



Deploy SMB client-based services

ONTAP 9

NetApp
February 12, 2026

Table of Contents

Deploy SMB client-based services	1
Use offline files to allow caching of files for offline use	1
Learn about using offline files to allow caching of ONTAP SMB files for offline use	1
Learn about requirements for using offline ONTAP SMB files	2
Guidelines for deploying offline ONTAP SMB files	2
ONTAP commands to configure offline SMB file support	3
Configure offline files support on ONTAP SMB shares by using the Computer Management MMC	5
Use roaming profiles to store user profiles centrally on a SMB server associated with the SVM	6
Learn about using roaming profiles to store ONTAP SMB user profiles centrally	6
Learn about requirements for using roaming ONTAP SMB profiles	6
Configure roaming ONTAP SMB profiles through the Active Directory Users and Computers MMC	7
Use folder redirection to store data on a SMB server	7
Learn about using folder redirection to store data on ONTAP SMB servers	7
Learn about requirements for using ONTAP SMB folder redirection	8
Configure ONTAP SMB folder redirection using Windows Properties	8
Learn about accessing the ONTAP ~snapshot directory from Windows clients using SMB 2.x	9
Recover files and folders using Previous Versions	10
Learn about recovering ONTAP SMB files and folders using previous versions	10
ONTAP SMB requirements for using Microsoft Previous Versions	10
View and manage ONTAP SMB snapshot data with the Windows Previous Versions tab	11
Determine whether ONTAP SMB snapshots are available for Previous Versions use	12
Create ONTAP SMB snapshot configurations to enable Previous Versions access	13
Learn about restoring Previous Versions directories that contain ONTAP SMB junctions	14

Deploy SMB client-based services

Use offline files to allow caching of files for offline use

Learn about using offline files to allow caching of ONTAP SMB files for offline use

ONTAP supports the Microsoft Offline Files feature, or *client-side caching*, which allows files to be cached on the local host for offline use. Users can use the offline files functionality to continue working on files even when they are disconnected from the network.

You can specify whether Windows user documents and programs are automatically cached on a share or whether the files must be manually selected for caching. Manual caching is enabled by default for new shares. The files that are made available offline are synchronized to the Windows client's local disk. Synchronization occurs when network connectivity to a specific storage system share is restored.

Because offline files and folders retain the same access permissions as the version of the files and folders saved on the CIFS server, the user must have sufficient permissions on the files and folders saved on the CIFS server to perform actions on the offline files and folders.

When the user and someone else on the network make changes to the same file, the user can save the local version of the file to the network, keep the other version, or save both. If the user keeps both versions, a new file with the local user's changes is saved locally and the cached file is overwritten with changes from the version of the file saved on the CIFS server.

You can configure offline files on a share-by-share basis by using share configuration settings. You can choose one of the four offline folder configurations when you create or modify shares:

- No caching

Disables client-side caching for the share. Files and folders are not automatically cached locally on clients and users cannot choose to cache files or folders locally.

- Manual caching

Enables manual selection of files to be cached on the share. This is the default setting. By default, no files or folders are cached on the local client. Users can choose which files and folders they want to cache locally for offline use.

- Automatic document caching

Enables user documents to be automatically cached on the share. Only files and folders that are accessed are cached locally.

- Automatic program caching

Enables programs and user documents to be automatically cached on the share. Only files, folders, and programs that are accessed are cached locally. Additionally, this setting allows the client to run locally cached executables even when connected to the network.

For more information about configuring offline files on Windows servers and clients, consult the Microsoft TechNet Library.

Related information

- [Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM](#)
- [Learn about using folder redirection to store data on servers](#)
- [Learn about using BranchCache to cache share content at a branch office](#)
- [Microsoft TechNet Library: technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)

Learn about requirements for using offline ONTAP SMB files

Before you can use the Microsoft Offline Files feature with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

ONTAP version requirements

ONTAP releases support offline files.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports offline files on all versions of SMB.

Windows client requirements

The Windows client must support the offline files.

For the latest information about which Windows clients supports the Offline Files feature, see the Interoperability Matrix.

mysupport.netapp.com/matrix

Guidelines for deploying offline ONTAP SMB files

There are some important guidelines you need to understand when you deploy offline files on home directory shares that have the `showsnapshot` share property set on home directories.

If the `showsnapshot` share property is set on a home directory share that has offline files configured, Windows clients cache all of the snapshots under the `~snapshot` folder in the user's home directory.

Windows clients cache all of the snapshots under the home directory if one of more of the following is true:

- The user makes the home directory available offline from the client.

The contents of the `~snapshot` folder in the home directory is included and made available offline.

- The user configures folder redirection to redirect a folder such as `My Documents` to the root of a home directory residing on the CIFS server share.

Some Windows clients might automatically make the redirected folder available offline. If the folder is redirected to the root of the home directory, the `~snapshot` folder is included in the cached offline content.



Offline file deployments where the `~snapshot` folder is included in offline files should be avoided. The snapshots in the `~snapshot` folder contain all data on the volume at the point at which ONTAP created the snapshot. Therefore, creating an offline copy of the `~snapshot` folder consumes significant local storage on the client, consumes network bandwidth during offline files synchronization, and increases the time it takes to synchronize offline files.

ONTAP commands to configure offline SMB file support

You can configure offline files support using the ONTAP CLI by specifying one of the four offline files setting when you create SMB shares or at any time by modifying existing SMB shares. Manual offline files support is the default setting.

About this task

When configuring offline files support, you can choose one of the following four offline files settings:

Setting	Description
<code>none</code>	Disallows Windows clients from caching any files on this share.
<code>manual</code>	Allows users on Windows clients to manually select files to be cached.
<code>documents</code>	Allows Windows clients to cache user documents that are used by the user for offline access.
<code>programs</code>	Allows Windows clients to cache programs that are used by the user for offline access. Clients can use the cached program files in offline mode even if the share is available.

You can choose only one offline file setting. If you modify an offline files setting on an existing SMB share, the new offline files setting replaces the original setting. Other existing SMB share configuration settings and share properties are not removed or replaced. They remain in effect until they are explicitly removed or changed.

Steps

1. Perform the appropriate action:

If you want to configure offline files on...	Enter the command...
A new SMB share	<pre>vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none manual documents programs}</pre>

If you want to configure offline files on...	Enter the command...
An existing SMB share	<pre>vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none manual documents programs}</pre>

2. Verify that the SMB share configuration is correct: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Example

The following command creates an SMB share named “data1” with offline files set to documents:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
browsable
changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: Offline files
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: documents
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

The following command modifies an existing SMB share named “data1” by changing the offline files setting to manual and adding values for the file and directory mode creation mask:

```
cluster1::> vsserver cifs share modify -vsserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data1
-instance
```

```

                Vserver: vs1
                Share: data1
    CIFS Server NetBIOS Name: VS1
                Path: /data1
    Share Properties: oplocks
                    browsable
                    changenotify
    Symlink Properties: enable
    File Mode Creation Mask: 644
    Directory Mode Creation Mask: 777
    Share Comment: Offline files
    Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                Volume Name: -
    Offline Files: manual
    Vscan File-Operations Profile: standard
    Maximum Tree Connections on Share: 4294967295
    UNIX Group for File Create: -
```

Related information

[Add or remove share properties on existing shares](#)

Configure offline files support on ONTAP SMB shares by using the Computer Management MMC

If you want to permit users to cache files locally for offline use, you can configure offline files support by using the Computer Management MMC (Microsoft Management Console).

Steps

1. To open the MMC on your Windows server, in Windows Explorer, right-click the icon for the local computer, and then select **Manage**.
2. On the left panel, select **Computer Management**.
3. Select **Action > Connect to another computer**.

The Select Computer dialog box appears.

4. Type the name of the CIFS server or click **Browse** to locate the CIFS server.

If the name of CIFS server is the same as the storage virtual machine (SVM) host name, type the SVM

name. If the CIFS server name is different from the SVM host name, type the name of the CIFS server.

5. Click **OK**.
6. In the console tree, click **System Tools > Shared Folders**.
7. Click **Shares**.
8. In the results pane, right-click the share.
9. Click **Properties**.

Properties for the share you selected are displayed.

10. In the **General** tab, click **Offline Settings**.

The Offline Settings dialog box appears.

11. Configure the offline availability options as appropriate.
12. Click **OK**.

Use roaming profiles to store user profiles centrally on a SMB server associated with the SVM

Learn about using roaming profiles to store ONTAP SMB user profiles centrally

ONTAP supports storing Windows roaming profiles on a CIFS server associated with the storage virtual machine (SVM). Configuring user roaming profiles provides advantages to the user such as automatic resource availability regardless of where the user logs in. Roaming profiles also simplify the administration and management of user profiles.

Roaming user profiles have the following advantages:

- Automatic resource availability

A user's unique profile is automatically available when that user logs in to any computer on the network that is running Windows 8, Windows 7, Windows 2000, or Windows XP. Users do not need to create a profile on each computer they use on a network.

- Simplified computer replacement

Because all of the user's profile information is maintained separately on the network, a user's profile can be easily downloaded onto a new, replacement computer. When the user logs in to the new computer for the first time, the server copy of the user's profile is copied to the new computer.

Related information

- [Learn about using offline files to allow caching of files for offline use](#)
- [Learn about using folder redirection to store data on servers](#)

Learn about requirements for using roaming ONTAP SMB profiles

Before you can use Microsoft's roaming profiles with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

ONTAP version requirements

ONTAP support roaming profiles.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports roaming profiles on all versions of SMB.

Windows client requirements

Before a user can use the roaming profiles, the Windows client must support the feature.

For the latest information about which Windows clients support roaming profiles, see the Interoperability Matrix.

[NetApp Interoperability Matrix Tool](#)

Configure roaming ONTAP SMB profiles through the Active Directory Users and Computers MMC

If you want to automatically make a user's profile available when that user logs on to any computer on the network, you can configure roaming profiles through the Active Directory Users and Computers MMC snap-in. If you are configuring roaming profiles on Windows Server, you can use the Active Directory Administration Center.

Steps

1. On the Windows server, open the Active Directory Users and Computers MMC (or the Active Directory Administration Center on Windows servers).
2. Locate the user for which you want to configure a roaming profile.
3. Right-click the user and click **Properties**.
4. On the **Profile** tab, enter the profile path to the share where you want to store the user's roaming profile, followed by %username%.

For example, a profile path might be the following: \\vs1.example.com\profiles\%username%. The first time a user logs in, %username% is replaced with the user's name.



In the path \\vs1.example.com\profiles\%username%, profiles is the share name of a share on storage virtual machine (SVM) vs1 that has Full Control rights for Everyone.

5. Click **OK**.

Use folder redirection to store data on a SMB server

Learn about using folder redirection to store data on ONTAP SMB servers

ONTAP supports Microsoft folder redirection, which enables users or administrators to redirect the path of a local folder to a location on the CIFS server. It appears as if redirected folders are stored on the local Windows client, even though the data is stored on an SMB share.

Folder redirection is intended mostly for organizations that have already deployed home directories, and that want to maintain compatibility with their existing home directory environment.

- Documents, Desktop, and Start Menu are examples of folders that you can redirect.
- Users can redirect folders from their Windows client.
- Administrators can centrally configure and manage folder redirection by configuring GPOs in Active Directory.
- If administrators have configured roaming profiles, folder redirection enables administrators to divide user data from profile data.
- Administrators can use folder redirection and offline files together to redirect data storage for local folders to the CIFS server, while allowing users to cache the content locally.

Related information

- [Learn about using offline files to allow caching of files for offline use](#)
- [Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM](#)

Learn about requirements for using ONTAP SMB folder redirection

Before you can use Microsoft's folder redirection with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

ONTAP version requirements

ONTAP support Microsoft folder redirection.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports Microsoft's folder redirection on all versions of SMB.

Windows client requirements

Before a user can use Microsoft's folder redirection, the Windows client must support the feature.

For the latest information about which Windows clients support folder redirection, see the Interoperability Matrix.

mysupport.netapp.com/matrix

Configure ONTAP SMB folder redirection using Windows Properties

You can configure folder redirection using the Windows Properties window. The advantage to using this method is that the Windows user can configure folder redirection without assistance from the SVM administrator.

Steps

1. In Windows Explorer, right-click the folder that you want to redirect to a network share.
2. Click **Properties**.

Properties for the share you selected are displayed.

3. In the **Shortcut** tab, click **Target** and specify the path to the network location where you want to redirect the selected folder.

For example, if you want to redirect a folder to the data folder in a home directory that is mapped to Q: \, specify Q: \data as the target.

4. Click **OK**.

For more information about configuring offline folders, consult the Microsoft TechNet Library.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Learn about accessing the ONTAP ~snapshot directory from Windows clients using SMB 2.x

The method that you use to access the ~snapshot directory from Windows clients using SMB 2.x differs from the method used for SMB 1.0. You need to understand how to access the ~snapshot directory when using SMB 2.x connections to successfully access data stored in snapshots.

The SVM administrator controls whether users on Windows clients can view and access the ~snapshot directory on a share by enabling or disabling the showsnapshot share property using commands from the vservers cifs share properties families.

When the showsnapshot share property is disabled, a user on a Windows client using SMB 2.x cannot view the ~snapshot directory and cannot access snapshots within the ~snapshot directory, even when manually entering the path to the ~snapshot directory or to specific snapshots within the directory.

When the showsnapshot share property is enabled, a user on a Windows client using SMB 2.x still cannot view the ~snapshot directory either at the root of the share or within any junction or directory below the root of the share. However, after connecting to a share, the user can access the hidden ~snapshot directory by manually appending \~snapshot to the end of the share path. The hidden ~snapshot directory is accessible from two entry points:

- At the root of the share
- At every junction point in the share space

The hidden ~snapshot directory is not accessible from non-junction subdirectories within the share.

Example

With the configuration shown in the following example, a user on a Windows client with an SMB 2.x connection to the "eng" share can access the ~snapshot directory by manually appending \~snapshot to the share path at the root of the share and at every junction point in the path. The hidden ~snapshot directory is accessible from the following three paths:

- \\vs1\eng\~snapshot
- \\vs1\eng\projects1\~snapshot
- \\vs1\eng\projects2\~snapshot

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume          junction-path
-----
vs1      vs1_root        /
vs1      vs1_vol1        /eng
vs1      vs1_vol2        /eng/projects1
vs1      vs1_vol3        /eng/projects2

cluster1::> vsserver cifs share show
Vserver  Share  Path  Properties  Comment  ACL
-----
vs1      eng   /eng  oplocks     -        Everyone / Full Control
        changenotify
        browsable
        showsnapshot
```

Recover files and folders using Previous Versions

Learn about recovering ONTAP SMB files and folders using previous versions

The ability to use Microsoft Previous Versions is applicable to file systems that support snapshots in some form and have them enabled. Snapshot technology is an integral part of ONTAP. Users can recover files and folders from snapshots from their Windows client by using the Microsoft Previous Versions feature.

Previous Versions functionality provides a method for users to browse through the snapshots or to restore data from a snapshot without a storage administrator's intervention. Previous Versions is not configurable. It is always enabled. If the storage administrator has made snapshots available on a share, then the user can use Previous Versions to perform the following tasks:

- Recover files that were accidentally deleted.
- Recover from accidentally overwriting a file.
- Compare versions of file while working.

The data stored in snapshots is read-only. Users must save a copy of a file to another location to make any changes to the file. Snapshots are periodically deleted; therefore, users need to create copies of files contained in Previous Versions if they want to indefinitely retain a previous version of a file.

ONTAP SMB requirements for using Microsoft Previous Versions

Before you can use Previous Versions with your CIFS server, you need to know which versions of ONTAP and SMB, and which Windows clients, support it. You also need to know about the snapshot setting requirement.

ONTAP version requirements

Supports Previous Versions.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports Previous Versions on all versions of SMB.

Windows client requirements

Before a user can use Previous Versions to access data in snapshots, the Windows client must support the feature.

For the latest information about which Windows clients support Previous Versions, see the Interoperability Matrix.

[NetApp Interoperability Matrix Tool](#)

Requirements for snapshot settings

To use Previous Versions to access data in snapshots, an enabled snapshot policy must be associated to the volume containing the data, clients must be able to access to the snapshot data, and snapshots must exist.

View and manage ONTAP SMB snapshot data with the Windows Previous Versions tab

Users on Windows client machines can use the Previous Versions tab on the Windows Properties window to restore data stored in snapshots without needing to involve the storage virtual machine (SVM) administrator.

About this task

You can only use the Previous Versions tab to view and manage data in snapshots of data stored on the SVM if the administrator has enabled snapshots on the volume containing the share, and if the administrator configures the share to show snapshots.

Steps

1. In Windows Explorer, display the contents of the mapped drive of the data stored on the CIFS server.
2. Right-click the file or folder in the mapped network drive whose snapshots you want to view or manage.
3. Click **Properties**.

Properties for the file or folder you selected are displayed.

4. Click the **Previous Versions** tab.

A list of available snapshots of the selected file or folder is displayed in the Folder versions: box. The listed snapshots are identified by the snapshot name prefix and the creation timestamp.

5. In the **Folder versions:** box, right-click the copy of the file or folder that you want to manage.
6. Perform the appropriate action:

If you want to...	Do the following...
View data from that snapshot	Click Open .
Create a copy of data from that snapshot	Click Copy .

Data in snapshots is read-only. If you want to make modifications to files and folders listed in the Previous Versions tab, you must save a copy of the files and folders that you want to modify to a writable location and make modifications to the copies.

- After you finish managing snapshot data, close the **Properties** dialog box by clicking **OK**.

For more information about using the Previous Versions tab to view and manage snapshot data, consult the Microsoft TechNet Library.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Determine whether ONTAP SMB snapshots are available for Previous Versions use

You can view snapshots from the Previous Versions tab only if an enabled snapshot policy is applied to the volume containing the share, and if the volume configuration allows access to snapshots. Determining snapshot availability is helpful when assisting a user with Previous Versions access.

Steps

- Determine whether the volume on which the share data resides has automatic snapshots enabled and whether clients have access to snapshot directories: `volume show -vserver vservers-name -volume volume-name -fields vservers, volume, snapdir-access, snapshot-policy, snapshot-count`

The output displays what snapshot policy is associated with the volume, whether client snapshot directory access is enabled, and the number of available snapshots.

- Determine whether the associated snapshot policy is enabled: `volume snapshot policy show -policy policy-name`
- List the available snapshots: `volume snapshot show -volume volume_name`

For more information about configuring and managing snapshot policies and snapshot schedules, see [Data Protection](#).

Example

The following example displays information about snapshot policies associated with the volume named "data1" that contains the shared data and available snapshots on "data1".

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-----
vs1      data1  true                default                10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1

                Number of Is
Policy Name      Schedules Enabled Comment
-----
default          3 true      Default policy with hourly, daily &
weekly schedules.
  Schedule      Count      Prefix      SnapMirror Label
  -----
  hourly        6        hourly      -
  daily         2        daily       daily
  weekly        2        weekly      weekly

cluster1::> volume snapshot show -volume data1

                ---Blocks---
Vserver  Volume  Snapshot                State      Size  Total%  Used%
-----
vs1      data1
        weekly.2012-12-16_0015  valid      408KB    0%    1%
        daily.2012-12-22_0010  valid      420KB    0%    1%
        daily.2012-12-23_0010  valid      192KB    0%    0%
        weekly.2012-12-23_0015  valid      360KB    0%    1%
        hourly.2012-12-23_1405  valid      196KB    0%    0%
        hourly.2012-12-23_1505  valid      196KB    0%    0%
        hourly.2012-12-23_1605  valid      212KB    0%    0%
        hourly.2012-12-23_1705  valid      136KB    0%    0%
        hourly.2012-12-23_1805  valid      200KB    0%    0%
        hourly.2012-12-23_1905  valid      184KB    0%    0%
```

Related information

- [Create snapshot configurations to enable Previous Versions access](#)
- [Data protection](#)

Create ONTAP SMB snapshot configurations to enable Previous Versions access

The Previous Versions functionality is always available, provided that client access to snapshots is enabled and provided that snapshots exist. If your snapshot configuration does not meet these requirements, you can create a snapshot configuration that does.

Steps

1. If the volume containing the share to which you want to allow Previous Versions access does not have an associated snapshot policy, associate a snapshot policy to the volume and enable it by using the `volume modify` command.

Learn more about `volume modify` in the [ONTAP command reference](#).

2. Enable access to the snapshots by using the `volume modify` command to set the `-snap-dir` option to `true`.

Learn more about `volume modify` in the [ONTAP command reference](#).

3. Verify that snapshot policies are enabled and that access to snapshot directories is enabled by using the `volume show` and `volume snapshot policy show` commands.

Learn more about `volume show` and `volume snapshot policy show` in the [ONTAP command reference](#).

For more information about configuring and managing snapshot policies and snapshot schedules, see [Data Protection](#).

Related information

[Data protection](#)

Learn about restoring Previous Versions directories that contain ONTAP SMB junctions

There are certain guidelines you should keep in mind when using Previous Versions to restore folders that contain junction points.

When using Previous Versions to restore folders that have child folders that are junction points, the restore can fail with an `Access Denied` error.

You can determine whether the folder that you are attempting to restore contains a junction by using the `vol show` command with the `-parent` option. You can also use the `vserver security trace` commands to create detailed logs about file and folder access issues.

Related information

[Creating and managing data volumes in NAS namespaces](#)

Copyright information

Copyright © 2026 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.