cluster are replicated to the remote site.

### Steps

1. In System Manager, select **Protection > Policies**; then select **Replication policies**.
2. Select  **Add**.
3. Enter a name for the replication policy or accept the default name; then enter a description.
4. Select the **Policy scope**.

If you want to apply the replication policy to the entire cluster, select **Cluster**. If you want the replication policy applied only to the storage units in a specific storage VM, select **Storage VM**.

5. Select the **Policy type**.

Option	Steps
Copy data to the remote site after it is written to the source.	<ol style="list-style-type: none"> <li>a. Select <b>Asynchronous</b>.</li> <li>b. Under <b>Transfer snapshots from source</b>, accept the default transfer schedule or select a different one.</li> <li>c. Select to transfer all snapshots or to create rules to determine which snapshots to transfer.</li> <li>d. Optionally, enable network compression.</li> </ol>
Write data to the source and remote sites simultaneously.	<ol style="list-style-type: none"> <li>a. Select <b>Synchronous</b>.</li> </ol>

6. Select **Save**.

### What's next?

You have created a replication policy and are now ready to create a replication relationship between your ASA r2 system and your remote location.

### For more information

Learn more about [storage VMs for client access](#).



### Step 3: Create a replication relationship

A snapshot replication relationship establishes a connection between your ASA r2 system and a remote location so that you can replicate consistency groups to a remote cluster. Replicated consistency groups can be used for disaster recovery or for data migration.

For protection against ransomware attacks, when you set up your replication relationship, you can select to lock the destination snapshots. Locked snapshots cannot be deleted accidentally or maliciously. You can use locked snapshots to recover data if a storage unit is compromised by a ransomware attack.


#### Before you begin

If you want to lock your destination snapshots, you must [initialize the Snapshot compliance clock](#) before you create the replication relationship.

Create a replication relationship with or without locked destination snapshots.

## With locked snapshots

### Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Select a consistency group.
3. Select ; then select **Protect**.
4. Under **Remote protection**, select **Replicate to a remote cluster**.
5. Select the **Replication policy**.

You must select a *vault* replication policy.

6. Select **Destination settings**.
7. Select **Lock destination snapshots to prevent deletion**
8. Enter the maximum and minimum data retention period.
9. To delay the start of the data transfer, deselect **Start transfer immediately**.

The initial data transfer begins immediately by default.

10. Optionally, to override the default transfer schedule, select **Destination settings**, then select **Override transfer schedule**.


Your transfer schedule must be a minimum of 30 minutes to be supported.


11. Select **Save**.

## Without locked snapshots

### Steps

1. In System Manager, select **Protection > Replication**.
2. Select to create the replication relationship with local destination or local source.

Option	Steps
Local destinations	<ol style="list-style-type: none"><li>1. Select <b>Local destinations</b>, then select .</li><li>2. Search for and select the source consistency group.</li></ol> <p>The <i>source</i> consistency group refers to the consistency group on your local cluster that you want to replicate.</p>

Option	Steps
Local sources	<ol style="list-style-type: none"> <li>1. Select <b>Local sources</b>, then select  .</li> <li>2. Search for and select the source consistency group.  The <i>source</i> consistency group refers to the consistency group on your local cluster that you want to replicate.</li> <li>3. Under <b>Replication destination</b>, select the cluster to replicate to; then select the storage VM.</li> </ol>

3. Select a replication policy.
4. To delay the start of the data transfer, select **Destination settings**; then deselect **Start transfer immediately**.

The initial data transfer begins immediately by default.

5. Optionally, to override the default transfer schedule, select **Destination settings**, then select **Override transfer schedule**.

Your transfer schedule must be a minimum of 30 minutes to be supported.

6. Select **Save**.


### What's next?

Now that you have created a replication policy and relationship, your initial data transfer begins as defined in your replication policy. You can optionally test your replication failover to verify that successful failover can occur if your ASA r2 system goes offline.

## Step 4: Test replication failover

Optionally, validate that you can successfully serve data from replicated storage units on a remote cluster if the source cluster is offline.

### Steps

1. In System Manager, select **Protection > Replication**.
2. Hover over the replication relationship you want to test, then select .
3. Select **Test failover**.
4. Enter the failover information, then select **Test failover**.

### What's next?

Now that your data is protected with snapshot replication for disaster recovery, you should [encrypt your data at rest](#) so that it can't be read if a disk in your ASA r2 system is repurposed, returned, misplaced or stolen.

# Protect your Kubernetes applications on ASA r2 storage systems

Use Astra Control Center to protect your Kubernetes applications. Astra Control Center allows you to migrate applications and data from one Kubernetes cluster to another, replicate applications to a remote system using NetApp SnapMirror technology, and clone applications from staging to production.

## For more information

[Learn more about protecting Kubernetes applications using Astra Control.](#)

## Restore data on ASA r2 storage systems

Data in a consistency group or storage unit that is protected by snapshots can be restored if it is lost or corrupted.

### Restore a consistency group

Restoring a consistency group replaces the data in all the storage units in the consistency group with the data from a snapshot. Changes made to the storage units after the snapshot was created are not restored..


You can restore a consistency group from a local or remote snapshot.

#### Restore from a local snapshot

##### Steps


1. In System Manager, select **Protection > Consistency groups**.
2. Double-click the consistency group containing the data you need to restore.

The consistency group details page opens.

3. Select **Snapshots**.
4. Select the snapshot you want to restore; then select .
5. Select **Restore consistency group from this snapshot**; then select **Restore**.

#### Restore from a remote snapshot

##### Steps

1. In System Manager, select **Protection > Replication**.
2. Select **Local destinations**.
3. Select the **Source** you want to restore, then select .
4. Select **Restore**.
5. Select the cluster, storage VM, and consistency group to which you want to restore data.
6. Select the snapshot you want to restore from.
7. When prompted, enter "restore"; then select **Restore**.

## Result

Your consistency group is restored to the point in time of the snapshot used for restoration.


## Restore a storage unit

Restoring a storage unit replaces all the data in the storage unit with the data from a snapshot. Changes made to the storage unit after the snapshot was created are not restored.

### Steps

1. In System Manager, select **Storage**.
2. Double-click the storage unit containing the data you need to restore.

The storage unit details page opens.

3. Select **Snapshots**.
4. Select the snapshot you want to restore.
5. Select ; then select **Restore**.
6. Select **Use this snapshot to restore the storage unit**; then select **Restore**.

## Result

Your storage unit is restored to the point in time of the snapshot used for restoration.

## Manage ONTAP consistency groups on ASA r2 storage systems


A consistency group is a collection of storage units that are managed as a single unit. Use consistency groups for simplified storage management. For example, suppose you have a database consisting of 10 storage units in a consistency group, and you need to back up the entire database. Instead of backing up each storage unit, you can back up the entire database by simply adding snapshot data protection to the consistency group. Backing up the storage units as a consistency group instead of individually also provides a consistent backup of all the units, while backing up units individually could potentially create inconsistencies.

### Add snapshot data protection to a consistency group

When you add snapshot data protection to a consistency group, local snapshots of the consistency group are taken at regular intervals based on a pre-defined schedule.





You can use snapshots to [restore data](#) that is lost or corrupted.

### Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group you want to protect.
3. Select ; then select **Edit**.
4. Under **Local protection**, select **Schedule snapshots**.

5. Select a snapshot policy.

Accept the default snapshot policy, select an existing policy, or create a new policy.

Option	Steps
Select an existing snapshot policy	Select  next to the default policy; then select the existing policy that you want to use.
Create a new snapshot policy	<ol style="list-style-type: none"><li>Select  <b>Add</b> ; then enter the new policy name.</li><li>Select the policy scope.</li><li>Under <b>Schedules</b> select  <b>Add</b> .</li><li>Select the name that appears under <b>Schedule name</b>;  then select  .</li><li>Select the policy schedule.</li><li>Under <b>Maximum snapshots</b>, enter the maximum number of snapshots that you want to retain of the consistency group.</li><li>Optionally, under <b>SnapMirror label</b> enter a SnapMirror label.</li><li>Select <b>Save</b>.</li></ol>

6. Select **Edit**.


### What's next

Now that your data is protect with snapshots, you should [set up snapshot replication](#) to copy your consistency groups to a geographically remote location for backup and disaster recovery.

## Remove snapshot data protection from a consistency group

When you remove snapshot data protection from a consistency group, snapshots are disabled for all the storage units in the consistency group.

### Steps

- In System Manager, select **Protection > Consistency groups**.
- Hover over the consistency group you want to stop protecting.
- Select ; then select **Edit**.
- Under **Local protection**, deselect Schedule snapshots.
- Select **Edit**.

### Result

Snapshots will not be taken for any of the storage units in the consistency group.


## Add storage units to a consistency group

Expand the amount of storage managed by a consistency group by adding storage units to the consistency group.

You can add existing storage units to your consistency group or you can create new storage units to add to the consistency group.


### Add existing storage units

#### Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group you want to expand.
3. Select ; then select **Expand**.
4. Select **Using existing storage units**.
5. Select the storage units to add to the consistency group; then select **Expand**.

### Add new storage units

#### Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group you want to expand.
3. Select ; then select **Expand**.
4. Select **Using new storage units**.
5. Enter the number of units you want to create and the capacity per unit.

If you create more than one unit, each unit is created with the same capacity and the same host operating system. To assign a different capacity to each unit, select **Add a different capacity** to assign a different capacity to each unit.

6. Select **Expand**.

#### What's next

After you create a new storage unit, you should [add host initiators](#) and [map the newly created storage unit to a host](#). Adding host initiators makes hosts eligible to access the storage units and perform data operations. Mapping a storage unit to a host allows the storage unit to begin serving data to the host it is mapped to.

#### What's next?

Existing snapshots of the consistency group won't include your newly added storage units. You should [create an immediate snapshot](#) of your consistency group to protect your newly added storage units until the next scheduled snapshot is automatically created.

## Remove a storage unit from a consistency group

You should remove a storage unit from a consistency group if you want to delete the storage unit, if you want manage it as part of a different consistency group, or if you no longer need to protect the data it contains. Removing a storage unit from a consistency group breaks the relationship between the storage unit and the consistency group, but does not delete the storage unit.

#### Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Double-click the consistency group from which you want to remove a storage unit.

3. In the **Overview** section, under **Storage units**, select the storage unit you want to remove; then select **Remove from consistency group**.

### Result

The storage unit is no longer a member of the consistency group.

### What's next

If you need to continue data protection for the storage unit, add the storage unit to another consistency group.


## Delete a consistency group

If you no longer need to manage the members of a consistency group as a single unit, you can delete the consistency group. After a consistency group is deleted, the storage units previously in the group remain active on the cluster.

### Before you begin

If the consistency group you want to delete is in a replication relationship, you must break the relationship before you delete the consistency group. After you delete a previously replication consistency group, the storage units that were in the consistency group remain active on the cluster and their replicated copies remain on the remote cluster.

### Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group you want to delete.
3. Select ; then select **Delete**.
4. Accept the warning, then select **Delete**.

### What's next?

After you delete a consistency group, the storage units previously in the consistency group are no longer protected by snapshots. Consider adding these storage units to another consistency group to protect them against data loss.

## Manage ONTAP data protection policies and schedules on ASA r2 storage systems

Use snapshot policies to protect data in your consistency groups on an automated schedule. Use policy schedules within snapshot policies to determine how often snapshots are taken.

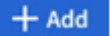
### Create a new protection policy schedule

A protection policy schedule defines how often a snapshots policy is executed. You can create schedules to run in regular intervals based on a number of days, hours, or minutes. For example, you can create a schedule to run every hour or to run only once per day. You can also create schedules to run at specific times on specific days of the week or month. For example, you can create a schedule to run at 12:15am on the 20th of every month.

Defining various protection policy schedules gives you the flexibility to increase or decrease the frequency of snapshots for different applications. This enables you to provide a greater level of protection and a lower risk of data loss for your critical workloads than what might be needed for less critical workloads.



## Steps

1. Select **Protection > Policies**; then select **Schedule**.
2. Select  .
3. Enter a name for the schedule; then select the schedule parameters.
4. Select **Save**.

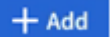
## What's next?

Now that you have created a new policy schedule, you can use the newly created schedule within your policies to define when snapshots are taken.

## Create a snapshot policy

A snapshot policy defines how often snapshots are taken, the maximum number of snapshots allowed, and how long snapshots are retained.

## Steps

1. In System Manager, select **Protection > Policies**; then select **Snapshot policies**.
2. Select  .
3. Enter a name for the snapshot policy.
4. Select **Cluster** to apply the policy to the entire cluster. Select **Storage VM** to apply the policy to an individual storage VM.
5. Select **Add a schedule**; then enter the snapshot policy schedule.
6. Select **Add policy**.


## What's next?

Now that you have created a snapshot policy, you can apply it to a consistency group. Snapshots will be taken of the consistency group based on the parameters you set in your snapshot policy.

## Apply a snapshot policy to a consistency group

Apply a snapshot policy to a consistency group to automatically create, retain, and label snapshots of the consistency group.

## Steps

1. In System Manager, select **Protection > Policies**; then select **Snapshot policies**.
2. Hover over the name of the snapshot policy you want to apply.
3. Select  ; then select **Apply**.
4. Select the consistency groups to which you want to apply the snapshot policy; then select **Apply**.

## What's next?


Now that your data is protected with snapshots, you should [set up a replication relationship](#) to copy your consistency groups to a geographically remote location for backup and disaster recovery.

## Edit, delete, or disable a snapshot policy

Edit a snapshot policy to modify the policy name, maximum number of snapshots, or the SnapMirror label. Delete a policy to remove it and its associated back up data from your cluster. Disable a policy to temporarily

stop the creation or transfer of snapshots specified by the policy.

### Steps

1. In System Manager, select **Protection > Policies**; then select **Snapshot policies**.
2. Hover over the name of the snapshot policy you want to edit.
3. Select ; then select **Edit**, **Delete**, or **Disable**.


### Result

You have modified, deleted or disabled the snapshot policy.

## Edit a replication policy

Edit a replication policy to modify the policy description, transfer schedule, and rules. You can also edit the policy to enable or disable network compression.

### Steps

1. In System Manager, select **Protection > Policies**.
2. Select **Replication policies**.
3. Hover over the replication policy that you want to edit; then select .
4. Select **Edit**.
5. Update the policy; then select **Save**.

### Result

You have modified the replication policy.

## Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## 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.