IBM System Storage N series

# Clustered Data ONTAP 8.2 Antivirus Configuration Guide

SC27-6605-00

# 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* on page 5).

## 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* on page 5) 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* on page 5).

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* on page 5).

**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

# File protection using virus scanning

You can configure virus scanning on an external server to protect files and data stored in a system running clustered Data ONTAP. You must configure scanner pools to define the external virus-scanning servers and on-access policies to scan files for viruses when they are accessed by a user (on-access scanning).

You must also configure the Vscan file-operations profile parameter to specify which action on the CIFS share can trigger virus scanning before you enable virus scanning on a Storage Virtual Machine (SVM).

**Note:** You must have completed the CIFS configuration before you configure virus scanning.

To ensure that files on the storage system are scanned and cleaned, you must configure the virus scanning across a cluster or an SVM. You must also understand the process of virus scanning and the components that are required for the antivirus setup.

Virus scanning is not supported on SVMs with Infinite Volume. Virus scanning is supported only on SVMs with FlexVol volumes.

## Antivirus architecture

To configure virus scanning successfully, you must be aware of the external virus-scanning components (also known as Vscan server components), the components of the system running clustered Data ONTAP, and how these components relate to each other in the antivirus architecture.

### Components of the Vscan server

| | |
|---|---|
| **Clustered Data ONTAP Antivirus Connector** | The Antivirus Connector is installed on the Vscan server to provide communication between the system running clustered Data ONTAP and the Vscan server. |
| **Antivirus software** | The antivirus software is installed and configured on the Vscan server to scan the files for any viruses or any other malicious data. The antivirus software must be compliant with clustered Data ONTAP. You must also specify the remedial actions to be taken on the infected files in this software. You can install this software based on the vendor. |

### Components of the system running clustered Data ONTAP

| | |
|---|---|
| **Scanner pool** | A scanner pool is used to validate and manage the connection between the Vscan servers and the Storage Virtual Machine (SVM). You can create a scanner pool for an SVM and define the list of Vscan servers and privileged users that can access and |

connect to that SVM. You can also specify the scan request and scan response timeout period. If the scan response to a scan request is not received within this timeout period, then the scan request is sent to an alternative Vscan server, if available.

**Scanner policy**

A scanner policy defines when the scanner pool will be active. A Vscan server is allowed to connect to an SVM only if its IP and privileged user are part of the active scanner pool list for that SVM.

**Note:** The scanner policies are all system defined and you cannot create a customized scanner policy.

A scanner policy can have one of the following values:

- Primary: Makes the scanner pool always active
- Secondary: Makes the scanner pool active only when none of the primary Vscan servers are connected
- Idle: Makes the scanner pool always inactive

**On-access policy**

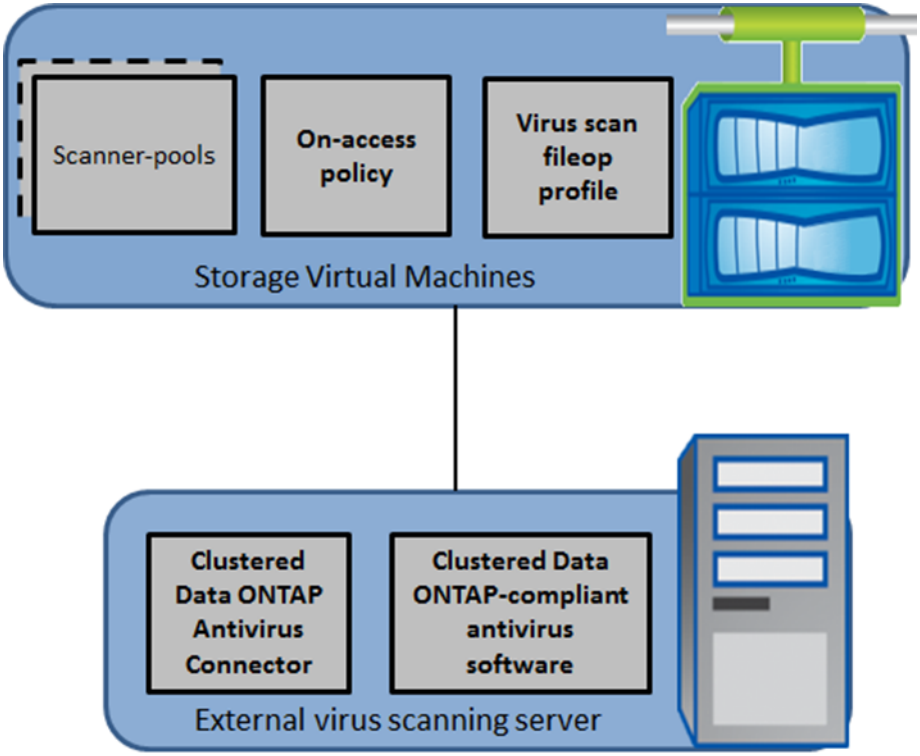
On-access policy defines the scope of scanning of files when accessed by a client. You can specify the maximum size of the file, which must be considered for virus scanning, and file extensions and paths to be excluded from scanning. You can also choose from the available set of filters to define the scope of scanning.

**Vscan file-operations profile**

The Vscan file-operations profile (-vscan-fileop-profile) parameter defines which action on the CIFS share can trigger virus scanning. You must configure this parameter while creating or modifying a CIFS share.

This parameter can have one of the following values:

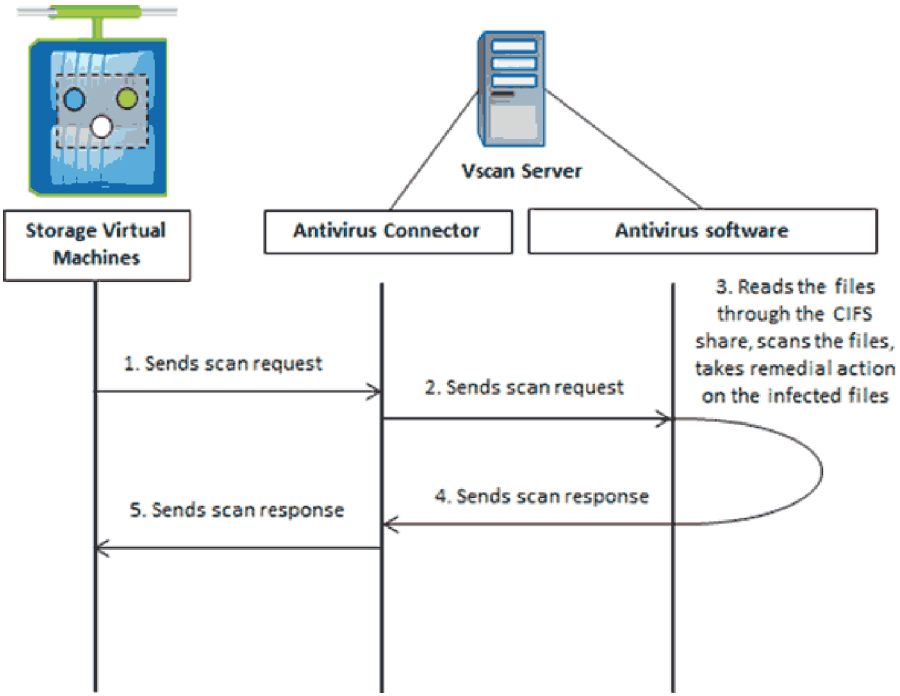
- no-scan: Virus scans are never triggered for this share.
- standard: Virus scans can be triggered by open, close, and rename operations. This is the default profile.
- strict: Virus scans can be triggered by open, read, close, and rename operations.
- writes-only: Virus scans can be triggered only when a file that has been modified is closed.




## How virus scanning works

Virus scanning is performed on Vscan servers, which run the Antivirus Connector and the antivirus software. You can configure the system running clustered Data ONTAP to scan files when they are modified or accessed by a client.

The following is the virus scanning process when it is enabled on a Storage Virtual Machine (SVM):



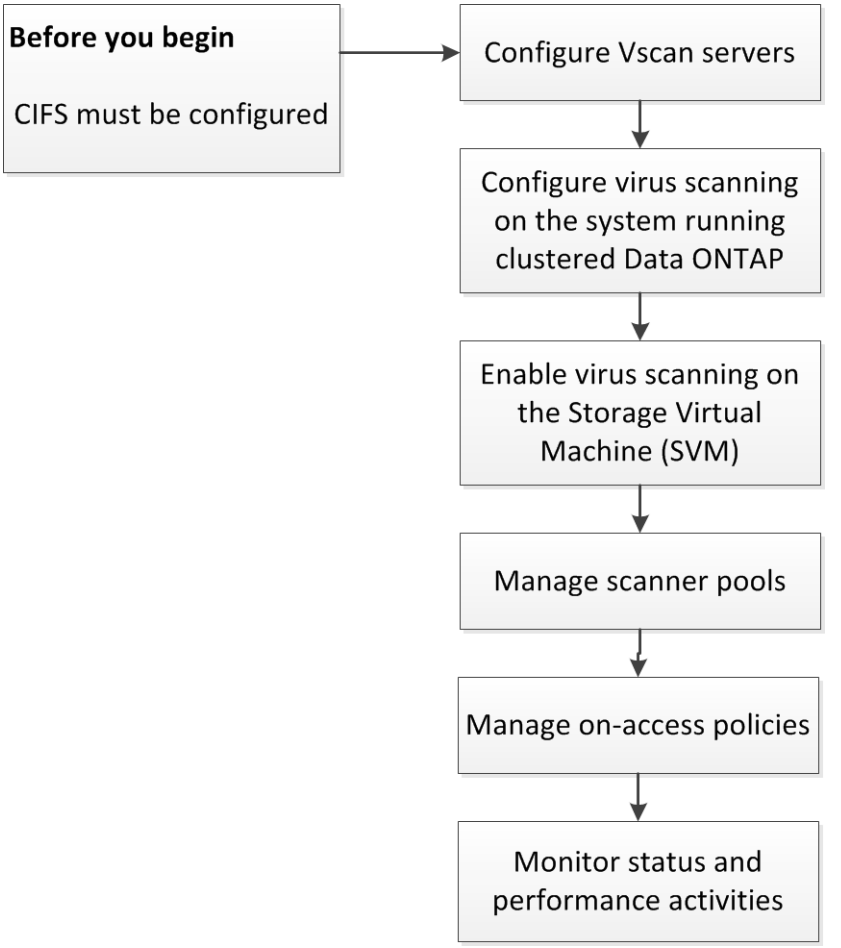

1. When a file is accessed by a client, in a way that it matches the on-access policy that has been set for an SVM and the Vscan file-operations profile parameter that has been set for the CIFS shares, a scan request is sent from the SVM to the Vscan server.
2. The Antivirus Connector receives the scan request and sends it to the antivirus software for scanning.
3. The antivirus software receives the scan request, reads the file through the CIFS share, scans the file, and takes remedial action on the infected file based on the configuration that has been set in the antivirus software.
4. The antivirus software sends the result of the action to the Antivirus Connector.
5. The Antivirus Connector sends the response to the SVM.

### Related concepts

*Antivirus architecture* on page 8

# Workflow for setting up and managing virus scanning

The workflow for setting up and managing virus scanning provides the high-level steps that a user must perform for setting up and managing the virus scanning activities.




**Related concepts**

*Antivirus architecture* on page 8

# Preparing to configure the Vscan servers

Before configuring the Vscan servers, you must be aware of certain requirements for installing and configuring the Vscan servers. You must also be aware of the vendors that provide the antivirus software.

## Requirements for Vscan servers

You should ensure that the Vscan server requirements are met before installing the Antivirus Connector and the antivirus software on the Vscan server.

### Antivirus Connector requirements

- The Antivirus Connector must be installed only on the following Windows platforms:
  - Windows 2008
  - Windows 2008 R2
  - Windows 2012
- .NET version 3.0 and above

**Note:** You must ensure that the SMB 2.0 protocol is enabled on a Windows server on which you are installing and running the Antivirus Connector.

### Antivirus software requirements

For information about the antivirus software requirements, see the vendor documentation.

#### Related concepts

*Configuring Vscan servers* on page 14

## Supported antivirus vendors

You must install and configure the antivirus software provided by the vendor on the Vscan servers to scan the files, take remedial actions, and send the response to the Antivirus Connector.

For information about the vendors, software, and the versions that are supported, see the N series Interoperability Matrices website (accessed and navigated as described in *Websites* on page 5).

#### Related concepts

*Information about installing and configuring the antivirus software* on page 14

# Configuring Vscan servers

You must set up one or more Vscan servers to ensure that files on your system are scanned for viruses. To do this, you must install and configure the Antivirus Connector and the antivirus software provided by the vendor.

## Information about installing and configuring the antivirus software

You must install and configure the antivirus software on the Vscan servers to ensure that the files that are sent from the system running clustered Data ONTAP are scanned and cleaned.

For information about installing and configuring the antivirus software, see the documentation provided by your vendor.

### Related concepts

*Requirements for Vscan servers* on page 13
*Supported antivirus vendors* on page 13

## Installing Antivirus Connector

You must install the Antivirus Connector to enable the antivirus software to communicate with one or more Storage Virtual Machines (SVMs).

### Before you begin

- You must have downloaded the Antivirus Connector setup file from the N series support website (accessed and navigated as described in *Websites* on page 5) and saved it to a directory on your hard drive.
- You must have ensured that the requirements to install the Antivirus Connector are met.
- You must have administrator privileges to install the Antivirus Connector.

### Steps

1. Start the Antivirus Connector installation wizard by running the appropriate setup file.
2. Click **Next**.

   The Destination Folder dialog box opens.
3. Click **Next** to install the Antivirus Connector to the folder that is listed or click **Change** to install to a different folder.

The ONTAP AV Connector Windows Service Credentials dialog box opens.

4. Enter your Windows service credentials or click **Add** to select a user.

   This user must be a valid domain user and must exist in the SVMs scanner pool to configure virus scanning.

5. Click **Next**.

   The Ready to Install the Program dialog box opens.

6. Click **Install** to begin the installation or click **Back** if you want to make any changes to the settings.

   A status box opens and charts the progress of the installation. Then, the InstallShield Wizard Completed dialog box opens.

7. Select **Configure ONTAP Management LIFs** check box if you want to continue with the configuration of the Data ONTAP management LIFs.

   **Note:** You must configure at least one ONTAP management LIF before this Vscan server can be used.

8. Select **Show the Windows Installer log** check box if you want to view the installation logs.

9. Click **Finish** to end the installation and to close the InstallShield wizard.

   The Configure ONTAP Management LIFs for Polling icon is saved on the desktop to configure the ONTAP management LIFs.

### Related concepts

*Configuring Antivirus Connector* on page 15
*Requirements for Vscan servers* on page 13

### Related information

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

# Configuring Antivirus Connector

You must configure the Antivirus Connector to specify one or more Storage Virtual Machines (SVMs) that you want to connect to by entering the Data ONTAP Management LIF, poll information, and the account credentials. You can also modify the details of an SVM connection or remove an SVM connection.

### Related tasks

*Installing Antivirus Connector* on page 14

## Adding an SVM to the Antivirus Connector

You add a Storage Virtual Machine (SVM) to the Antivirus Connector by adding a Data ONTAP management LIF, which will be polled to retrieve the list of data LIFs. You must also provide the poll information and the account credentials.

### Before you begin

- You must have ensured that the management LIF or the IP address of an SVM is enabled for `ontapi`.
- You must have created a user with at least read-only access to the `network interface` command directory for `ontapi`. For more information about creating a user, see the `security login role create` and `security login create` man pages.

  **Note:** You can also use the domain user as an account by adding an authentication tunnel SVM for an administrative SVM. For more information, see the `security login domain-tunnel create` man page.

### About this task

When you complete the installation of the Antivirus Connector successfully, the Configure ONTAP Management LIFs for Polling icon is saved on the desktop.

### Steps

1. Double-click the **Configure ONTAP Management LIFs for Polling** icon available on your desktop.

   The Configure ONTAP Management LIFs for Polling dialog box opens.

2. Enter the management LIF or IP address of the SVM that you want to add.

   You can also enter the cluster management LIF. If the cluster management LIF is specified, all SVMs within that cluster which are serving CIFS can use the Vscan server.

3. Enter the poll duration, in seconds.

   The poll duration is the frequency in which the Antivirus Connector checks for changes to the SVMs or cluster's LIF configuration. The default poll interval is 60 seconds.

4. Enter the account name and password.
5. Click **Test** to verify the connectivity and authenticate the connection.
6. Click **Update** to add the management LIF to the list of management LIFs to poll.
7. Click **Save** to save the connection to the registry.
8. Click **Export** if you want to export the list of connections to a registry import/export file.

   This is useful if multiple Vscan servers will use the same set of management LIFs.

#### Related tasks

*Installing Antivirus Connector* on page 14

## Modifying the details of an SVM connection

You can update the details of a Storage Virtual Machine (SVM) connection by modifying the Data ONTAP management LIF and the poll information.

#### Before you begin

You must have created a user with at least read-only access to the `network interface` command directory for `ontapi`. For more information about creating a user, see the `security login role create` and `security login create` man pages.

**Note:** You can also use the domain user as an account by adding an authentication tunnel SVM for an administrative SVM. For more information, see the `security login domain-tunnel create` man page.

#### About this task

When you complete the installation of the Antivirus Connector successfully, the Configure ONTAP Management LIFs for Polling icon is saved on the desktop.

#### Steps

1. Double-click the **Configure ONTAP Management LIFs for Polling** icon available on your desktop.

   The Configure ONTAP Management LIFs for Polling dialog box opens.
2. Select the IP address of the SVM and click **Update**.
3. Update the information, as required.
4. Click **Save** to save the changes.
5. Click **Export** if you want to export the list of connections to a registry import/export file.

#### Related tasks

*Adding an SVM to the Antivirus Connector* on page 16

## Removing an SVM connection from the Antivirus Connector

If you no longer require a Storage Virtual Machine (SVM) connection, you can remove it.

#### About this task

When you complete the installation of the Antivirus Connector successfully, the Configure ONTAP Management LIFs for Polling icon is saved on the desktop.

### Steps

1. Double-click the **Configure ONTAP Management LIFs for Polling** icon available on your desktop.

   The Configure ONTAP Management LIFs for Polling dialog box opens.
2. Select one or more IP addresses of the SVM and click **Remove**.
3. Click **Save** to save the changes.
4. Click **Export** if you want to export the list of connections to a registry import/export file.

### Related tasks

*Adding an SVM to the Antivirus Connector* on page 16

# Configuring virus scanning

After you have set up the Vscan servers, you must configure scanner pools and on-access policies on the system running clustered Data ONTAP. You must also configure the Vscan file-operations profile parameter before you enable Vscan on a Storage Virtual Machine (SVM).

**Note:** You must have completed the CIFS configuration before you begin to configure virus scanning.

For information about configuring CIFS, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.

## Creating a scanner pool

You must create a scanner pool for a Storage Virtual Machine (SVM, formerly known as Vserver) or a cluster to define the list of Vscan servers and privileged users that are allowed to access and connect to that SVM or cluster.

### About this task

- You can create a scanner pool for an individual SVM or for a cluster. The scanner pool created for the cluster is available to all the SVMs within that cluster. However, you must apply the scanner policy individually on the SVM, that must use the scanner pool, within the cluster.
- You can create a maximum of 20 scanner pools per SVM.
- You can include a maximum of 100 Vscan servers and privileged users in a scanner pool.

### Step

1. Use the `vserver vscan scanner-pool create` command to create a scanner pool.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool create` man page.

**Example**

The following example shows how to create a scanner pool named “SP1” on an SVM named “vs1”:

```
Cluster::> vserver vscan scanner-pool create -vserver vs1 -scanner-
pool SP1 -servers 1.1.1.1,2.2.2.2 -privileged-users cifs\u1,cifs\u2
```

### Related concepts

*Managing scanner pools* on page 26

### Related tasks

*Applying a scanner policy to a scanner pool* on page 20

# Applying a scanner policy to a scanner pool

You must apply a scanner policy to every scanner pool defined on a Storage Virtual Machine (SVM, formerly known as Vserver). This policy defines when the scanner pool will be active. By default, the scanner policy applied to a scanner pool is `idle`.

### Before you begin

You must have created a scanner pool.

### About this task

You can apply only one scanner policy to a scanner pool. A Vscan server is allowed to connect to an SVM only if its IP address and privileged user are part of the active scanner pool list for that SVM.

### Step

1. Use the `vserver vscan scanner-pool apply-policy` command to apply a scanner policy to a scanner pool.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool apply-policy` man page.

**Example**

The following example shows how to apply the scanner policy named “primary” to a scanner pool named “SP1” on an SVM named “vs1”:

```
Cluster::> vserver vscan scanner-pool apply-policy -vserver vs1 -
scanner-pool SP1  -scanner-policy primary
```

### Related tasks

*Viewing active scanner pools of SVMs* on page 27

# Creating an on-access policy

You must create an on-access policy for a Storage Virtual Machine (SVM, formerly known as Vserver) or a cluster to define the scope of scanning. You can specify the maximum size of the file which must be considered for virus scanning and file extensions and paths to be excluded from scanning.

### About this task

- By default, clustered Data ONTAP creates an on-access policy named `default_CIFS` and enables it for all the existing SVMs. You can use the `default_CIFS` on-access policy or you can create a customized on-access policy.
- You can create an on-access policy for an individual SVM or for a cluster. The on-access policy created for the cluster is available to all the SVMs within that cluster. However, you must enable the on-access policy individually on all the SVMs within the cluster.
- You can create a maximum of 10 on-access policies per SVM. However, you can enable only one on-access policy at a time.
- You can exclude a maximum of 100 paths and file extensions from virus scanning in one on-access policy.

### Step

1. Use the `vserver vscan on-access-policy create` command to create an on-access policy.

   For information about the parameters that you can use with this command, see the `vserver vscan on-access-policy create` man page.

**Example**

The following example shows how to create an on-access policy named “Policy1” on an SVM named “vs1”:

```
Cluster::> vserver vscan on-access-policy create -vserver vs1 -
policy-name Policy1 -protocol CIFS -filters scan-ro-volume -max-
file-size 3GB -file-ext-to-exclude "mp3","txt" -paths-to-exclude
"\vol\a b\","\vol\a,b\"
```

### Related concepts

*Managing on-access policies* on page 33

# Enabling an on-access policy

After you create an on-access scan policy, you must enable it for a Storage Virtual Machine (SVM, formerly known as Vserver).

### About this task

You can enable only one on-access policy of a specified protocol for an SVM at a time.

### Step

1. Use the `vserver vscan on-access-policy enable` command to enable an on-access policy for an SVM.

   For information about the parameters that you can use with this command, see the `vserver vscan on-access-policy enable` man page.

**Example**

The following example shows how to enable an on-access policy named "Policy1" on an SVM named "vs1":

```
Cluster::> vserver vscan on-access-policy enable -vserver vs1 -
policy-name Policy1
```

### Related tasks

*Disabling an on-access policy* on page 34

# Modifying the Vscan file-operations profile for CIFS share

While creating a CIFS share, you must have configured the -vscan-fileop-profile parameter to specify which action on the CIFS share can trigger virus scanning. By default, the value is `Standard`. You can use the default value or you can change the value by using the `vserver cifs share modify` command.

### Before you begin

You must have created the CIFS share.

**Note:** Virus scanning will not be performed on CIFS shares for which the continuously-available parameter is set to Yes.

For more information about creating the CIFS shares, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.

### Step

1. Use the `vserver cifs share modify` command to modify the value of the -vscan-fileop-profile parameter.

   For more information about modifying the CIFS shares, see the `vserver cifs share modify` man page.

## Enabling virus scanning on an SVM

After you have completed configuring the scanner pool, on-access policy, and the Vscan file-operations profile parameter, you must enable virus scanning on a Storage Virtual Machine (SVM, formerly known as Vserver).

### Before you begin

- You must have created one or more scanner pools and applied the scanner policy to the scanner pools.
- You must have created an on-access policy and enabled it on an SVM.
- You must have configured the Vscan file-operations profile parameter.
- You must have ensured that the Vscan servers are available.

### About this task

When you enable virus scanning on an SVM, the SVM connects to the Vscan servers that are mentioned in the active scanner pool of that SVM.

### Step

1. Use the `vserver vscan enable` command to enable the virus scanning on an SVM.

   For information about the parameters that you can use with this command, see the `vserver vscan enable` man page.

**Example**

The following example shows how to enable virus scanning on an SVM named “vs1”:

```
Cluster::> vserver vscan enable -vserver vs1
```

### Related concepts

*Configuring Vscan servers* on page 14

# Disabling virus scanning on an SVM

You can disable virus scanning on a Storage Virtual Machine (SVM, formerly known as Vserver) by using the `vserver vscan disable` command.

### About this task

When you disable virus scanning on an SVM, the SVM is disconnected from all the connected Vscan servers.

### Step

1. Use the `vserver vscan disable` command to disable the virus scanning on an SVM.

   For information about the parameters that you can use with this command, see the `vserver vscan disable` man page.

**Example**

The following example shows how to disable virus scanning on an SVM named “vs1”:

```
Cluster::> vserver vscan disable -vserver vs1
```

### Related tasks

*Enabling virus scanning on an SVM* on page 23

# Resetting the status of the scanned files

You can discard the cached information or reset the status of the files that have already been scanned for a Storage Virtual Machine (SVM, formerly known as Vserver) by using the `vserver vscan reset` command. After running this command, all the files are available for scan when they are accessed.

### About this task

You can perform this operation in case of any misconfiguration while setting up and enabling virus scanning or if you want to restart the virus scanning process.

**Note:** This command can cause performance degradation because the files are scanned again when they are accessed.

**Step**

1. Use the `vserver vscan reset` command to reset the status of the files that have already been scanned for an SVM.

   For information about the parameters that you can use with this command, see the `vserver vscan reset` man page.

**Example**

The following example shows how to reset the status of the files that have already been scanned for an SVM named “vs1”:

```
Cluster::> vserver vscan reset -vserver vs1
```

# Managing scanner pools

You can manage scanner pools to view the scanner pool information and modify the Vscan servers and privileged users that are associated with the scanner pool. You can also modify the request and response timeout period, and delete a scanner pool, if it is no longer required.

## Viewing scanner pools of SVMs

You can view information about all scanner pools belonging to all Storage Virtual Machines (SVMs, formerly known as Vservers) or one scanner pool belonging to an SVM by using the `vserver vscan scanner-pool show` command.

### Step

1. Use the `vserver vscan scanner-pool show` command to view a scanner pool or a list of scanner pools of all SVMs.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool show` man page.

**Example**

The following examples show how to view the list of scanner pools of all SVMs and a scanner pool of an SVM:

```
Cluster::> vserver vscan scanner-pool show

        Scanner Pool                      Privileged Scanner
Vserver Pool    Owner    Servers          Users      Policy
------------------------------------------------------------
vs1     new     vserver  1.1.1.1, 2.2.2.2 cifs\u5    idle
vs1     p1      vserver  3.3.3.3          cifs\u1    primary
                                          cifs\u2
2 entries were displayed.

Cluster::> vserver vscan scanner-pool show -vserver vs1 -scanner-
pool new

Vserver: vs1
Scanner Pool: new
Applied Policy: idle
Current Status: off
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2
```

```
List of Privileged Users: cifs\u5
```

## Viewing active scanner pools of SVMs

You can view the list of active scanner pools belonging to all Storage Virtual Machines (SVMs, formerly known as Vservers) by using the `vserver vscan scanner-pool show-active` command. The list of active scanner pools is derived by merging the information about the active scanner pools on all SVMs.

### Step

1. Use the `vserver vscan scanner-pool show-active` command to view the list of active scanner pools of all SVMs.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool show-active` man page.

**Example**

The following example shows how to view the list of active scanner pools of all SVMs:

```
Cluster::> vserver vscan scanner-pool show-active

                                                      Privileged
Vserver  Scanner Pools Servers                        Users
---------------------------------------------------------------------
vs1      new, p1       1.1.1.1, 2.2.2.2, 3.3.3.3    cifs\u1, cifs\u4
vs2      clus, p2      3.3.3.3, 4.4.4.4, 5.5.5.5    cifs\u2, cifs\u5
2 entries were displayed.
```

## Modifying a scanner pool

You can update scanner pool information such as the list of Vscan servers and the privileged users that can connect to the Storage Virtual Machine (SVM, formerly known as Vserver) and the request and response timeout period.

### Step

1. Use the `vserver vscan scanner-pool modify` command to update the scanner pool information.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool modify` man page.

**Example**

The following example shows how to modify a scanner pool named “SP1” on an SVM named “vs1”:

```
Cluster::> vserver vscan scanner-pool modify -vserver vs1 -scanner-
pool SP1 -servers 3.3.3.3 -privileged-users cifs\u3
```

**Related tasks**

*Creating a scanner pool* on page 19

# Deleting a scanner pool

If you no longer need an unused scanner pool, you can delete it.

**Step**

1. Use the `vserver vscan scanner-pool delete` command to delete a scanner pool.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool delete` man page.

**Example**

The following example shows how to delete a scanner pool named “SP1” from a Storage Virtual Machine (SVM, formerly known as Vserver) named “vs1”:

```
Cluster::> vserver vscan scanner-pool delete -vserver vs1 -scanner-
pool SP1
```

**Related tasks**

*Creating a scanner pool* on page 19

# Adding privileged users to a scanner pool

You can add one or more privileged users to a scanner pool to define the privileged users that can connect to a Storage Virtual Machine (SVM, formerly known as Vserver) by using the `vserver vscan scanner-pool privileged-users add` command.

### Before you begin

You must have created a scanner pool for an SVM.

### Step

1. Use the `vserver vscan scanner-pool privileged-users add` command to add one or more privileged users to a scanner pool.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool privileged-users add` man page.

**Example**

The following example shows how to add the privileged users named “cifs\u2” and “cifs\u3” to a scanner pool named “SP1” on an SVM named “vs1”:

```
Cluster::> vserver vscan scanner-pool privileged-users add -vserver
vs1 -scanner-pool SP1 -privileged-users cifs\u2,cifs\u3
```

### Related tasks

*Modifying a scanner pool* on page 27

# Removing privileged users from a scanner pool

If you no longer require privileged users, you can remove them from the scanner pool by using the `vserver vscan scanner-pool privileged-users remove` command.

### Step

1. Use the `vserver vscan scanner-pool privileged-users remove` command to remove one or more privileged users from a scanner pool.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool privileged-users remove` man page.

**Example**

The following example shows how to remove the privileged users named “cifs\u2” and “cifs \u3” from a scanner pool named “SP1” on a Storage Virtual Machine (SVM, formerly known as Vserver) named “vs1”:

```
Cluster::> vserver vscan scanner-pool privileged-users remove -
vserver vs1 -scanner-pool SP1 -privileged-users cifs\u2,cifs\u3
```

**Related tasks**

*Modifying a scanner pool* on page 27

# Viewing the privileged users of all scanner pools

You can view the list of privileged users of all scanner pools by using the `vserver vscan scanner-pool privileged-users show` command.

**Step**

1. Use the `vserver vscan scanner-pool privileged-users show` command to view the list of privileged users of all scanner pools.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool privileged-users show` man page.

**Example**

The following example shows how to view the list of privileged users for all scanner pools:

```
Cluster::> vserver vscan scanner-pool privileged-users show

Vserver         Scanner Pool      Privileged Users
------------------------------------------------
Cluster         clus              cifs\u5
vs1             new               cifs\u7
vs1             clus              cifs\u5
vs1             p1                cifs\u1, cifs\u2
vs2             clus              cifs\u5
vs2             p2                cifs\u2
6 entries were displayed.
```

# Adding Vscan servers to a scanner pool

You can add one or more Vscan servers to a scanner pool to define the Vscan servers that can connect to a Storage Virtual Machine (SVM, formerly known as Vserver) by using the `vserver vscan scanner-pool servers add` command.

### Before you begin

You must have created a scanner pool for an SVM.

### Step

1. Use the `vserver vscan scanner-pool servers add` command to add one or more Vscan servers to a scanner pool.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool servers add` man page.

**Example**

The following example shows how to add a list of Vscan servers to a scanner pool named "SP1" on an SVM named "vs1":

```
Cluster::> vserver vscan scanner-pool servers add -vserver vs1 -
scanner-pool SP1 -servers 10.10.10.10,11.11.11.11
```

### Related tasks

*Modifying a scanner pool* on page 27

# Removing Vscan servers from a scanner pool

If you no longer require a Vscan server, you can remove it from the scanner pool by using the `vserver vscan scanner-pool servers remove` command.

### Step

1. Use the `vserver vscan scanner-pool servers remove` command to remove one or more Vscan servers from a scanner pool.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool servers remove` man page.

**Example**

The following example shows how to remove a list of Vscan servers from a scanner pool named “SP1” on a Storage Virtual Machine (SVM, formerly known as Vserver) named “vs1”:

```
Cluster::> vserver vscan scanner-pool servers remove -vserver vs1 -
scanner-pool SP1 -servers 10.10.10.10,11.11.11.11
```

**Related tasks**

*Modifying a scanner pool* on page 27

# Viewing the Vscan servers of all scanner pools

You can view the list of Vscan servers of all scanner pools to manage the Vscan server connections by using the `vserver vscan scanner-pool servers show` command.

**Step**

1. Use the `vserver vscan scanner-pool servers show` command to view the list of Vscan servers of all scanner pools.

   For information about the parameters that you can use with this command, see the `vserver vscan scanner-pool servers show` man page.

**Example**

The following example shows how to display the list of Vscan servers of all scanner pools:

```
Cluster::> vserver vscan scanner-pool servers show

Vserver         Scanner Pool      Servers
-----------------------------------------------------------------
Cluster         clus              5.5.5.5
vs1             new               1.1.1.1, 2.2.2.2
vs1             clus              5.5.5.5
vs1             p1                3.3.3.3, 10.10.10.10, 11.11.11.11
vs2             clus              5.5.5.5
vs2             p2                3.3.3.3, 4.4.4.4
6 entries were displayed.
```

# Managing on-access policies

You can manage on-access policies to define the scope of scanning files, when accessed by a client. You can modify the maximum size of the file, which must be considered for virus scanning, and file extensions and paths to be excluded from scanning. You can also delete and disable an on-access policy, if it is no longer required.

## Viewing on-access policies of SVMs

You can view information about all on-access policies belonging to all Storage Virtual Machines (SVMs, formerly known as Vservers) or one on-access policy belonging to an SVM to manage the on-access policies by using the `vserver vscan on-access-policy show` command.

### Step

1. Use the `vserver vscan on-access-policy show` command to view an on-access policy or a list of on-access policies of all SVMs.

   For information about the parameters that you can use with this command, see the `vserver vscan on-access-policy show` man page.

**Example**

The following examples show how to view the list of on-access policies of all SVMs and an on-access policy of an SVM:

```
Cluster::> vserver vscan on-access-policy show

         Policy    Policy                          File-Ext Policy
Vserver  Name      Owner   Protocol Paths Excluded  Excluded Status
---------------------------------------------------------------------
Cluster  default_  cluster CIFS     -               -        off
         CIFS
vs1      default_  cluster CIFS     -               -        on
         CIFS
vs1      new       vserver CIFS     \vol\temp       txt      off
vs2      default_  cluster CIFS     -               -        on
         CIFS
4 entries were displayed.


Cluster::> vserver vscan on-access-policy show -instance -vserver
vs1 -policyname new

Vserver: vs1
Policy: new
Policy Status: off
```

```
Policy Config Owner: vserver
File-Access Protocol: CIFS
Filters: scan-ro-volume
Max File Size Allowed for Scanning: 4GB
File-Paths Not to Scan: \vol\temp
File-Extensions Not to Scan: txt
```

# Modifying an on-access policy

You can modify an on-access policy to define the scope of scanning files, when accessed by a client. You can also modify the maximum size of the file considered for virus scanning and the file extensions and paths to be excluded from scanning.

### Step

1. Use the `vserver vscan on-access-policy modify` command to update the on-access policy.

   For information about the parameters that you can use with this command, see the `vserver vscan on-access-policy modify` man page.

**Example**

The following example shows how to modify an on-access policy named “Policy1” on a Storage Virtual Machine (SVM, formerly known as Vserver) named “vs1”:

```
vserver vscan on-access-policy modify -vserver vs1 -policy-name
Policy1 -filters scan-ro-volume -max-file-size 10GB -file-ext-to-
exclude "mp3" -paths-to-exclude "\vol1\temp","\vol2\a"
```

### Related tasks

*Creating an on-access policy* on page 21

# Disabling an on-access policy

You can disable an on-access policy for a Storage Virtual Machine (SVM, formerly known as Vserver) by using the `vserver vscan on-access-policy disable` command.

### Step

1. Use the `vserver vscan on-access-policy disable` command to disable an on-access policy for an SVM.

For information about the parameters that you can use with this command, see the `vserver vscan on-access-policy disable` man page.

**Example**

The following example shows how to disable an on-access policy named “Policy1” on an SVM named “vs1”:

```
Cluster::> vserver vscan on-access-policy disable -vserver vs1 -
policy-name Policy1
```

**Related tasks**

*Enabling an on-access policy* on page 22

# Deleting an on-access policy

If you no longer need an on-access policy, you can delete it by using the `vserver vscan on-access-policy delete` command.

**Step**

1. Use the `vserver vscan on-access-policy delete` command to delete an on-access policy.

   For information about the parameters that you can use with this command, see the `vserver vscan on-access-policy delete` man page.

**Example**

The following example shows how to delete an on-access policy named “Policy1” from a Storage Virtual Machine (SVM, formerly known as Vserver) named “vs1”:

```
Cluster::> vserver vscan on-access-policy delete -vserver vs1 -
policy-name Policy1
```

**Related tasks**

*Creating an on-access policy* on page 21

# Monitoring status and performance activities

You can monitor the critical aspects of the Vscan module, such as the health of the Vscan servers, the number of files that have been scanned, and so on. You can also view information about the Vscan server connection. This information helps you in diagnosing issues related to the Vscan server.

## Commands for viewing Vscan server information

You can view the connection status of the Vscan servers to help you understand the connections that are already in use and the connections that can be used. You can also view the summary and detailed information about the connection status.

| If you want to... | Enter the following command... |
|---|---|
| View the summary of the connection status | `vserver vscan connection-status show` |
| View detailed information about the connection status | `vserver vscan connection-status show-all` |
| View the status of the connections that are available but are not connected | `vserver vscan connection-status show-not-connected` |
| View information about the connected Vscan server | `vserver vscan connection-status show-connected` |

For more information about these commands, see the man pages.

## Viewing Vscan statistics

You can view the Vscan specific statistics to monitor performance and diagnose issues.

### About this task

You must use the `statistics start` and optional `statistics stop` commands to collect a data sample. For more information about these commands, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

### Step

1. Enter the appropriate command.

| If you want to... | Enter the following command... |
|---|---|
| View the Vscan specific statistics | **`statistics show -object offbox_vscan`** |
| View the list of counters available | **`statistics catalog counter show –object offbox_vscan`** |

For more information about these commands, see the man pages.

### Examples

The following example displays descriptions of selected statistic objects related to Vscan in the cluster:

```
cluster1::> statistics catalog counter show -object offbox_vscan

Object: offbox_vscan
    Counter                     Description
    --------------------------- ----------------------------------------------
    active_connections          Total number of current active connections
    clean                       Total number of scan responses marking file
                                as clean
    connect_accepted            Total number of connect requests from
                                Vscanner that were accepted
    filer_disconnected          Total number of disconnects initiated by
                                clustered ONTAP because connection is not
                                valid anymore
[...]

cluster1::> statistics start -object offbox_vscan -sample-id 2
Statistics collection is being started for Sample-id: 2

cluster1::> statistics show -object offbox_vscan -sample-id 2

Object: offbox_vscan
Instance: vserver_1
Start-time: 7/26/2013 19:02:02
End-time: 7/26/2013 19:02:30
Cluster: cluster1

    Counter                                             Value
    --------------------------------------------------------
    active_connections                                      0
    clean                                                   0
    connect_accepted                                        0
    filer_disconnected                                      0
[…]

cluster1::> statistics stop -sample-id 2
Statistics collection is being stopped for Sample-id: 2
```

# Copyright and trademark 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, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. 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

## R



## S



## V



## W

NA 210-06376_A0, Printed in USA

SC27-6605-00