IBM System Storage N series

Clustered Data ONTAP 8.2 Multiprotocol File Access Express Guide

SC27-6408-00

Contents

Preface

About this guide

This document applies to IBM N series systems running Data ONTAP, including systems with gateway functionality. If the terms *Cluster-Mode* or *clustered Data ONTAP* are used in this document, they refer to the Data ONTAP features and functionality designed for clusters, which are different from 7-Mode and prior Data ONTAP 7.1, 7.2, and 7.3 release families.

In this document, the term *gateway* describes IBM N series storage systems that have been ordered with gateway functionality. Gateways support various types of storage, and they are used with third-party disk storage systems—for example, disk storage systems from IBM, HP®, Hitachi Data Systems®, and EMC®. In this case, disk storage for customer data and the RAID controller functionality is provided by the back-end disk storage system. A gateway might also be used with disk storage expansion units specifically designed for the IBM N series models.

The term *filer* describes IBM N series storage systems that either contain internal disk storage or attach to disk storage expansion units specifically designed for the IBM N series storage systems. Filer storage systems do not support using third-party disk storage systems.

Supported features

IBM System Storage N series storage systems are driven by NetApp Data ONTAP software. Some features described in the product software documentation are neither offered nor supported by IBM. Please contact your local IBM representative or reseller for further details.

Information about supported features can also be found on the N series support website (accessed and navigated as described in Websites).

Websites

IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. The following web pages provide N series information:

- A listing of currently available N series products and features can be found at the following web page:

  www.ibm.com/storage/nas/
- The IBM System Storage N series support website requires users to register in order to obtain access to N series support content on the web. To understand how the N series support web content is organized and navigated, and to access the N series support website, refer to the following publicly accessible web page:

  www.ibm.com/storage/support/nseries/

  This web page also provides links to AutoSupport information as well as other important N series product resources.
- IBM System Storage N series products attach to a variety of servers and operating systems. To determine the latest supported attachments, go to the IBM N series interoperability matrix at the following web page:

www.ibm.com/systems/storage/network/interophome.html

- For the latest N series hardware product documentation, including planning, installation and setup, and hardware monitoring, service and diagnostics, see the IBM N series Information Center at the following web page:

  publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Getting information, help, and service

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your IBM N series product, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure they are connected.
- Check the power switches to make sure the system is turned on.
- Use the troubleshooting information in your system documentation and use the diagnostic tools that come with your system.
- Refer to the N series support website (accessed and navigated as described in Websites) for information on known problems and limitations.

Using the documentation

The latest versions of N series software documentation, including Data ONTAP and other software products, are available on the N series support website (accessed and navigated as described in Websites).

Current N series hardware product documentation is shipped with your hardware product in printed documents or as PDF files on a documentation CD. For the latest N series hardware product documentation PDFs, go to the N series support website.

Hardware documentation, including planning, installation and setup, and hardware monitoring, service, and diagnostics, is also provided in an IBM N series Information Center at the following web page:

publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Hardware service and support

You can receive hardware service through IBM Integrated Technology Services. Visit the following web page for support telephone numbers:

www.ibm.com/planetwide/

Firmware updates

IBM N series product firmware is embedded in Data ONTAP. As with all devices, ensure that you run the latest level of firmware. Any firmware updates are posted to the N series support website (accessed and navigated as described in Websites).

Note: If you do not see new firmware updates on the N series support website, you are running the latest level of firmware.

Verify that the latest level of firmware is installed on your machine before contacting IBM for technical support.

How to send your comments

Your feedback helps us to provide the most accurate and high-quality information. If you have comments or suggestions for improving this document, please send them by email to starpubs@us.ibm.com.

Be sure to include the following:

- Exact publication title
- Publication form number (for example, GC26-1234-02)
- Page, table, or illustration numbers
- A detailed description of any information that should be changed

Deciding whether to use this guide

This guide describes how to set up multiprotocol file access for UNIX and Windows clients when the security style of the volume is either NTFS or UNIX. It provides instructions on how to provision storage, create NTFS or UNIX security-style volumes, create shares and exports to the provisioned volumes, and then secure access to the files and folders by configuring NTFS or UNIX mode permissions.

This guide follows IBM best practices, and uses OnCommand System Manager to complete tasks when possible. You should use this guide if you do not want information about all the available options or a lot of conceptual background for the tasks.

This guide is based on the following assumptions:

- You have already created the CIFS and NFS servers for the Vserver on which you want to create SMB shares and NFS exports.

  For more information, see the *Data ONTAP Multiprotocol Server Configuration Express Guide*.
- At least one data LIF for the Vserver on which the NFS and CIFS servers are configured exists and is reachable by clients needing to access data.
- The cluster time is being synchronized with an NTP server.
- You have downloaded and are running System Manager 3.0 or later, and you have made a connection to the cluster that contains the Vserver.
- DNS is configured on the Vserver.
- DNS entries on the DNS server exist that map the CIFS server name to existing data LIFs used by the CIFS server.
- A network path from the CIFS server to the Active Directory domain controllers exists.
- Name mapping between Windows and UNIX users has been configured and validated.

  For more information, see the topic "Mapping UNIX and Windows user names" in the *Data ONTAP Multiprotocol Server Configuration Express Guide*.

If these assumptions are not correct for your installation, or if you want more conceptual background information, you should see the following documentation instead:

- *Clustered Data ONTAP System Administration Guide for Cluster Administrators* (for Vserver creation)
- *Clustered Data ONTAP Physical Storage Management Guide* (for aggregate creation)
- *Clustered Data ONTAP Logical Storage Management Guide* (for volume creation)
- *Clustered Data ONTAP File Access and Protocols Management Guide* (for NFSv3, NFSv4, and SMB)
- *Clustered Data ONTAP Network Management Guide* (for LIF management)
- *OnCommand System Manager Help* (available within the product)

The procedure in this Express Guide configures Multiprotocol access to NTFS or UNIX security-style volumes. If you want to configure another type of access, the following Express Guides are available:

- *NFSv3 File Access Express Guide*
  Configure NFS access to UNIX security-style volumes.
- *SMB File Access Express Guide*
  Configure SMB access to NTFS security-style volumes.

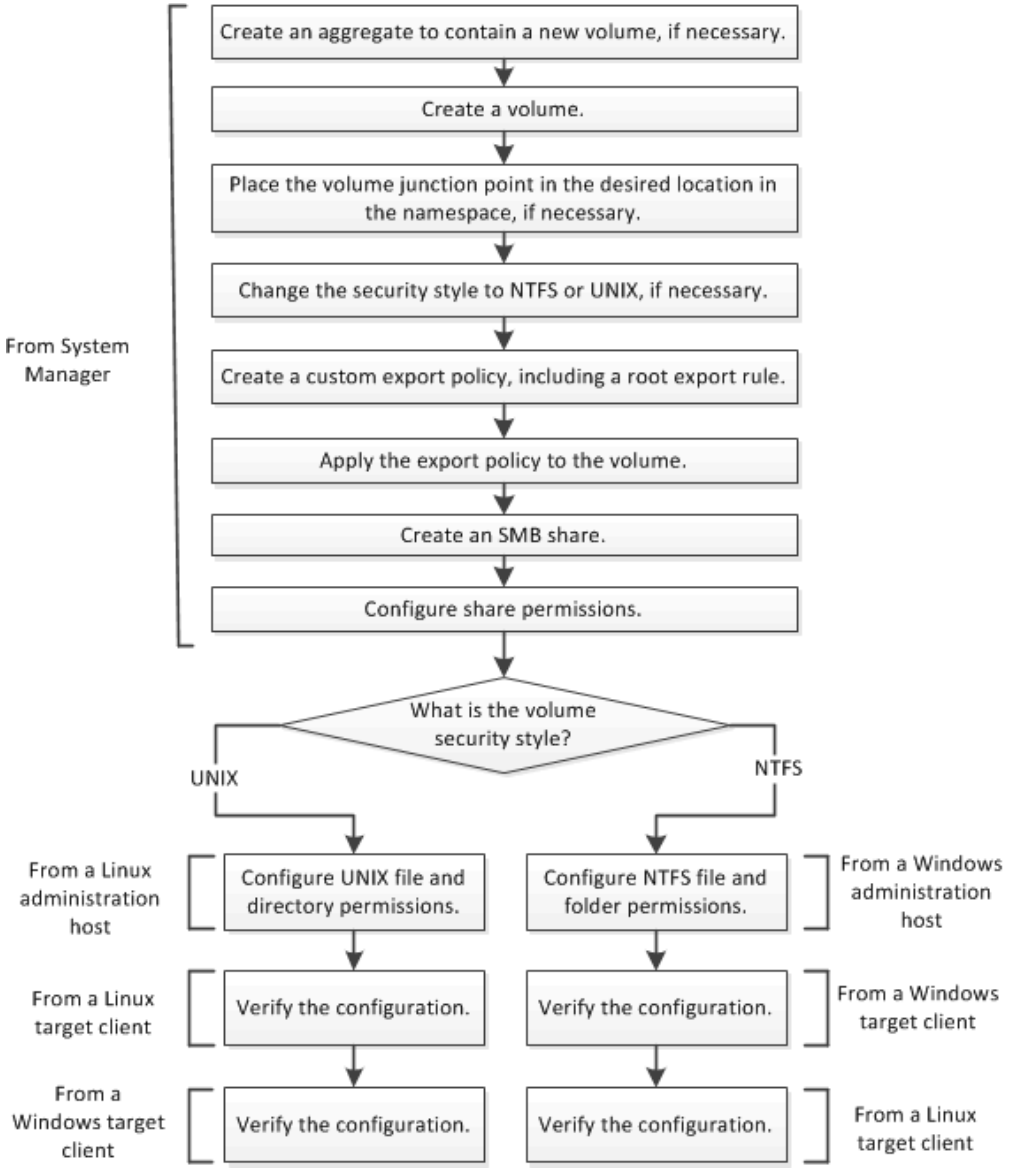
This documentation is available on the IBM N series support website (accessed and navigated as described in Websites).

Related information:

IBM N series support website: www.ibm.com/storage/support/nseries

Multiprotocol file access configuration workflow

Configuring multiprotocol file access involves creating an aggregate, creating a volume, placing the volume in the desired location in the namespace, changing the volume security style if necessary, creating a share and configuring share permissions, exporting the volume, and configuring NTFS file and folder permissions or UNIX file and directory permissions. You can then test SMB and NFSv3 file access.



Creating an aggregate

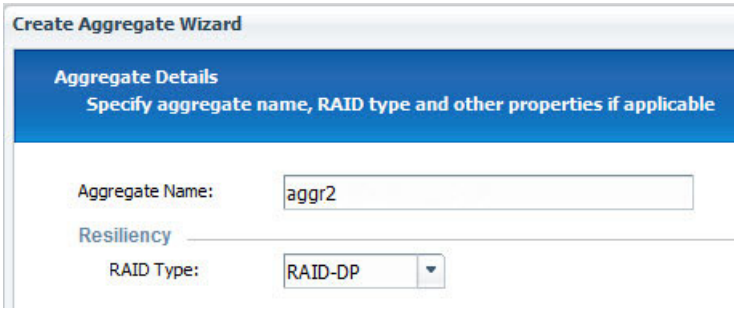
You create an aggregate to provide storage to one or more FlexVol volumes. Aggregates are made up of physical storage objects, such as HDDs and SSDs.

About this task

This procedure is performed using System Manager.

Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand either the **Cluster** or the **Nodes** hierarchy in the left navigation pane.
3. In the navigation pane, click **Storage** > **Aggregates**.
4. Click **Create**.
5. In the Create Aggregate wizard, click **Next**.
6. Optional: If you want to change the default name, specify a new name, such as `aggr2`. The default aggregate name ends in a date and time stamp.



7. Accept the default value for **RAID Type**, and click **Next**. You can change the RAID type later if necessary.
8. In the Aggregate Details page, click **Select disks**.
9. In the Change Disk Selection page, select the node on which you want to create the aggregate, specify at least 5 disks in the **Number of capacity disks to use** field, and click **Save and Close**.
10. Click **Create**.
11. Click **Finish**.

Results

The aggregate is created with the specified configuration and added to the list of aggregates in the Aggregates window.

Creating a volume

You must create a FlexVol volume to contain your data. Data must not be stored in the root volume of the Vserver.

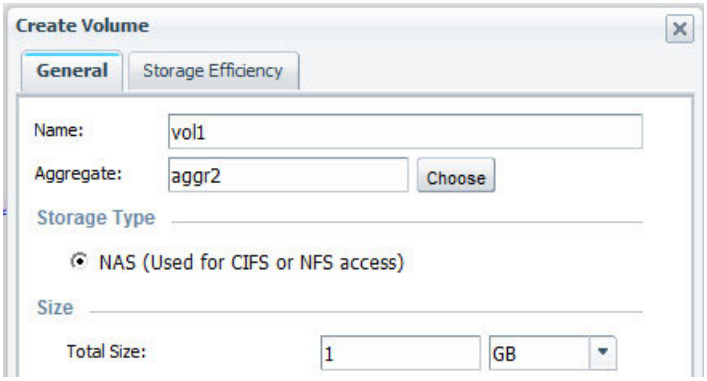
About this task

This procedure is performed using System Manager.

Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver and click **Storage** > **Volumes**.
4. Click **Create**. The Create Volume dialog box is displayed.

5. If you want to change the default name, specify a new name, such as `vol1`. By default, the volume name ends in a date and time stamp.
6. Select the aggregate that you created earlier for the volume.
7. Specify the size of the volume.



8. Accept the default value for the Snapshot reserve.

   The default space reserved for Snapshot copies is five percent for NAS volumes.
9. Ensure that Storage Type is set to **NAS**.
10. Click **Create**. The volume inherits the security style of the Vserver root volume.
11. In the Volume window, verify that the new volume is in the list.

Modifying the junction point of the new volume

When a volume is created in System Manager, it is mounted by default at the root volume using the volume name as the junction point. You can modify the junction point of the new volume if required by your storage architecture.

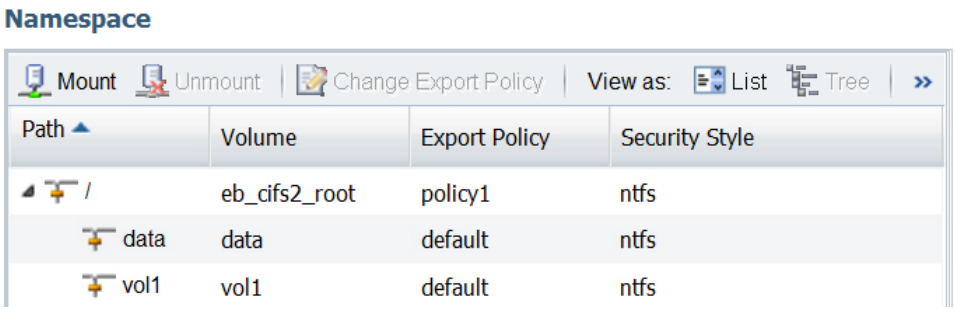
About this task

You must first unmount the volume from the current junction point and then remount it at the new junction point at the desired location within the Vserver namespace.

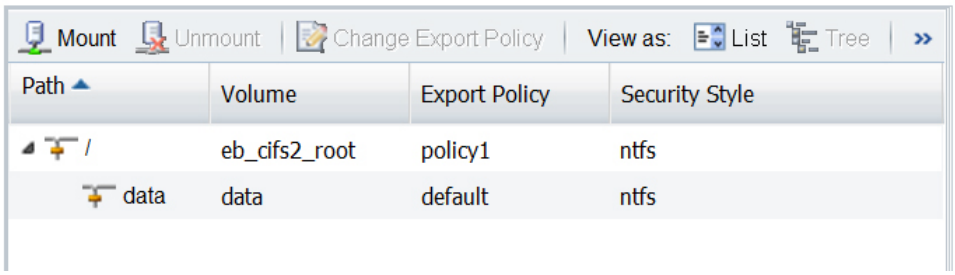
When you mount the volume to a junction point within your namespace, you specify a junction name and a junction path. The junction name is appended to the junction path to become the mount path. You use the mount path when configuring SMB shares and NFS exports.

Procedure

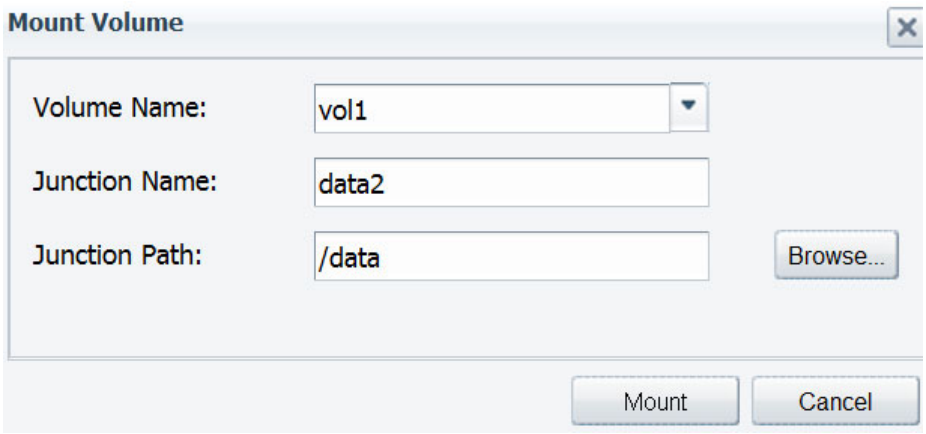
1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver, and then click **Storage** > **Namespace**. The junction path for each volume is displayed in the Namespace window.



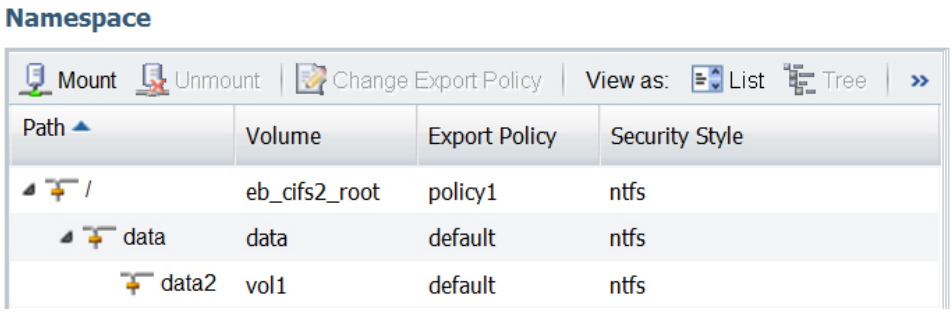
4. Select the volume that needs to be unmounted, and then click **Unmount**. The **Unmount Volume** box opens.
5. Select the confirmation check box, and then click **Unmount**. The volume is removed from the list of mounted volumes.



6. Click **Mount**.
7. In the **Mount Volume** box, specify the following details:
   a. Select the volume that you want to mount.
   b. If you want to change the default junction name, specify a new junction name.
   c. Click **Browse**, select the junction path on which you want the volume mounted, and then click **OK**.



8. Click **Mount**.
9. Verify the new junction path in the Namespace window.

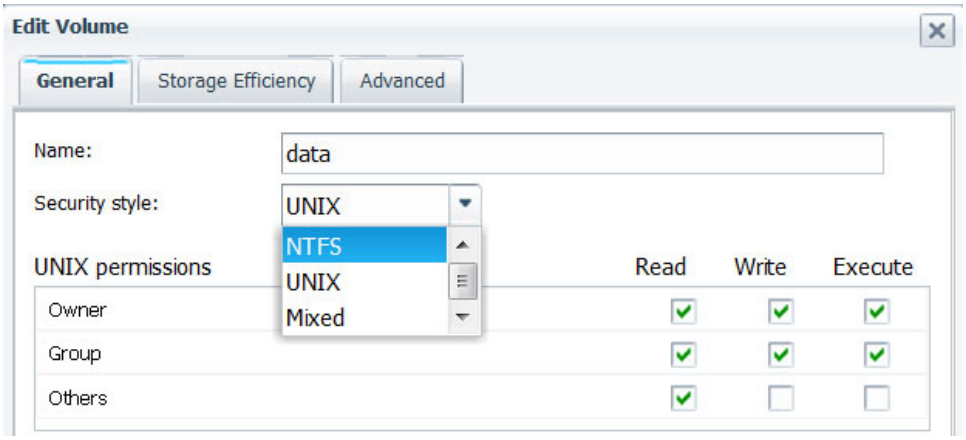


Changing the security style of the new volume

When a volume is created in System Manager, it inherits the security style of the Vserver root volume. You should check the security style and change it to NTFS or UNIX if necessary.

Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver, and then click **Storage** > **Volumes**.
4. Select the volume you just created, and then click **Edit**.
5. Select the desired security style.



6. Click **Save and Close** to save your changes, and then close the dialog box.

Creating an export policy in System Manager

Export policies contain a set of rules to specify the access that clients have to volumes in a Vserver. You must create an export policy for your new volume; otherwise, the new volume inherits the Vserver default export policy.

Before you begin

The Vserver default export policy must include a rule that allows all clients access through NFSv3. Without such a rule, all NFS clients are denied access to the Vserver and its volumes, regardless of the export policies on volumes mounted on the root volume.

For more information, see the topic "Opening the NFS export policy to all clients" in the *Data ONTAP Multiprotocol Server Configuration Express Guide*.

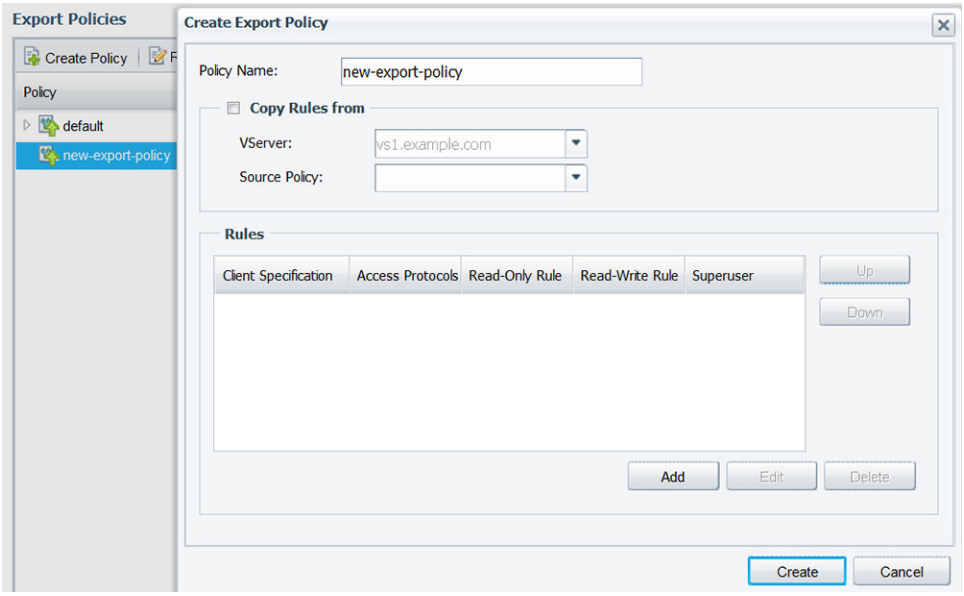
About this task

- This procedure creates rules for an administration host with superuser access and for a group of clients with read/write access.

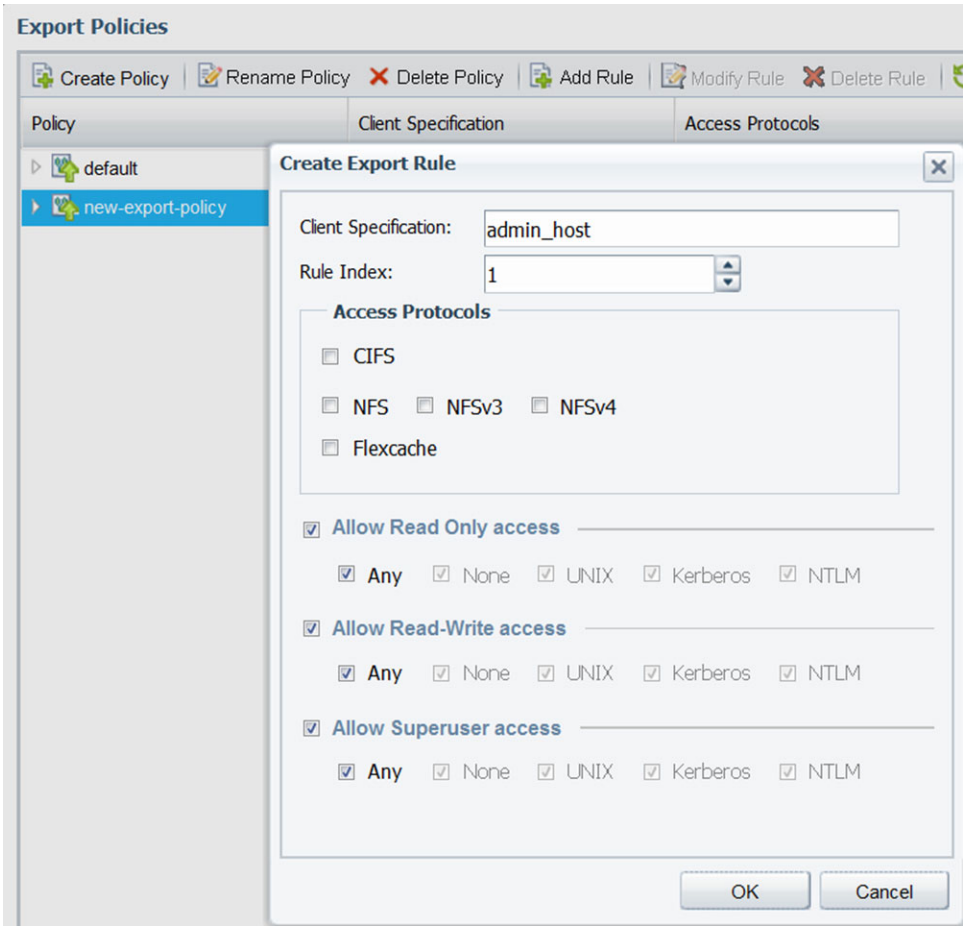
  You can create additional rules for the policy at any time.
- For more information about client specification options, see System Manager Online Help for the Export Policies screen (by clicking **? Help**).
- For more information about access and security types, and about export rules in general, see "How export rules work" in the *Clustered Data ONTAP File Access and Protocols Management Guide* and the man page for the **vserver export-policy rule create** command.

Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver, and then click **Policies** > **Export Policies**.
4. Click **Create Policy**, and then specify a policy name.

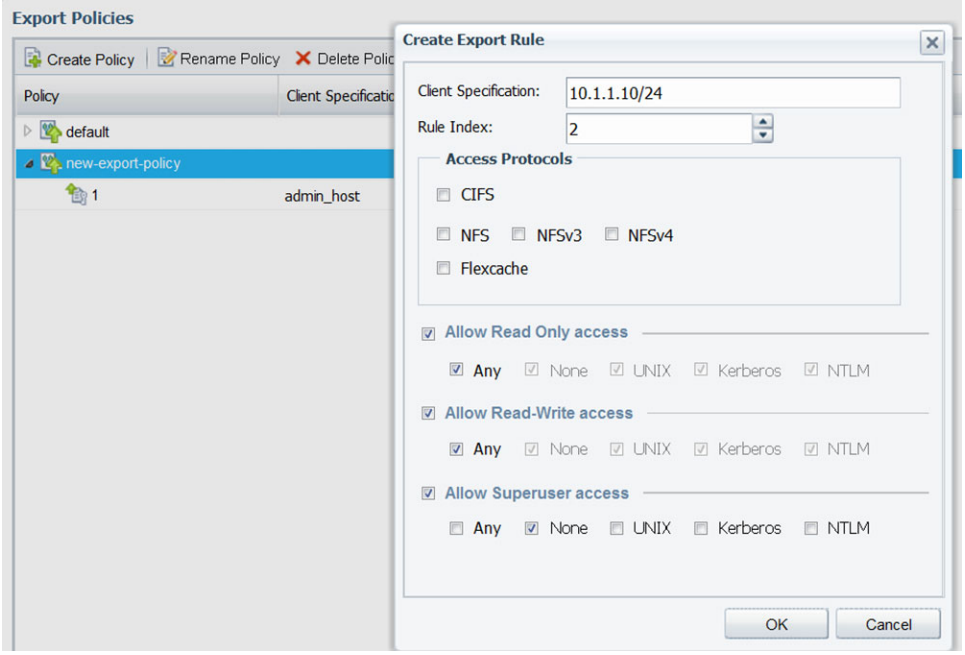


5. Select the new policy, and then click **Add Rule** to add the first export rule. In the Create Export Rule dialog box, perform the following steps:
   a. Specify the client (or clients) from which the exported volume will be administered.
   b. Select **1** for the **Rule Index**.
   c. Leave all the access protocols unselected; doing so allows access to all protocols. It is not necessary to specify NFSv3.
   d. Select **Any** for each access type.
   e. Click **OK**.



The first rule is added to the export policy.

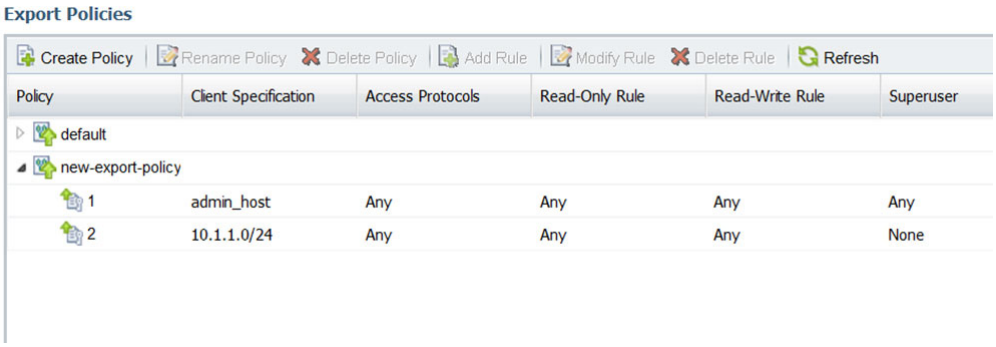
6. Select the new policy, and then click **Add Rule** to add the first export rule. In the Create Export Rule dialog box, perform the following steps:
   a. Specify the client (or clients) that will access the exported volume. This example matches a range of IP addresses with a subnet mask expressed as a number of bits.
   b. Select **2** for the **Rule Index**.
   c. Leave all the access protocols unselected; doing so allows access to all protocols. It is not necessary to specify NFSv3.
   d. Select **Any** for Read-Only and Write-Only access.
   e. Deselect **Any**, and then select **None** for Superuser access.
   f. Click **OK**.



The second rule is added to the export policy.

Results

A new export policy is created with two rules.

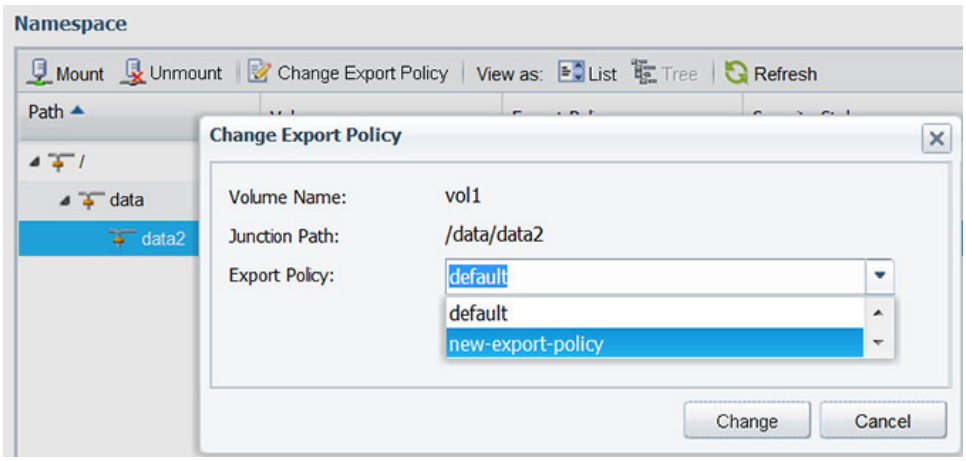


Applying export policies to volumes

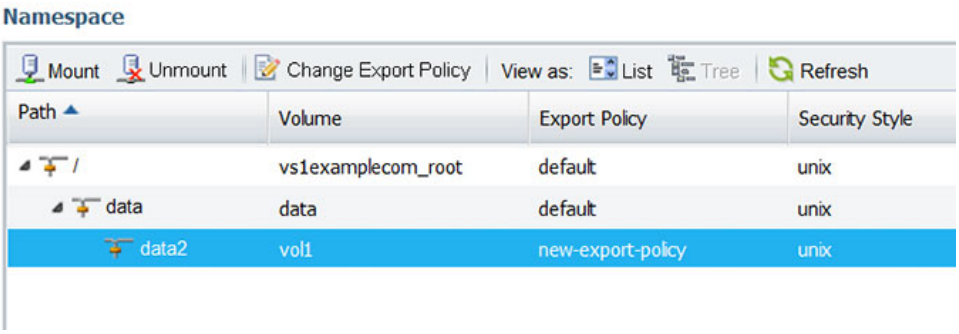
When a volume is created, it automatically inherits the default export policy of the root volume of the Vserver. This procedure describes how to apply your customized export policy.

Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver, and then click **Storage** > **Namespace**.
4. Select the volume, and then click **Change Export Policy**.
5. Select the export policy, and then click **Change**.



6. Verify that the Export Policy column in the Namespace window displays the export policy that you applied to the volume.



Results

The default export policy is replaced with your new custom policy.

Creating an SMB share

Before SMB clients can access a volume, you must create an SMB share on the volume.

About this task

This procedure is performed using System Manager.

Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver and click **Storage** > **Shares**.
4. Click **Create Share**.
5. Click **Browse** and select the volume that you created earlier.
6. Specify a name for the new share.
7. Provide a description for the share and click **Create**.

Results

The share is created with the access permissions set to Full Control for the Everyone group. You can modify the share permissions later if required.

Modifying the access control list of CIFS shares

If the default access control list (ACL) for CIFS shares does not meet your requirements, you can modify the ACLs for each share.

About this task

By default, CIFS shares are created with access permissions that permit Full Control for Everyone. You can modify these permissions to be more restrictive, or leave the access controls unrestricted and modify the NTFS file and folder permissions instead.

Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver and click **Storage** > **Shares**.
4. Select the share whose access you want to change, and click **Edit**.
5. In the Permissions tab, click **Add**.
6. Enter the name of a User or Group defined in the Windows Active Directory domain that includes the Vserver.
7. With the new user or group selected, select the permissions that you require, and click **Save**.
8. Verify that the updated share access permission is listed in the Share Access Control window.

What to do next

Depending on the security style of the new volume, complete one of the following tasks:

- Controlling access to files using UNIX permissions
- Modifying NTFS file permissions

Controlling access to files using UNIX permissions

To make the new data volume available to clients, you must mount the exported volume as root, change the owner and group, and set appropriate access to directories and files using UNIX file permissions. You can verify the new settings from the cluster.

Before you begin

- You must have the login information for the root user.
- You must have the junction path of the volume that you created.

  In these examples, /data/data2 is the junction path to the new volume named vol1.
- You must have access to the administration host identified in the first export rule for the task Creating an export policy in System Manager.

- You must have the IP address of the data LIF for the Vserver that contains the new volume.

  The IP address of the data LIF can be found in System Manager under **Vservers** > **Configuration** > **Network Interfaces**. Alternatively, you can provide a host name that is mapped to the data LIF's IP address in the DNS server.

Procedure

1. Log in as the root user to the administration host.
2. Create and mount a new directory:
   a. Change the directory to the `/mnt` directory:
      `cd /mnt/`
   b. Create a mount directory for the new volume:
      `mkdir /mnt/test1`
   c. Mount the volume at this new directory:
      `mount -t nfs -o nfsvers=3,hard IPAddress:junction_path /mnt/test1`
      If you mapped an entry for the volume name in the DNS server, you can use that name instead of *IPAddress*.

   The following commands create a directory named `test1`, mount the vol1 volume at the 192.0.2.130 IP address to the `test1 /mnt` directory, and change to the new `test1` directory:

```
host# cd /mnt
host# mkdir /mnt/test1
host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/data/data2 /mnt/test1
```

3. Update UNIX ownership and permissions in the new directory:
   a. Display the directory information:
      `ls –ld /mnt/test1`
      You should see the default export permissions for the volume:

```
host# ls -ld /mnt/test1
drwxrw-rw- 1 root root 2453 Sep 25 2013 /mnt/test1
```

   b. Change the volume's owner and group to desired values. The default values are usually **root** and **root**, or something similar, which will not permit access to regular UNIX users. You must specify an owner and group that are included in an identity store that is accessible to both the client and the Vserver. The following command changes the owner and group:
      `chown gouldg:engr /mnt/test1`
   c. Adjust the file permissions for your users and groups if the default values are not appropriate. To enable execute permission for the group but restrict others to read-only:
      `chmod 774 mnt/test1`
   d. Verify that the new settings are correct:
      `ls –ld /mnt/test1`
      You should see the new owner, group, and permissions settings:

```
host# ls -ld /mnt/test1
drwxrwxr-- 1 gouldg engr 2453 Sep 25 2013 /mnt/test1
```

4. At the CLI prompt of the system containing the new volume, verify that the updates you made on the client system are visible to the Vserver:
   `cluster1::> vserver security file-directory show -vserver VserverName -path /data/vol1`
   You should see the changes you made from the client, where the UNIX user

and group IDs (UID and GID) correspond to the names you entered with the **chown** command, in a display similar to the following:

```
cluster1::> vserver security file-directory show -vserver vs0 -path /data/data2
                Vserver: vs0
              File Path: /data/data2
      Security Style: unix
     Effective Style: unix
      DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 101
       Unix Group Id: 110
      Unix Mode Bits: 774
Unix Mode Bits in Text: rwxrwxr--
               ACLs: -
```

What to do next

Verify multiprotocol access to this volume by testing client connections.

- Testing NFSv3 access from a UNIX client
- Testing SMB access from a Windows client

Modifying NTFS file permissions

You can control access to folders and files on the SMB share using NTFS file permissions.

Before you begin

You must be logged in as a Windows user that is authenticated to the Active Directory domain that includes the Vserver. This user must have sufficient administrative rights to manage NTFS permissions for files and folders on the mapped drive.

Procedure

1. On a Windows client, use Windows Explorer to map a drive to the CIFS server name followed by the name of share that you created. If the CIFS server is named vs0.example.com and the share is named Test, you should enter the following:

   `\\vs0.example.com\Test`
2. Adjust the NTFS permissions for the drive, or a file or folder that you create on the drive.
   a. Right-click the drive, folder, or file, and then select **Properties**.
   b. Select the Security tab, and adjust the security settings for the groups and users as required.
3. Remove the drive mapping by selecting **Tools** > **Disconnect network drive**.

What to do next

Verify multiprotocol access to this volume by testing client connections.

- Testing SMB access from a Windows client
- Testing NFSv3 access from a UNIX client

Testing NFSv3 access from a UNIX client

You should verify that you have configured NFSv3 correctly by using a UNIX client to access the exported volume and write data to the file system.

Before you begin

- You must be logged in to a client that you specified as having read/write privileges in Creating an export policy in System Manager.
- You must have the junction path of the volume that you created.

  In these examples, /data/data2 is the junction path to the new volume named vol1.
- You must have the IP address of the data LIF for the Vserver that contains the new volume *or* a name for the exported volume that is mapped to the data LIF's IP address in the DNS server.

Procedure

1. As root, log in to a client system that is configured for NFS access.
2. As root, create and mount a new folder using the IP address of the Vserver:
   a. Change the directory to the `/mnt` directory:
      `cd /mnt`
   b. Create a new mount directory:
      `mkdir /mnt/test1`
   c. Mount the volume at this new directory:
      `mount -t nfs -o nfsvers=3,hard IPAddress:/junction_path /mnt/test1`

   The following commands create a directory named `test1`, mount the vol1 volume at the 192.0.2.130 IP address to the `/mnt/test1` directory, and change to the new `test1` directory:

```
host# cd /mnt
host# mkdir /mnt/test1
host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/data/data2 /mnt/test1
```

3. As a regular UNIX user, create a new file, verify that it exists, and write text to it:
   a. Switch to a regular UNIX user:
      `su user_name`
   b. Change the directory to the new folder:
      `cd test1`
   c. Create a test file:
      `touch filename`
   d. Verify that the file exists:
      `ls -l filename`
   e. Write text to the test file:
      `cat >filename`
      After entering the command, type some text, then press Ctrl-D.
   f. Display the content of the test file:
      `cat filename`
   g. Remove the test file:
      `rm -r filename`
   h. Return to the parent directory:
      `cd ..`

```
host# su hewitta
host$ cd test1
host$ touch myfile1
host$ ls -l myfile1
-rwxrwxr-- 1 hewitta eng 0 Sep 25 12:34 myfile1
host$ cat >myfile1
This text inside the first file
host$ cat myfile1
This text inside the first file
host$ rm -r myfile1
host$ cd ..
```

4. If you created a DNS entry for the data LIF of the Vserver, repeat the previous tests with a folder that is mounted using the DNS name. The following commands create a folder named `test2`, mount it using the name of the Vserver, and test access by creating and writing to a file named `myfile2`:

```
host# mkdir /mnt/test2
host# mount -t nfs -o nfsvers=3,hard vs0.example.com:/data/data2 /mnt/test2
host# su hewitta
host$ cd test2
host$ touch myfile2
host$ ls -l myfile2
-rwxrwxr-- 1 hewitta eng 0 Sep 25 13:58 myfile2
host:mnt/test1 # cat >myfile2
This text inside the second file
host:mnt/test1 # cat myfile2
This text inside the second file
host:mnt/test1 # rm -r myfile2
```

Testing SMB access from a Windows client

You should verify that you have configured SMB correctly by using a Windows client to access the SMB share and write data to the share.

Before you begin

You must be logged in as a Windows user that is authenticated to the Active Directory domain that includes the Vserver.

About this task

This procedure is performed on a Windows client.

Procedure

1. Use Windows Explorer to map a drive to the CIFS server name followed by the name of share that you created. If the CIFS server is named vs0.example.com and the share is named Test, you should enter the following:
   `\\vs0.example.com\Test`
2. On the newly created drive, create a test file. Use Notepad to create a text file called `test.txt`. The file is saved successfully to the SMB share.
3. Delete the test file.

Where to find additional information

All of the following documentation is available from the IBM N series support website (accessed and navigated as described in Websites):

Express guides

Data ONTAP Multiprotocol Server Configuration Express Guide
Describes how to quickly set up the SMB/CIFS and NFS services on a Vserver in Data ONTAP 8.2, in preparation for configuring SMB and NFSv3 client access to files contained on the Vserver.

SMB File Access Express Guide
Describes how to quickly configure SMB access to files contained in NTFS security-style volumes in Data ONTAP 8.2.

NFSv3 File Access Express Guide
Describes how to quickly configure NFSv3 access to files contained in UNIX security-style volumes in Data ONTAP 8.2.

Reference guides

The following reference documentation, which is available from the IBM N series support website (accessed and navigated as described in Websites), can help you further configure client access.

OnCommand System Manager Help
Describes how to use OnCommand System Manager to complete typical tasks. Available within the product.

Clustered Data ONTAP File Access and Protocols Management Guide
Describes how to manage file access on IBM systems with CIFS and NFS protocols.

Clustered Data ONTAP Logical Storage Management Guide
Describes how to efficiently manage your logical storage resources on systems running clustered Data ONTAP, using volumes, FlexClone volumes, files and LUNs, FlexCache volumes, deduplication, compression, qtrees, and quotas.

Clustered Data ONTAP Network Management Guide
Describes how to connect your cluster to your Ethernet networks and how to manage logical interfaces (LIFs).

Clustered Data ONTAP System Administration Guide for Cluster Administrators
Describes general system administration for storage systems running clustered Data ONTAP.

Technical Reports

Note: These technical reports contain information about NetApp products that IBM licenses and in some cases customizes. Technical reports might contain information about models and features that are not supported by IBM.

Technical Report-3967 Deployment and Best Practices Guide for Data ONTAP 8.1 Cluster-Mode Windows File Services
Describes setting up CIFS/SMB, including best practices and troubleshooting information.

Technical Report-4067 Clustered Data ONTAP NFS Implementation Guide

Serves as an NFSv3 and NFSv4 operational guide and provides an overview of the clustered Data ONTAP 8.2 operating system with a focus on NFSv4. It details steps in the configuration of an NFS server, NFSv4 features, and the differences between clustered Data ONTAP and Data ONTAP operating in 7-Mode.

Technical Report-4073 Secure Unified Authentication with NetApp Storage Systems: Kerberos, NFSv4, and LDAP for User Authentication over NFS

Explains how to configure clustered Data ONTAP for use with UNIX-based Kerberos version 5 (krb5) servers for NFS storage authentication and Windows Server Active Directory (AD) as the KDC and Lightweight Directory Access Protocol (LDAP) identity provider.

Technical Report-3580 NFSv4 Enhancements and Best Practices Guide: Data ONTAP Implementation

Describes the best practices that should be followed while implementing NFSv4 components on AIX, Linux, or Solaris clients attached to IBM N series storage systems.

Related information:

IBM N series support website: www.ibm.com/storage/support/nseries

Copyright and trademark information

This section includes copyright and trademark information, and important notices.

Copyright information

References in this documentation to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's or NetApp's intellectual property rights may be used instead of the IBM or NetApp product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM and NetApp, are the user's responsibility.

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.A. 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

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 http://www.ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Mars, 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, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, 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.

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

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

NetApp NetCache is certified RealSystem compatible.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

For additional information, visit the web at:
http://www.ibm.com/ibm/licensing/contact/

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may

vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Index

U

V

NA 210-06368_A0, Printed in USA

SC27-6408-00