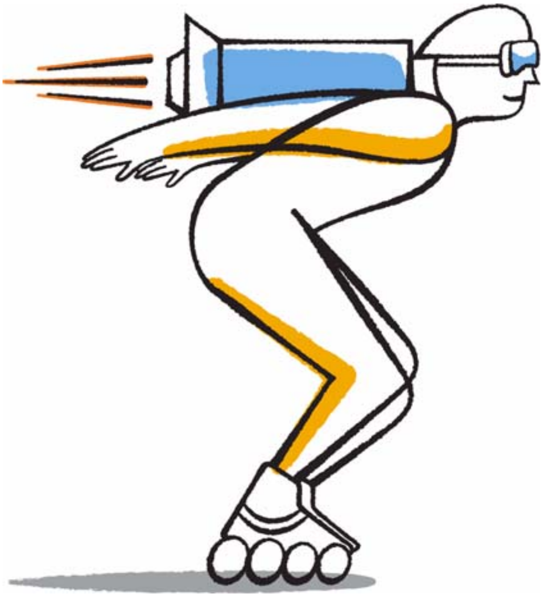
Data ONTAP® 8.1

Multi-protocol Express Guide
For 7-Mode Administrators Learning Cluster-Mode



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

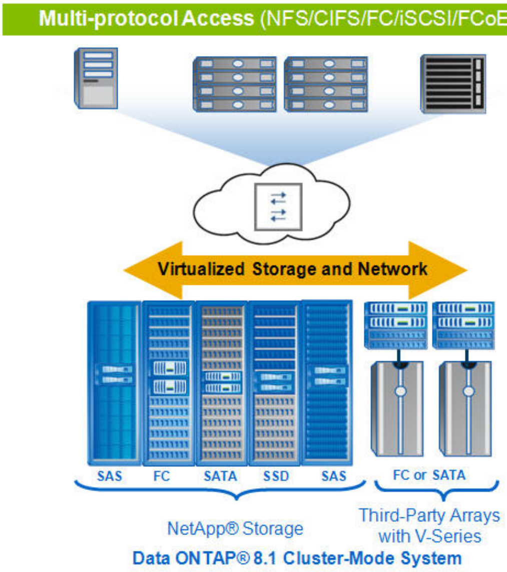
Part number: 215-07235_A0
October 2012

Contents

Deciding whether to use this guide

If you are familiar with Data ONTAP operating in 7-Mode, but now you need to understand how to use Data ONTAP operating in Cluster-Mode in both NFS and CIFS environments, you should use this guide.

The following image shows how Data ONTAP operates in environments using different protocols:


Multi-protocol Access (NFS/CIFS/FC/iSCSI/FCoE)
Virtualized Storage and Network
SAS
FC
SATA
SSD
SAS
FC or SATA
NetApp® Storage
Third-Party Arrays with V-Series
Data ONTAP® 8.1 Cluster-Mode System

This guide assumes standard software configurations and NetApp best practices, but does not provide information about all available software options and background descriptions for the tasks.

- This guide assumes that your storage system and Data ONTAP have been successfully installed and a cluster has been created.
- This guide assumes that you downloaded and are running NetApp OnCommand System Manager 2.0.2 or later for all applicable tasks. It does not include procedures using the Data ONTAP command-line interface (CLI) except when the CLI is the only way to complete a task.
- This guide assumes that you have already configured a Vserver that has both NFS and CIFS enabled. If you have not, see the *Data ONTAP CIFS Express Guide*.
- If a multi-protocol Vserver has already been created, it is likely that UNIX users, UNIX groups, and name mappings exist. In this case, you can use this guide to create additional users, groups, and name mappings or to edit existing users, groups, and name mappings.

For more background information, you should see the following documentation:

- *Data ONTAP NFSv3 Express Guide*
- *Data ONTAP CIFS Express Guide*
- *Data ONTAP Software Setup Guide for Cluster-Mode* (for new systems)
- *Data ONTAP System Administration Guide for Cluster-Mode* (for Vserver creation)
- *Data ONTAP File Access and Protocols Management Guide for Cluster-Mode* (for NFS and CIFS)
- *Data ONTAP Network Management Guide for Cluster-Mode*
- *OnCommand System Manager Help* (available both from within the product and as a PDF).

This documentation is available from the Product Documentation section of the NetApp Support Site at *support.netapp.com*.

Mode differences in multi-protocol environments

The transition from Data ONTAP operating in 7-Mode to Data ONTAP operating in Cluster-Mode affects multi-protocol environments, such as file sharing and user account access in NFS and CIFS.

The following differences affect the multi-protocol environments:

File sharing between NFS and CIFS

Data ONTAP allows NFS clients to access CIFS files and CIFS clients to access NFS files. To allow NFS and CIFS client access, you must set up both NFS and CIFS access on the Vserver. You must also configure name mappings or configure the default users.

Data ONTAP uses Windows NT File System (NTFS) security semantics to determine whether a UNIX user, on an NFS client, has access to a file in a mixed or NTFS qtree with NTFS access control lists (ACLs).

File naming conventions depend on both the network clients' operating systems and the file-sharing protocols.

User account access differences in NFS and CIFS

After setting up NFS and CIFS access, you must create user accounts to allow client access to files on a Vserver, create the necessary UNIX groups and users, and map Windows (CIFS) and UNIX (NFS) user names to each other.

These user accounts are required only if the Vserver is configured for CIFS only or is configured for NFS and CIFS. The user accounts are not mandatory if the Vserver is configured for NFS only.

File sharing between NFS and CIFS

Data ONTAP allows NFS clients to access CIFS files and CIFS clients to access NFS files. This eliminates the need to have the same data stored on two separate CIFS and NFS servers to provide access to the same data through both protocols.

To allow NFS and CIFS client access, you must set up both an NFS server and a CIFS server on the Vserver. You must also configure name mappings or the default users.

Related concepts

NFS and CIFS file naming dependencies on page 7

Related tasks

Creating a name mapping for NFS or CIFS on page 11

CIFS file access from NFS clients

Data ONTAP uses Windows NT File System (NTFS) security semantics to determine whether a UNIX user, on an NFS client, has access to a file in a mixed or NTFS qtree.

Data ONTAP determines this access information by mapping a UNIX user ID (UID) and a CIFS user (SID), and then using the CIFS credential to verify that the user has access rights to the file. A CIFS credential consists of a primary security identifier (SID), usually the user's Windows user name, and one or more group SIDs that correspond to Windows groups of which the user is a member. Data ONTAP maps the UID to the CIFS credential and enters the mapping in a credential cache for reuse.

NFS and CIFS file naming dependencies

File naming conventions depend on both the network clients' operating systems and the file-sharing protocols.

The operating system and the file-sharing protocols determine the following:

- Characters a file name can use
- Case-sensitivity of a file name

Characters a file name can use

If you are sharing a file between clients on different operating systems, you should use characters that are valid in both operating systems.

For example, if you use UNIX to create a file, don't use a colon (:) in the file name because the colon is not allowed in MS-DOS file names. Because restrictions on valid characters vary from one operating system to another, see the documentation for your client operating system for more information about prohibited characters.

Case-sensitivity of a file name

File names are case-sensitive for NFS clients and case-insensitive but case-preserving for CIFS clients.

For example, if a CIFS client creates `Spec.txt`, both CIFS and NFS clients display the file name as `Spec.txt`. However, if a CIFS user later tries to create `spec.txt`, the name is not allowed because, to the CIFS client, that name currently exists. If an NFS user later creates a file named `spec.txt`, NFS and CIFS clients display the file name differently, as follows:

- On NFS clients, you see both file names as they were created, `Spec.txt` and `spec.txt`, because file names are case-sensitive.
- On CIFS clients, you see `Spec.txt` and `Spec~1.txt`.

  Data ONTAP creates the `Spec~1.txt` file name to differentiate the two files.

Changing UNIX permissions to NTFS permissions

To manage UNIX permissions of files or folders in mixed security-style volumes or qtrees using a Windows client, you can use the Security tab on Windows clients and configure NTFS access control lists (ACLs).

About this task

You must first remove the UNIX security objects and then replace them with Windows security objects. By removing UNIX security objects and adding Windows users and groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

Steps

1. Access the Windows **Security** tab.
2. Remove the listed entries.
3. Replace the entries with the required Windows User and Group objects.
4. On the Windows User and Group objects, configure the NTFS-based ACLs.
5. If you do not want to propagate these changes to all subfolders and files, change the propagation choice.

   When you change permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files.

Creating and managing user accounts in both NFS and CIFS

After creating the NFS and CIFS servers, you must create user accounts to allow client access to files on a Vserver. You can use OnCommand System Manager to create the necessary UNIX groups and users and to map Windows (CIFS) and UNIX (NFS) users' names to each other.

About this task

The following high-level steps summarize the Vserver user account operations that you can perform in System Manager.

Steps

1. In System Manager, create a UNIX group in Vservers.

   You must create at least one group before creating a user.
2. Create UNIX users in Vservers.
3. If you do not want to map individual users between UNIX and Windows, create a default user to support authentication for users on one platform who might not be mapped on the other.
4. Map individual UNIX and Windows users to each other.

Related tasks

Creating a local UNIX group on page 9
Creating a local UNIX user for NFS or CIFS on page 10
Configuring a default Windows user on page 11
Creating a name mapping for NFS or CIFS on page 11

Creating a local UNIX group

UNIX groups are generally used as containers to simplify administration of access privileges. To support this deployment strategy in Data ONTAP, you can use OnCommand System Manager to create a local UNIX group for a Vserver. When you create UNIX users, you must assign them to a group.

Steps

1. Open System Manager and double-click your storage system name.
2. Open the **Vservers** hierarchy.
3. Select a Vserver.

4. Select **Configuration** > **Local Users and Groups** > **UNIX**.
5. Click **Add Group**.
6. Enter the **Group Name** and select the **Group ID** number.

   The name and ID are user-defined.
7. Click **Add**.

Related tasks

Creating a local UNIX user for NFS or CIFS on page 10

Creating a local UNIX user for NFS or CIFS

Many administrators create local UNIX users for system users to reduce overhead because a separate name server is not required. You can use OnCommand System Manager to create local UNIX users. A local UNIX user is a UNIX user you create on a Vserver as a UNIX name services option and that is used in the processing of name mappings.

Before you begin

You must have at least one UNIX group established.

Steps

1. Open System Manager and double-click your storage system name.
2. Open the **Vservers** hierarchy.
3. Select a Vserver.
4. Select **Configuration** > **Local Users and Groups** > **UNIX**.
5. Click the **Users** tab.
6. Click **Add User**.
7. In the view that appears, enter the user name.
8. Select a number for the User ID.
9. Select the Group Name.
10. Enter the user's full name.
11. Click **Add**.

Related tasks

Creating a local UNIX group on page 9

Configuring a default Windows user

If you want to create a generic account to use if all other mapping attempts fail for a user, you can use OnCommand System Manager to configure a default user. A default user account is also useful if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not configure a default user.

About this task

For NFS authentication, if you do not want to map each UNIX user to an individual Windows user, you can instead specify a default Windows user.

Steps

1. Open System Manager and double-click your storage system name.
2. Open the **Vservers** hierarchy.
3. Select **Configuration** > **Protocols** > **NFS**, and click **Edit**.
4. In the **Default Windows User** field, enter the user name of your default user.

   The default user can have a domain or local account, and the name and ID are user-defined.
5. Click **Save**.

Related tasks

Creating a name mapping for NFS or CIFS on page 11

Creating a name mapping for NFS or CIFS

You can use OnCommand System Manager to create name mappings for the Windows and UNIX user names to each other.

Steps

1. Open System Manager and double-click your storage system name.
2. Open the **Vservers** hierarchy.
3. Select a Vserver.
4. Select **Configuration** > **Local Users and Groups** > **Name Mapping**.
5. Click **Add**.
6. In **Add Name Mapping Entry**, select the direction of the mapping you want from the menu:
   - **Windows to UNIX** for mapping individual CIFS users to also have NFS access

- **UNIX to Windows** for mapping individual NFS users to also have CIFS access
- **Kerberos to UNIX** for mapping individual Kerberos users to also have NFS access

7. In **Position**, select the number specifying the required position in the priority list of a new mapping.
8. In **Pattern**, enter the pattern specifying the user name structure to be matched, up to 256 characters in length.
9. In **Replacement**, enter the replacement pattern, up to 256 characters in length.

   #### Example

   If you want to map a UNIX user name to Windows, you can enter `johnd` as the **Pattern** and `ENG\\John` for **Replacement**.
10. Repeat steps 4 through 9 to map all of the names on the selected Vserver.
11. Repeat all of the previous steps on a different Vserver to map those users.

Related concepts

Name mapping concepts on page 12

Related tasks

Configuring a default Windows user on page 11

Name mapping concepts

Data ONTAP goes through a number of steps when attempting to map user names. They include checking the local name mapping database and LDAP, trying the user name, and using the default user if configured.

When Data ONTAP has to obtain a UNIX name for a Windows user, it first checks the local name mapping database and/or LDAP for an existing mapping. If no mapping is found, it checks whether the lowercase Windows user name is a valid user name in the UNIX domain. If this does not work, it uses the default UNIX user provided it is configured. If the default UNIX user is not configured and it cannot obtain a mapping this way either, it returns an error.

When Data ONTAP has to obtain a Windows name for a UNIX user, it first checks the local name mapping database and/or LDAP for an existing mapping. If Data ONTAP does not find a mapping, it tries to find a Windows account that matches the UNIX name in the CIFS domain. If this does not work, it uses the default CIFS user, provided it is configured. If the default CIFS user is not configured and it cannot obtain a mapping this way either, it returns an error.

Note: You can modify the order of checking the local name mapping database or LDAP first by modifying the order of services defined by the `-nm-switch` for the Vserver.

Name mapping patterns using regular expressions

Data ONTAP keeps a set of conversion rules for each Vserver. Each rule consists of two pieces: a *pattern* and a *replacement*. You can use regular expressions to enter patterns for name mapping conversion rules.

Conversion rules use a pattern and a replacement:

- The pattern is a UNIX-style regular expression.
- The replacement is a string containing escape sequences representing subexpressions from the pattern.

As an example, the following rule converts the CIFS user named jones in the domain named ENG into the UNIX user named jones:

Pattern	**Replacement**
ENG\\jones	jones

The backslash is a special character in regular expressions and must be used or escaped with another backslash.

Regular expressions are not case-sensitive when mapping from Windows to UNIX. However, they are case-sensitive for Kerberos-to-UNIX and UNIX-to-Windows mappings.

For details about regular expressions, see the *OnCommand System Manager Help* in the product or on the NetApp Support Site at *support.netapp.com*, your UNIX system administration documentation, or the online UNIX documentation for `regex`.

NFS client authentication

NFS clients can access your Vserver using the NFS protocol provided that Data ONTAP can properly authenticate the user.

When an NFS client connects to the Vserver, Data ONTAP obtains the UNIX credentials for the user by checking different name services, depending on the name services configuration of the Vserver. The options are local UNIX accounts, NIS domains, and LDAP domains. At least one of them must be configured so that Data ONTAP can successfully authorize the user. You can specify multiple name services and the order in which they are searched.

In a pure NFS environment with UNIX volume security styles, this configuration is sufficient to authenticate a user connecting from an NFS client and provide the proper file access.

If you are using mixed or NTFS volume security styles, Data ONTAP must obtain a CIFS user name for the UNIX user for authentication with a Windows domain controller. This can happen either by mapping individual users using local UNIX accounts or LDAP domains, or by using a default CIFS user instead. You can specify which name services are searched in which order, or specify a default CIFS user.

CIFS concepts

CIFS clients can access files on a Vserver using the CIFS protocol provided Data ONTAP can properly authenticate the user.

When a CIFS client connects to a Vserver, Data ONTAP authenticates the user with a Windows domain controller. Data ONTAP uses two methods to obtain the domain controllers to use for authentication:

- It queries DNS servers in the domain that the Vserver is configured to use for domain controller information.
- It queries a list of preferred domain controllers you can optionally specify.

Next, Data ONTAP must obtain UNIX credentials for the user. It does this by using mapping rules on the Vserver or a LDAP server, or by using a default UNIX user instead. You can specify for a Vserver which mapping services are searched in which order, or specify a default UNIX user.

Data ONTAP then checks different name services for UNIX credentials for the user, depending on the name services configuration of a Vserver. The options are local UNIX accounts, NIS domains, and LDAP domains. You must configure at least one of them so Data ONTAP can successfully authorize the user. You can specify multiple name services and the order in which they are searched.

Where to find additional information

There are additional documents and tools to help you learn how to do more advanced configuration of your multi-protocol storage system.

Express Guides

Data ONTAP NFSv3 Express Guide	Describes how to set up NFSv3 access for clients in the Cluster-Mode environment. It includes information to help administrators who are familiar with the 7-Mode environment to perform these tasks in the Cluster-Mode environment.
Data ONTAP CIFS Express Guide	Describes how to set up CIFS access for clients in the Cluster-Mode environment. It includes information to help administrators who are familiar with the 7-Mode environment to perform these tasks in the Cluster-Mode environment.

Documentation references

OnCommand System Manager Help	Describes how to use OnCommand System Manager to complete typical tasks. Available both from within the product and as a PDF download.
Data ONTAP 7-Mode to Cluster-Mode Command Map	Provides a mapping of 7-Mode commands to Cluster-Mode commands.
Data ONTAP File Access and Protocols Management Guide for Cluster-Mode	Describes how to manage file access on NetApp systems with CIFS and NFS protocols.

This documentation is available from the Product Documentation section of the NetApp Support Site at *support.netapp.com*.

Tool references

The following tool can help you monitor and manage your storage system. The tool is available from the NetApp Support Site.

Interoperability Matrix Tool (IMT)	Lists supported combinations of hardware components, software versions, firmware, and drivers.

Copyright information

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, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the web at *www.ibm.com/legal/copytrade.shtml*.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index