



Use Cloud Volumes Service for AWS

Cloud Volumes Service for AWS

NetApp

March 29, 2022

Table of Contents

- Use Cloud Volumes Service for AWS 1
 - Managing Cloud Volumes Service for AWS 1
 - Manage cloud volumes snapshots 8

Use Cloud Volumes Service for AWS

Managing Cloud Volumes Service for AWS

Cloud Manager enables you to create cloud volumes based on your [Cloud Volumes Service for AWS](#) subscription. You can also discover cloud volumes that you have already created from the Cloud Volumes Service interface and add them to a working environment.



With the launch of [Amazon FSx for ONTAP](#), you can no longer create new CVS for AWS working environments in Cloud Manager. However, if you had previously added CVS for AWS working environments to Cloud Manager, you can continue to create and manage volumes.

Create cloud volumes

For configurations where volumes already exist in the Cloud Volumes Service working environment you can use these steps to add new volumes.

For configurations where no volumes exist, you can create your first volume directly from Cloud Manager after you have set up your Cloud Volumes Service for AWS subscription. In the past, the first volume had to be created directly in the Cloud Volumes Service user interface.

Before you begin

- If you want to use SMB in AWS, you must have set up DNS and Active Directory.
- When planning to create an SMB volume, you must have a Windows Active Directory server available to which you can connect. You will enter this information when creating the volume. Also, make sure that the Admin user is able to create a machine account in the Organizational unit (OU) path specified.
- You will need this information when creating the first volume in a new region/working environment:
 - AWS account ID: A 12-digit Amazon account identifier with no dashes. To find your account ID, refer to this [AWS topic](#).
 - Classless Inter-Domain Routing (CIDR) Block: An unused IPv4 CIDR block. The network prefix must range between /16 and /28, and it must also fall within the ranges reserved for private networks (RFC 1918). Do not choose a network that overlaps your VPC CIDR allocations.

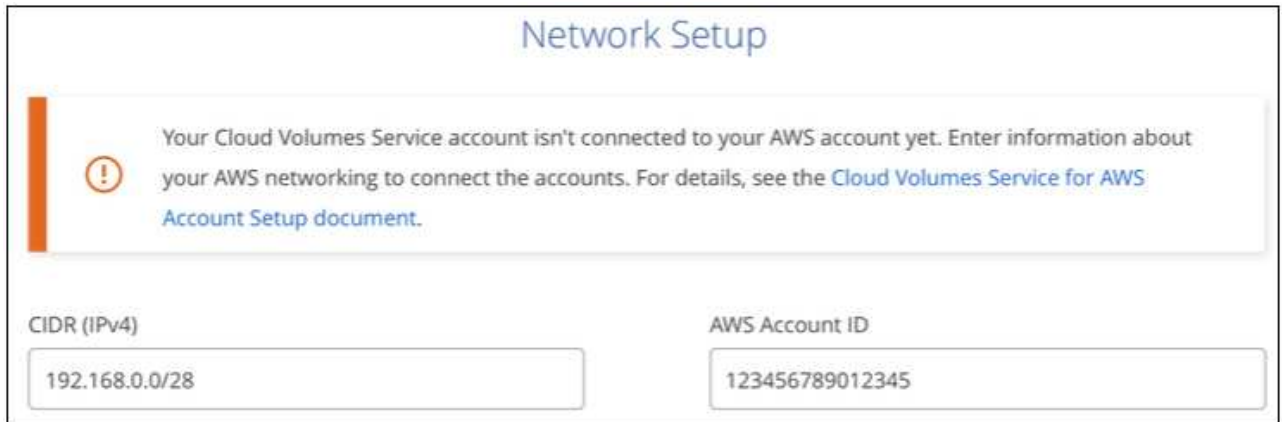
Steps

1. Select a CVS for AWS working environment and click **Add New Volume**.



2. If you are adding the first volume to the working environment in the region, you have to add AWS networking information.

- a. Enter the IPv4 range (CIDR) for the region.
- b. Enter the 12-digit AWS account ID (with no dashes) to connect your Cloud Volumes account to your AWS account.
- c. Click **Continue**.



3. The Accepting Virtual Interfaces page describes some steps you will need to perform after you add the volume so that you are prepared to complete that step. Just click **Continue** again.
4. In the Details & Tags page, enter details about the volume:
 - a. Enter a name for the volume.
 - b. Specify a size within the range of 100 GiB to 90,000 GiB (equivalent to 88 TiBs).
[Learn more about allocated capacity.](#)
 - c. Specify a service level: Standard, Premium, or Extreme.
[Learn more about service levels.](#)
 - d. Enter one or more tag names to categorize the volume if you want.
 - e. Click **Continue**.
5. In the Protocol page, select NFS, SMB, or Dual Protocol and then define the details. Required entries for NFS and SMB are shown in separate sections below.
6. In the Volume Path field, specify the name of the volume export you will see when you mount the volume.
7. If you select Dual-protocol you can select the security style by selecting NTFS or UNIX. Security styles affect the file permission type used and how permissions can be modified.
 - UNIX uses NFSv3 mode bits, and only NFS clients can modify permissions.
 - NTFS uses NTFS ACLs, and only SMB clients can modify permissions.
8. For NFS:
 - a. In the NFS Version field, select NFSv3, NFSv4.1, or both depending on your requirements.
 - b. Optionally, you can create an export policy to identify the clients that can access the volume. Specify the:
 - Allowed clients by using an IP address or Classless Inter-Domain Routing (CIDR).

- Access rights as Read & Write or Read Only.
- Access protocol (or protocols if the volume allows both NFSv3 and NFSv4.1 access) used for users.
- Click **+ Add Export Policy Rule** if you want to define additional export policy rules.

The following image shows the Volume page filled out for the NFS protocol:

The screenshot shows the 'Protocol' configuration interface. At the top, 'NFS Protocol' is selected. Below, the 'Export Policy' section contains two rules. The first rule has a 'Volume Path' of 'vol1' and an 'Allowed Client & Access' of '192.168.1.2/24' with 'Read & Write' permissions and both 'NFSv3' and 'NFSv4.1' versions selected. The second rule has an 'Allowed Client & Access' of '192.168.1.22/24' with 'Read & Write' permissions and 'NFSv4.1' selected.

9. For SMB:

- You can enable SMB session encryption by checking the box for SMB Protocol Encryption.
- You can integrate the volume with an existing Windows Active Directory server by completing the fields in the Active directory section:

| Field | Description |
|---|--|
| DNS Primary IP Address | The IP addresses of the DNS servers that provide name resolution for the SMB server. Use a comma to separate the IP addresses when referencing multiple servers, for example, 172.31.25.223, 172.31.2.74.. |
| Active Directory Domain to join | The FQDN of the Active Directory (AD) domain that you want the SMB server to join. When using AWS Managed Microsoft AD, use the value from the "Directory DNS name" field. |
| SMB Server NetBIOS name | A NetBIOS name for the SMB server that will be created. |
| Credentials authorized to join the domain | The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain. |

| Field | Description |
|---------------------|--|
| Organizational Unit | The organizational unit within the AD domain to associate with the SMB server. The default is CN=Computers for connections to your own Windows Active Directory server. If you configure AWS Managed Microsoft AD as the AD server for the Cloud Volumes Service, you should enter OU=Computers,OU=corp in this field. |

The following image shows the Volume page filled out for the SMB protocol:

SMB Connectivity Setup

DNS Primary IP Address: 127.0.0.1

User Name: administrator

Active Directory Domain to Join: yourdomain.com up to 107 characters

Password:

SMB Server NetBIOS Name: WEName

Organizational Unit: CN=Computers



You should follow the guidance on AWS security group settings to enable cloud volumes to integrate with Windows Active Directory servers correctly. See [AWS security group settings for Windows AD servers](#) for more information.

10. In the Volume from Snapshot page, if you want this volume to be created based on a snapshot of an existing volume, select the snapshot from the Snapshot Name drop-down list.
11. In the Snapshot Policy page, you can enable Cloud Volumes Service to create snapshot copies of your volumes based on a schedule. You can do this now or edit the volume later to define the snapshot policy.

See [Creating a snapshot policy](#) for more information about snapshot functionality.

12. Click **Add Volume**.

The new volume is added to the working environment.

After you finish

If this is the first volume created in this AWS subscription, you need to launch the AWS Management Console to accept the two virtual interface that will be used in this AWS region to connect all your cloud volumes. See the [NetApp Cloud Volumes Service for AWS Account Setup Guide](#) for details.

You must accept the interfaces within 10 minutes after clicking the **Add Volume** button or the system may time out. If this happens, email cvs-support@netapp.com with your AWS Customer ID and NetApp Serial Number. Support will fix the issue and you can restart the onboarding process.

Then continue with [Mounting the cloud volume](#).

Mount the cloud volume

You can mount a cloud volume to your AWS instance. Cloud volumes currently support NFSv3 and NFSv4.1 for Linux and UNIX clients, and SMB 3.0 and 3.1.1 for Windows clients.

Note: Please use the highlighted protocol/dialect supported by your client.

Steps

1. Open the working environment.
2. Hover over the volume and click **Mount the volume**.

NFS and SMB volumes display mount instructions for that protocol. Dual-protocol volumes provide both sets of instructions.

3. Hover over the commands and copy them to your clipboard to make this process easier. Just add the destination directory/mount point at the end of the command.

NFS example:

Mount the volume - testk

Setting up your instance

1. Open an SSH client and connect to your instance.
2. Install the nfs client on your instance.

On Red Hat Enterprise Linux or SuSE Linux instance:

```
$ sudo yum install -y nfs-utils
```

On an Ubuntu or Debian instance:

```
$ sudo apt-get install nfs-common
```

Mounting your volume

1. Create a new directory on your instance:

```
$ sudo mkdir /dir
```

2. Mount your NFSv3 volume using the command below:

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsiz=65536,vers=3,tc...
```

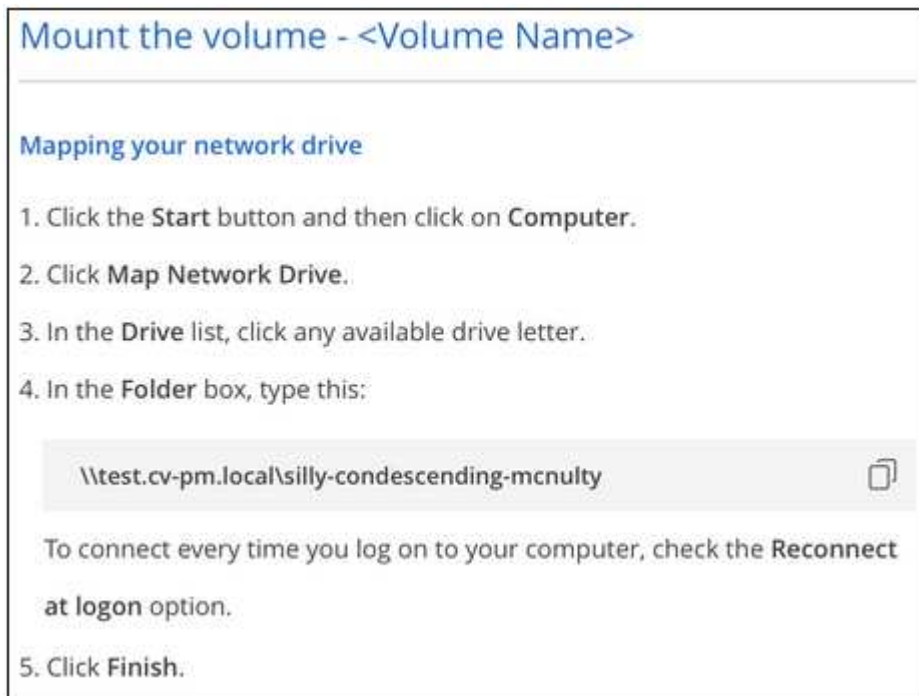
3. Mount your NFSv4.1 volume using the command below:

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsiz=65536,vers=4.1,t...
```

The maximum I/O size defined by the `rsize` and `wsiz` options is 1048576, however 65536 is the recommended default for most use cases.

Note that Linux clients will default to NFSv4.1 unless the version is specified with the `vers=<nfs_version>` option.

SMB example:



4. Connect to your Amazon Elastic Compute Cloud (EC2) instance by using an SSH or RDP client, and then follow the mount instructions for your instance.

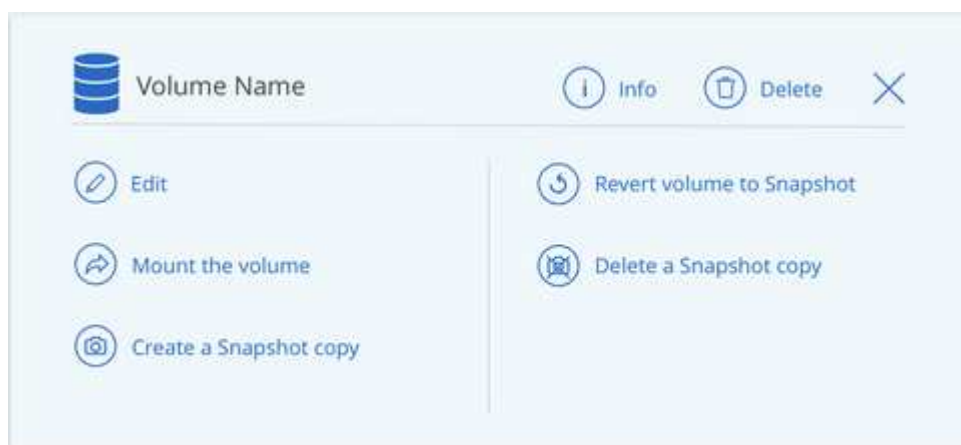
After completing the steps in the mount instructions, you have successfully mounted the cloud volume to your AWS instance.

Managing existing volumes

You can manage existing volumes as your storage needs change. You can view, edit, restore, and delete volumes.

Steps

1. Open the working environment.
2. Hover over the volume.



3. Manage your volumes:

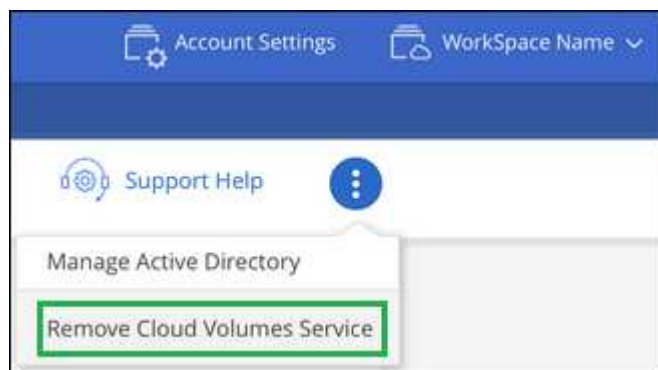
| Task | Action |
|---|---|
| View information about a volume | Select a volume, and then click Info . |
| Edit a volume (including snapshot policy) | a. Select a volume, and then click Edit . b. Modify the volume's properties and then click Update . |
| Get the NFS or SMB mount command | a. Select a volume, and then click Mount the volume . b. Click Copy to copy the command(s). |
| Create a Snapshot copy on demand | a. Select a volume, and then click Create a Snapshot copy . b. Change the snapshot name, if needed, and then click Create . |
| Replace the volume with the contents of a Snapshot copy | a. Select a volume, and then click Revert volume to Snapshot . b. Select a Snapshot copy and click Revert . |
| Delete a Snapshot copy | a. Select a volume, and then click Delete a Snapshot copy . b. Select the Snapshot copy you want to delete and click Delete . c. Click Delete again to confirm. |
| Delete a volume | a. Unmount the volume from all clients: <ul style="list-style-type: none"> ◦ On Linux clients, use the <code>umount</code> command. ◦ On Windows clients, click Disconnect network drive. b. Select a volume, and then click Delete . c. Click Delete again to confirm. |


Remove Cloud Volumes Service from Cloud Manager

You can remove a Cloud Volumes Service for AWS subscription and all existing volumes from Cloud Manager. The volumes are not deleted, they are just removed from the Cloud Manager interface.

Steps

1. Open the working environment.





2. Click the  button at the top of the page and click **Remove Cloud Volumes Service**.
3. In the confirmation dialog box, click **Remove**.

Manage Active Directory configuration

If you change your DNS servers or Active Directory domain, you need to modify the SMB server in Cloud Volumes Services so that it can continue to serve storage to clients.

You can also delete the link to an Active Directory if you no longer need it.

Steps

1. Open the working environment.
2. Click the  button at the top of the page and click **Manage Active Directory**.
3. If no Active Directory is configured, you can add one now. If one is configured, you can modify the settings or delete it using the  button.
4. Specify the settings for the Active Directory that you want to join:

| Field | Description |
|---|--|
| DNS Primary IP Address | The IP addresses of the DNS servers that provide name resolution for the SMB server. Use a comma to separate the IP addresses when referencing multiple servers, for example, 172.31.25.223, 172.31.2.74. |
| Active Directory Domain to join | The FQDN of the Active Directory (AD) domain that you want the SMB server to join. When using AWS Managed Microsoft AD, use the value from the "Directory DNS name" field. |
| SMB Server NetBIOS name | A NetBIOS name for the SMB server that will be created. |
| Credentials authorized to join the domain | The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain. |
| Organizational Unit | The organizational unit within the AD domain to associate with the SMB server. The default is CN=Computers for connections to your own Windows Active Directory server. If you configure AWS Managed Microsoft AD as the AD server for the Cloud Volumes Service, you should enter OU=Computers,OU=corp in this field. |

5. Click **Save** to save your settings.

Manage cloud volumes snapshots

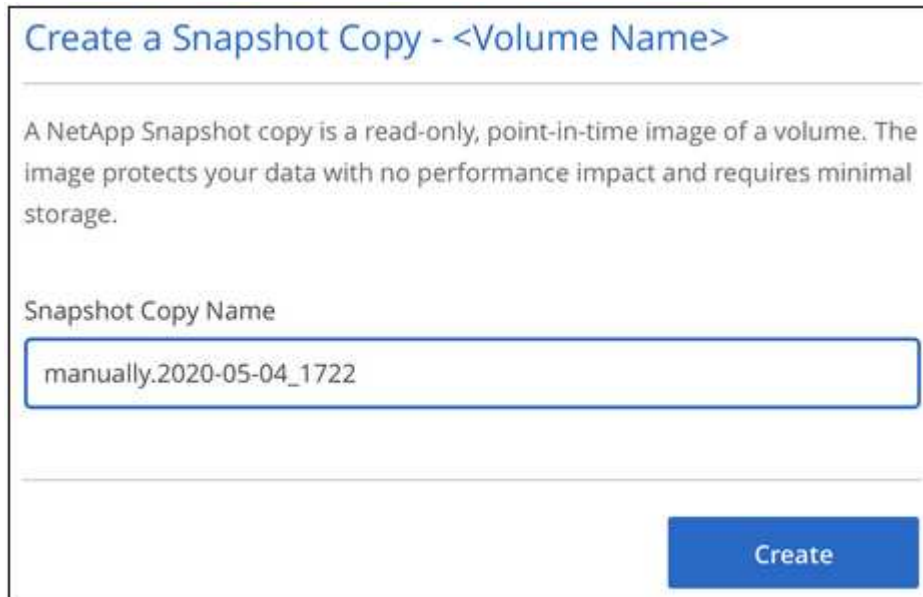
You can create a snapshot policy for each volume so that you can recover or restore the entire contents of a volume from an earlier time. You can also create an on-demand snapshot of a cloud volume when needed.

Create an on-demand snapshot

You can create an on-demand snapshot of a cloud volume if you want to create a snapshot with the current volume state.

Steps

1. Open the working environment.
2. Hover over the volume and click **Create a snapshot copy**.
3. Enter a name for the snapshot, or use the automatically generated name, and click **Create**.



Create a Snapshot Copy - <Volume Name>

A NetApp Snapshot copy is a read-only, point-in-time image of a volume. The image protects your data with no performance impact and requires minimal storage.

Snapshot Copy Name

manually.2020-05-04_1722

Create

Create or modify a snapshot policy

You can create or modify a snapshot policy as necessary for a cloud volume. You define the snapshot policy from the *Snapshot Policy* tab either when creating a volume or when editing a volume.

Steps

1. Open the working environment.
2. Hover over the volume and click **Edit**.
3. From the *Snapshot Policy* tab, move the enable snapshots slider to the right.
4. Define the schedule for snapshots:
 - a. Select the frequency: **Hourly**, **Daily**, **Weekly**, or **Monthly**
 - b. Select the number of snapshots you want to keep.
 - c. Select the day, hour, and minute when the snapshot should be taken.

Schedule Snapshot Policies:

| | | | |
|---|---------------------------------|---|---|
| <input checked="" type="checkbox"/> Hourly | Number of Snapshot to Keep | Minute | |
| | <input type="text" value="12"/> | <input type="text" value="30"/> | |
| <input type="checkbox"/> Daily | Number of Snapshot to Keep | Hour | Minute |
| | <input type="text" value="0"/> | <input type="text" value="0"/> | <input type="text" value="0"/> |
| <input checked="" type="checkbox"/> Weekly | Number of Snapshot to Keep | Days | Hour Minute |
| | <input type="text" value="3"/> | <div>Sunday x</div> | <input type="text" value="0"/> <input type="text" value="0"/> |
| <input type="checkbox"/> Monthly | Number of Snapshot to Keep | | Hour Minute |
| | <input type="text" value="0"/> | <div> <input type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday </div> | <input type="text" value="0"/> <input type="text" value="0"/> |

5. Click **Add volume** or **Update volume** to save your policy settings.

Disable a snapshot policy

You can disable a snapshot policy to stop snapshots from being created for a short period of time while retaining your snapshot policy settings.

Steps

1. Open the working environment.
2. Hover over the volume and click **Edit**.
3. From the *Snapshot Policy* tab, move the enable snapshots slider to the left.

Enable automatic Snapshot copies

When disabled, Cloud Volumes Service does not create Snapshot copies of your volumes.

4. Click **Update volume**.

When you want to re-enable the snapshot policy, move the enable snapshots slider to the right and click **Update volume**.

Delete a snapshot

You can delete a snapshot from the Volumes page.

Steps

1. Open the working environment.
2. Hover over the volume and click **Delete a Snapshot copy**.
3. Select the snapshot from the drop-down list and click **Delete**.



The screenshot shows a dialog box titled "Delete a Snapshot Copy - <Volume Name>". Inside the dialog, there is a message: "This action deletes the selected Snapshot copy." Below this message, there is a label "Snapshot Name" followed by a dropdown menu. The dropdown menu currently displays the text "manually.2020-05-04_1722" and has a small downward arrow on the right. At the bottom right of the dialog box, there is a blue button labeled "Delete".

4. In the confirmation dialog box, click **Delete**.

Revert a volume from a snapshot

You can revert a volume to an earlier point in time from an existing snapshot.

When you revert a volume, the content of the snapshot overwrites the existing volume configuration. Any changes that were made to the data in the volume after the snapshot was created are lost.

Note that clients do not need to remount the volume after the revert operation.

Steps

1. Open the working environment.
2. Hover over the volume and click **Revert volume to Snapshot**.
3. Select the snapshot that you want to use to restore the existing volume from the drop-down list and click **Revert**.

Revert volume to Snapshot - <Volume Name>



This action reverts the volume to a previous state. Any data saved after the Snapshot copy was created will be lost. This action can't be reversed.

Snapshot Name

- Select a snapshot copy -



Revert

Copyright Information

Copyright © 2022 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.