



# Provision NAS storage

## ONTAP System Manager

NetApp

December 14, 2020

This PDF was generated from [https://docs.netapp.com/us-en/ontap/concept\\_nas\\_provision\\_overview.html](https://docs.netapp.com/us-en/ontap/concept_nas_provision_overview.html) on December 14, 2020. Always check docs.netapp.com for the latest.

# Table of Contents

- Provision NAS storage ..... 1
  - NAS overview ..... 1
  - Provision NAS storage for VMware datastores ..... 1
  - Provision NAS storage for home directories ..... 1
  - Provision NAS storage for Linux servers using NFS ..... 2
  - Manage access using export policies ..... 3
  - Provision NAS storage for Windows servers using SMB/CIFS ..... 3
  - Provision NAS storage for both Windows and Linux using both NFS and SMB/CIFS ..... 4
  - Secure client access with Kerberos ..... 5
  - Provide client access with name services ..... 6
  - Provision NAS storage for large file systems using FlexGroup volumes ..... 7
  - Monitor volume usage with ONTAP File System Analytics ..... 7
  - Monitor NFS active clients ..... 9
  - Improve performance for multiple clients with FlexCache ..... 10
  - Enable NAS storage ..... 11

# Provision NAS storage

## NAS overview

ONTAP enables you to serve data to Linux and Windows clients simply, securely, and efficiently.

ONTAP System Manager supports workflows for:

- Initial configuration of clusters that you intend to use for NAS file services.
- Additional volume provisioning for changing storage needs.
- Configuration and maintenance for industry-standard authentication and security facilities.

Using ONTAP System Manager, you can manage NAS services at the component level:

- Protocols – NFS, SMB/CIFS, or both (NAS multiprotocol)
- Name services – DNS, LDAP, and NIS
- Name service switch
- Kerberos security
- Exports and shares
- Qtrees
- Name mapping of users and groups

If you need to learn more about ONTAP NAS features, you can review the *Concepts* guide and *Provisioning for NAS protocols* section in the [ONTAP 9 Documentation Center](#).

## Provision NAS storage for VMware datastores

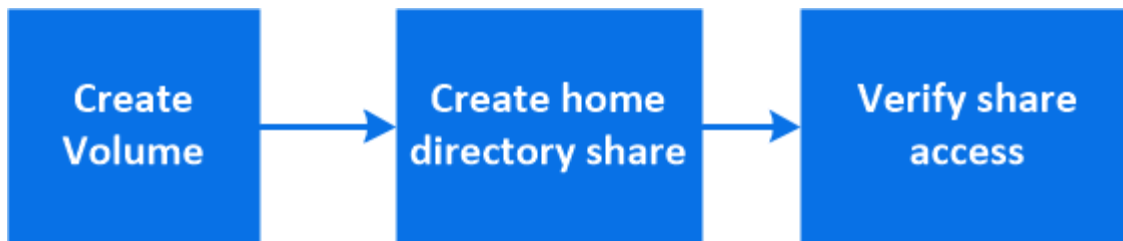
Create volumes to provide VMware datastores using the NFS protocol.

See the [NFS Configuration for ESXi using VSC Express Guide](#) for VMware datastore provisioning best practices.

## Provision NAS storage for home directories

Create volumes to provide storage for home directories using the SMB/CIFS protocol.

This procedure creates new volumes for home directories on an [existing SMB-enabled storage VM](#).



### Steps

1. In ONTAP System Manager, click **Storage** > **Volumes** and then click **Add**.
2. Click **Storage** > **Shares**, click **Add**, and select **Home Directory**.
3. On a Windows client, do the following to verify that the share is accessible.
  - a. In Windows Explorer, map a drive to the share in the following format:  
`\\_SMB_Server_Name__Share_Name_`  
  
If the share name was created with variables (%w, %d, or %u), be sure to test access with a resolved name.
  - b. On the newly created drive, create a test file, and then delete the file.

## Provision NAS storage for Linux servers using NFS

Create volumes to provide storage for Linux servers using the NFS protocol.

This procedure creates new volumes on an [existing NFS-enabled storage VM](#).



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

### Steps

1. In ONTAP System Manager, click **Storage** > **Volumes** and then click **Add**.

The default export policy grants full access to all users. You can add more restrictive rules to the export policy later.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

2. On a Linux client, do the following to verify access.
  - a. Create and mount the volume using the network interface of the storage VM.
  - b. On the newly mounted volume, create a test file, write text to it, and then delete the file.

After verifying access, you can [restrict client access with the volume's export policy](#) and set any desired UNIX ownership and permissions on the mounted volume.

# Manage access using export policies

Enable Linux client access to NFS servers by using export policies.

This procedure creates or modifies export policies for an [existing NFS-enabled storage VM](#).

## Steps

1. In ONTAP System Manager, Click **Storage > Volumes**.
2. Click an NFS-enabled volume and click **More**.
3. Click **Edit Export Policy** and then click **Select an existing policy** or **Add a new policy**.

# Provision NAS storage for Windows servers using SMB/CIFS

Create volumes to provide storage for Windows servers using the SMB/CIFS protocol.

This procedure creates new volumes on an [existing SMB-enabled storage VM](#).



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

## Steps

1. In ONTAP System Manager, click **Storage > Volumes** and then click **Add**.

The default share grants full access to all users. You can modify the Access Control List (ACL) later.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

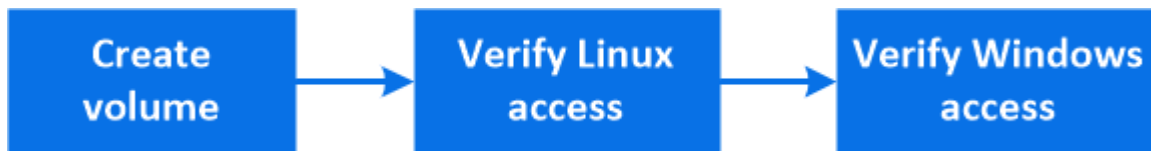
2. Switch to a Windows client to verify that the share is accessible.
  - a. In Windows Explorer, map a drive to the share in the following format:  
`\\_SMB_Server_Name__Share_Name_`
  - b. On the newly created drive, create a test file, write text to it, and then delete the file.

After verifying access, you can [restrict client access with the share ACL](#) and set any desired security properties on the mapped drive.

# Provision NAS storage for both Windows and Linux using both NFS and SMB/CIFS

Create volumes to provide storage for clients using either the NFS or SMB/CIFS protocol.

This procedure creates new volumes on an [existing storage VM enabled for both NFS and SMB protocols](#).



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

## Steps

1. In ONTAP System Manager, click **Storage > Volumes** and then click **Add**.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

2. Click **More Options** and select **Share via NFS**.

The default setting grants full access to all users. You can add more restrictive rules to the export policy later.

3. Select **Share via SMB/CIFS**.

The share is created with a default Access Control List (ACL) set to "Full Control" for the **Everyone** group. You can add restrictions to the ACL later.

4. On a Linux client, do the following to verify that the export is accessible.
  - a. Create and mount the volume using the network interface of the storage VM.
  - b. On the newly mounted volume, create a test file, write text to it, and then delete the file.
5. On a Windows client, do the following to verify that the share is accessible.
  - a. In Windows Explorer, map a drive to the share in the following format:  
`\\_SMB_Server_Name_\\Share_Name_`
  - b. On the newly created drive, create a test file, write text to it, and then delete the file.

After verifying access, you can [restrict client access with the volume's export policy](#), [restrict client access with the share ACL](#), and set any desired ownership and permissions on the exported and shared

volume.

## Secure client access with Kerberos

Enable Kerberos to secure storage access for NAS clients.

This procedure configures Kerberos on an existing storage VM enabled for [NFS](#) or [SMB](#).

Before beginning you should have configured DNS, NTP, and [LDAP](#) on the storage system.



### Steps

1. At the ONTAP command line, set UNIX permissions for the storage VM root volume.
  - a. Display the relevant permissions on the storage VM root volume: `volume show -volume root_vol_name-fields user,group,unix-permissions`

The root volume of the storage VM must have the following configuration:

Name...	Setting...
UID	root or ID 0
GID	root or ID 0
UNIX permissions	755

- b. If these values are not shown, use the `volume modify` command to update them.
2. Set user permissions for the storage VM root volume.
  - a. Display the local UNIX users: `vserver services name-service unix-user show -vserver vserver_name`

The storage VM should have the following UNIX users configured:

User name	User ID	Primary group ID
nfs	500	0
root	0	0



**Note:** The NFS user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user; see step 5.

- b. If these values are not shown, use the `vserver services name-service unix-user modify` command to update them.
3. Set group permissions for the storage VM root volume.

- a. Display the local UNIX groups: `vserver services name-service unix-group show -vserver vserver_name`

The storage VM should have the following UNIX groups configured:

Group name	Group ID
daemon	1
root	0

- b. If these values are not shown, use the `vserver services name-service unix-group modify` command to update them.
4. Switch to System Manager to configure Kerberos
5. In ONTAP System Manager, click **Storage** > **Storage VMs** and select the storage VM.
6. Click **Settings**.
7. Click  under Kerberos.
8. Click **Add** under Kerberos Realm, and complete the following sections:
  - Add Kerberos Realm  
  
Enter configuration details depending on KDC vendor.
  - Add Network Interface to Realm  
  
Click **Add** and select a network interface.
9. If desired, add mappings from Kerberos principal names to local user names.
  - a. Click **Storage** > **Storage VMs** and select the storage VM.
  - b. Click **Settings**, and then click  under **Name Mapping**.
  - c. Under **Kerberos to UNIX**, add patterns and replacements using regular expressions.

## Provide client access with name services

Enable ONTAP to look up host, user, group, or netgroup information using LDAP or NIS to authenticate NAS clients.



This procedure creates or modifies LDAP or NIS configurations on an existing storage VM enabled for [NFS](#) or [SMB](#).

For LDAP configurations, you should have the LDAP configuration details required in your environment and you should be using a default ONTAP LDAP schema.

### Steps

1. Configure the required service: click **Storage** > **Storage VMs**.



2. Select the storage VM, click **Settings**, and then click  for LDAP or NIS.
3. Include any changes in the name services switch: click  under Name Services Switch.

## Provision NAS storage for large file systems using FlexGroup volumes

A FlexGroup volume is a scalable NAS container that provides high performance along with automatic load distribution. FlexGroup volumes provide massive capacity (in petabytes), which considerably exceeds the FlexVol volume limits, without adding any management overhead.

ONTAP automatically selects the local tiers required for creating the FlexGroup volume.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

### Steps

1. Click **Storage > Volumes**.
2. Click **Add**.
3. Click **More Options** and then select **Distribute volume data across the cluster**.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

## Monitor volume usage with ONTAP File System Analytics

### File System Analytics overview

File System Analytics is a framework for collecting and displaying data about the contents of a FlexGroup or FlexVol volume.

File system analytics presents detailed information at each level of the volume's file system hierarchy, allowing you to:

- Assess capacity usage and trends
- Monitor file and directory counts
- Evaluate file activity and history

In ONTAP 9.8 and later, file system analytics can be displayed using ONTAP System Manager. You can also use ONTAP REST APIs to access the data programmatically.



Enabling file system analytics is expected to have a performance impact. Do not enable analytics if maximal performance is required in your environment. You can also disable analytics if your testing shows that the performance impact is unacceptable. When you disable analytics, previously collected data is no longer displayed for that volume.

File system analytics is not available for the following volume types:

- SnapMirror destination volumes
- SnapLock volumes
- Volumes containing LUNs
- Volumes used for SMB/CIFS audit
- Volumes transitioned from 7-mode systems
- Node root volumes (/mroot)

## Enable File System Analytics

To collect and display usage data, you must enable file system analytics. You can do so using System Manager, the ONTAP CLI, or REST APIs.

You can enable file system analytics when you create a new volume, or when you upgrade a system with volumes to ONTAP 9.8 or later. After upgrading, be sure that all upgrade processes have completed before enabling analytics.

Depending on the size and contents of the volume, enabling analytics might take some time while ONTAP processes existing data in the volume. System Manager displays progress and presents analytics data when complete. If you need more precise information about initialization progress, you can use the ONTAP CLI command `volume analytics show`.

### Steps

1. Click **Storage > Volumes**, then select the desired volume.
2. Click **Explorer**, then click **Enable Analytics** or **Disable Analytics**.

## View file system activity

After File System Analytics is enabled, by default, you can view the root directory contents of a selected volume sorted by the spaced used in each subtree

Clicking on any file system object allows you to browse the file system and to display detailed

information about each object in a directory. Information about directories can also be displayed graphically. Over time, historical data is displayed for each subtree. Space used is not sorted if there are more than 3000 records.

The file system analytics **Explorer** screen consists of three areas:

- Tree view of directories and subdirectories; expandable list showing name, size, modify history, and access history.
- Files; showing name, size, and accessed time for the object selected in the directory list.
- Active and inactive data comparison for the object selected in the directory list.

Accessed time is shown by default. However, if the volume default has been altered from the CLI, by setting the `-atime-update` option to `false` with the `volume modify` command, only last modified time is shown. For example:

- The tree view will not display the **access history**.
- The files view will be altered.
- The active/inactive data view will be based on modified time (`mtime`).

Using these displays, you can examine the following:

- File system locations consuming the most space
- Detailed information about a directory tree, including file and subdirectory count within directories and subdirectories
- File system locations that contain old data (for example, scratch, temp, or log trees)

Keep the following points in mind when interpreting file system analytics output:

- File system analytics show where and when your data is in use, not how much data is being processed. For example, large space consumption by recently accessed or modified files does not necessarily indicate high system processing loads.
- The way that the **Volume Explorer** tab calculates space consumption for file system analytics might differ from other tools. In particular, there could be significant differences compared to the consumption reported in the **Volume Overview** if the volume has storage efficiency features enabled. This is because the **Volume Explorer** tab does not include efficiency savings.

### *Steps*

1. Click **Storage > Volumes**, select the desired volume, then click **Explorer**.

## Monitor NFS active clients

Beginning with ONTAP 9.8, System Manager shows which NFS client connections are active when NFS is licensed on a cluster.

This allows you to quickly verify which NFS clients are actively connect to a storage VM, which are connected but idle, and which are disconnected.

For each NFS client IP address, the **NFS Clients** display shows:

- \* Time of last access
- \* Network interface IP address
- \* NFS connection version
- \* Storage VM name

In addition, a list of NFS clients active in the last 48 hours is also shown in the **Storage>Volumes** display and a count of NFS clients is includes in the **Dashboard** display.

#### *Step*

1. Display NFS client activity: Click **Hosts > NFS Clients**.

## Improve performance for multiple clients with FlexCache

You can use FlexCache volumes to speed up access to data or to offload traffic from heavily accessed volumes. FlexCache volumes are ideal for read-intensive workloads, especially where clients need to access the same data repeatedly.

The FlexCache volume can be on the same cluster as or on a different cluster than that of the remote volume. If the remote volume is on a different cluster, you need to have already peered the clusters and storage VMs.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

#### *Steps*

1. Click **Storage > Volumes**.
2. Click **Add**.
3. Click **More Options** and then select **Add as cache for a remote volume**.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

For any new data requests, the FlexCache volume requests the data from the remote volume and stores it. All the subsequent read requests for the data are then served directly from the FlexCache volume.

# Enable NAS storage






## Enable NAS storage for Linux servers using NFS

Modify storage VMs to enable NFS servers for serving data to Linux clients.

This procedure enables an existing storage VM. It is assumed that configuration details are available for any authentication or security services required in your environment.



### Steps

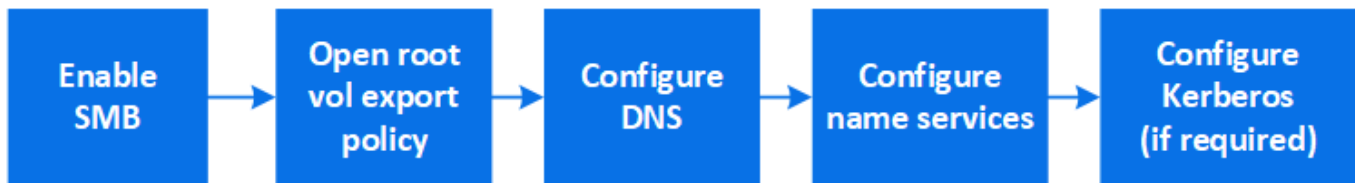
1. Enable NFS on an existing VM: click **Storage** > **Storage VMs**, select a storage VM, click **Settings**, and then click  under **NFS**.
2. Open the export policy of the storage VM root volume:
  - a. Click **Storage** > **Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
  - b. Click **Add** to add a rule.
    - Client specification = *0.0.0.0/0*
    - Access protocols = NFS
    - Access details = UNIX Read-Only
3. Configure DNS for host-name resolution: click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
4. Configure name services as required.
  - a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click for  LDAP or NIS.
  - b. Include any changes in the name services switch file: click  in the Name Services Switch tile.
5. Configure Kerberos if required:
  - a. Click **Storage** > **Storage VMs**, select the storage VM, and then click **Settings**.
  - b. Click  in the Kerberos tile and then click **Add**.

## Enable NAS storage for Windows servers using SMB/CIFS






Modify storage VMs to enable SMB servers for serving data to Windows clients.

This procedure enables an existing storage VM. It is assumed that configuration details are available

for any authentication or security services required in your environment.



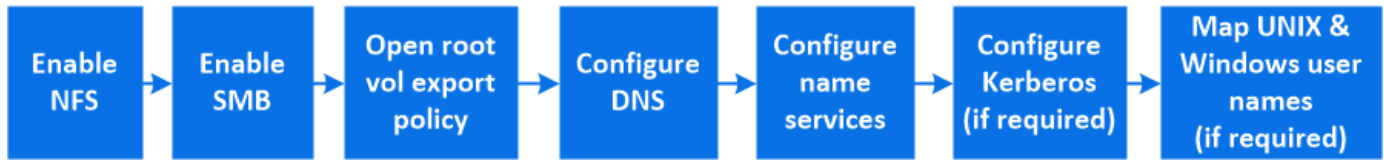
### Steps

1. Enable SMB/CIFS on an existing VM: click **Storage** > **Storage VMs**, select a storage VM, click **Settings**, and then click  under **SMB/CIFS**.
2. Open the export policy of the storage VM root volume:
  - a. Click **Storage** > **Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
  - b. Click **Add** to add a rule.
    - Client specification = **0.0.0.0/0**
    - Access protocols = SMB/CIFS
    - Access details = NTFS Read-Only
3. Configure DNS for host-name resolution:
  - a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
  - b. Switch to the DNS server and map the SMB server.
    - Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
    - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.
4. Configure name services as required
  - a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click  under **LDAP** or **NIS**.
  - b. Include any changes in the name services switch file: click  under **Name Services Switch**.
5. Configure Kerberos if required:
  - a. Click **Storage** > **Storage VMs**, select the storage VM, and then click **Settings**.
  - b. Click  under **Kerberos** and then click **Add**.








## Enable NAS storage for both Windows and Linux using both NFS and SMB/CIFS

Modify storage VMs to enable NFS and SMB servers to serve data to Linux and Windows clients.

This procedure enables an existing storage VM. It is assumed that configuration details are available for any authentication or security services required in your environment.



### Steps

1. Enable NFS on an existing VM: click **Storage** > **Storage VMs**, select a storage VM, click **Settings**, and then click  under **NFS**.
2. Enable SMB/CIFS on an existing VM: click  under **SMB/CIFS**.
3. Open the export policy of the storage VM root volume:
  - a. Click **Storage** > **Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
  - b. Click **Add** to add a rule.
    - Client specification = **0.0.0.0/0**
    - Access protocols = NFS
    - Access details = NFS Read-Only
4. Configure DNS for host-name resolution:
  - a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
  - b. When DNS configuration is complete, switch to the DNS server and map the SMB server.
    - Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
    - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.
5. Configure name services as required:
  - a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click  for LDAP or NIS.
  - b. Include any changes in the name services switch file: click  under **Name Services Switch**.
6. Configure Kerberos if required: click  in the Kerberos tile and then click **Add**.
7. Map UNIX and Windows user names if required: click  under **Name Mapping** and then click **Add**.

You should use this procedure only if your site has Windows and UNIX user accounts that do not map implicitly, which is when the lowercase version of each Windows user name matches the UNIX user name. This procedure can be done using LDAP, NIS, or local users. If you have two sets of users that do not match, you should configure name mapping.

## 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.