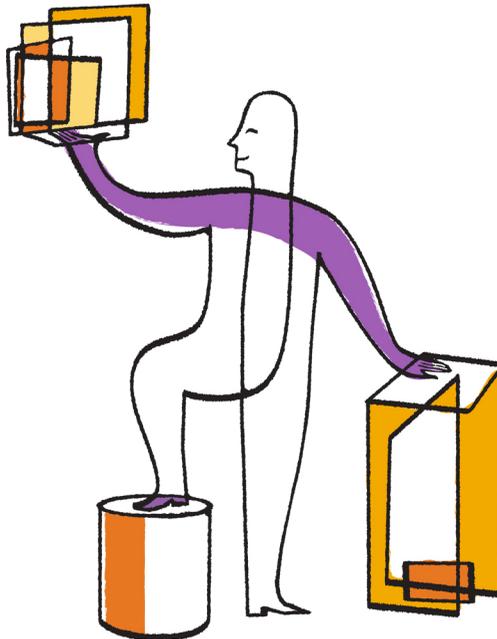




Updated for 8.2.1

Clustered Data ONTAP® 8.2

Antivirus Configuration Guide



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

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

Part number: 215-08502_C0
December 2014

Contents

File protection using virus scanning	5
Antivirus architecture	5
How virus scanning works	8
Workflow for setting up and managing virus scanning	9
Preparing to configure the Vscan servers	10
Requirements for Vscan servers	10
Supported antivirus vendors	11
Configuring Vscan servers	12
Information about installing and configuring the antivirus software	12
Installing Antivirus Connector	12
Configuring Antivirus Connector	13
Adding an SVM to Antivirus Connector	14
Modifying the details of an SVM connection	15
Removing an SVM connection from Antivirus Connector	16
Configuring virus scanning	17
Creating a scanner pool	17
Applying a scanner policy to a scanner pool	18
Creating an on-access policy	19
Enabling an on-access policy	20
Modifying the Vscan file-operations profile for CIFS share	20
Enabling virus scanning on an SVM	21
Disabling virus scanning on an SVM	22
Resetting the status of scanned files	22
Managing scanner pools	24
Viewing scanner pools of SVMs	24
Viewing active scanner pools of SVMs	25
Modifying a scanner pool	25
Deleting a scanner pool	26
Adding privileged users to a scanner pool	27
Removing privileged users from a scanner pool	27
Viewing the privileged users of all scanner pools	28
Adding Vscan servers to a scanner pool	29

Removing Vscan servers from a scanner pool	29
Viewing the Vscan servers of all scanner pools	30
Managing on-access policies	31
Viewing on-access policies of SVMs	31
Modifying an on-access policy	32
Disabling an on-access policy	32
Deleting an on-access policy	33
Monitoring status and performance activities	34
Commands for viewing Vscan server information	34
Viewing Vscan statistics	34
Copyright information	36
Trademark information	37
How to send your comments	38
Index	39

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 a 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:** The scanner pool becomes active at all times.
- **Secondary:** The scanner pool becomes active when none of the primary Vscan servers are connected.
- **Idle:** The scanner pool becomes inactive all the time.

On-access policy

On-access policy defines the scope of scanning the 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 one or more filters from the available set of filters to define the scope of scanning.

The following are the list of available filters:

- **scan-mandatory:** Enables mandatory scan. File access will be denied if there are no external virus-scanning servers available for virus scanning.
- **scan-ro-volume:** Enables scan also for read-only volume.
- **scan-execute-access:** Scans only files opened with execute-access (CIFS only). Files opened with `execute-access` (open with `execute` intent) are different from the `execute` permission on the file.

You can also choose not to use any of the filters by setting this parameter to "-". This will cause file accesses to be allowed even if the files are not scanned. Also, only read-write volumes are considered for scanning.

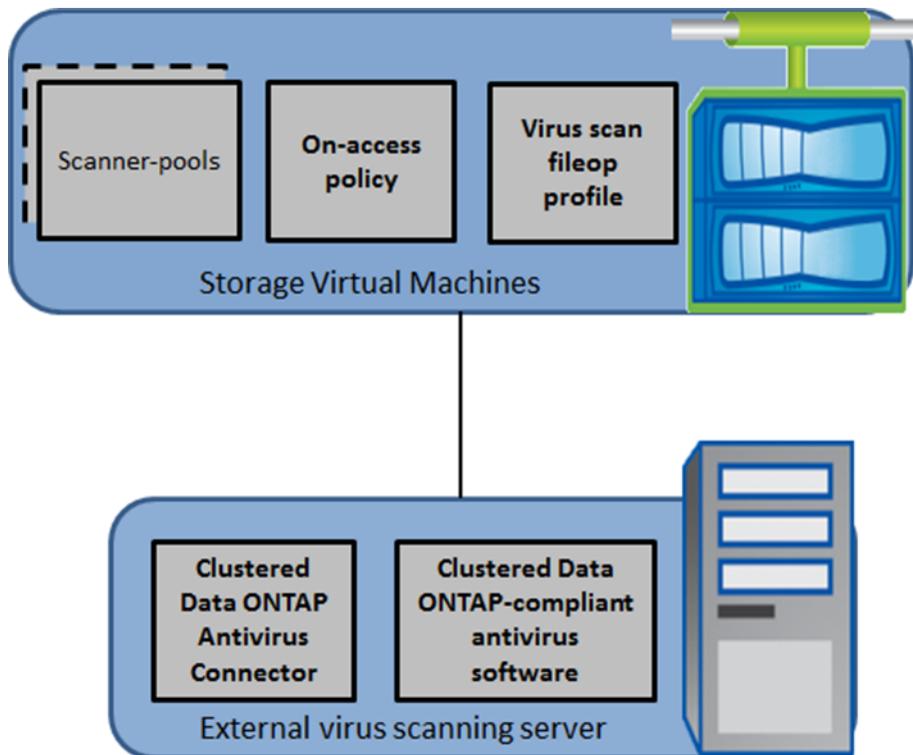
Vscan file-operations profile

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.

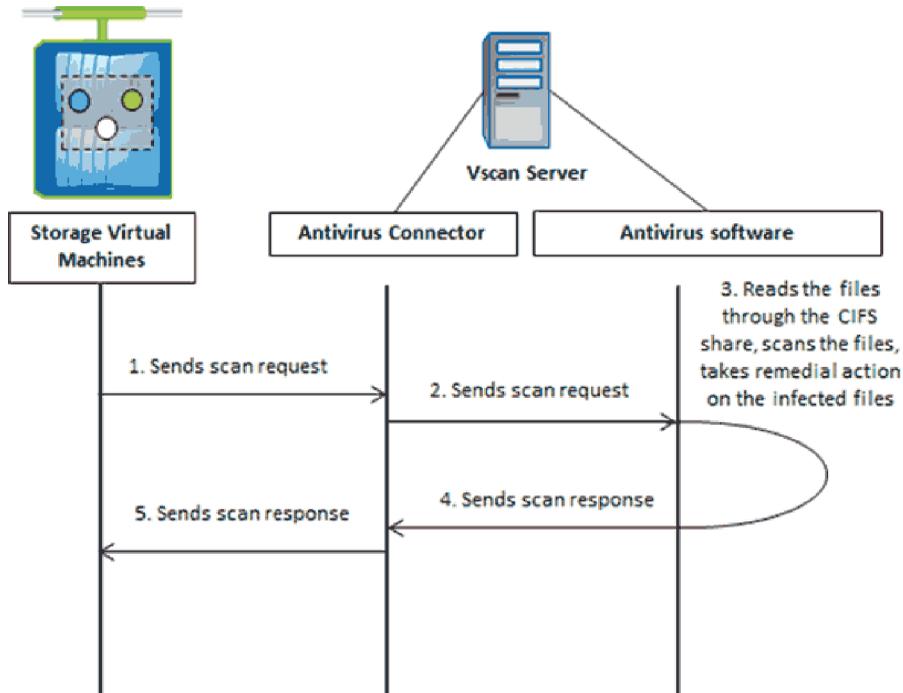
The following diagram shows the antivirus architecture and its relation with the Vscan server components:



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):



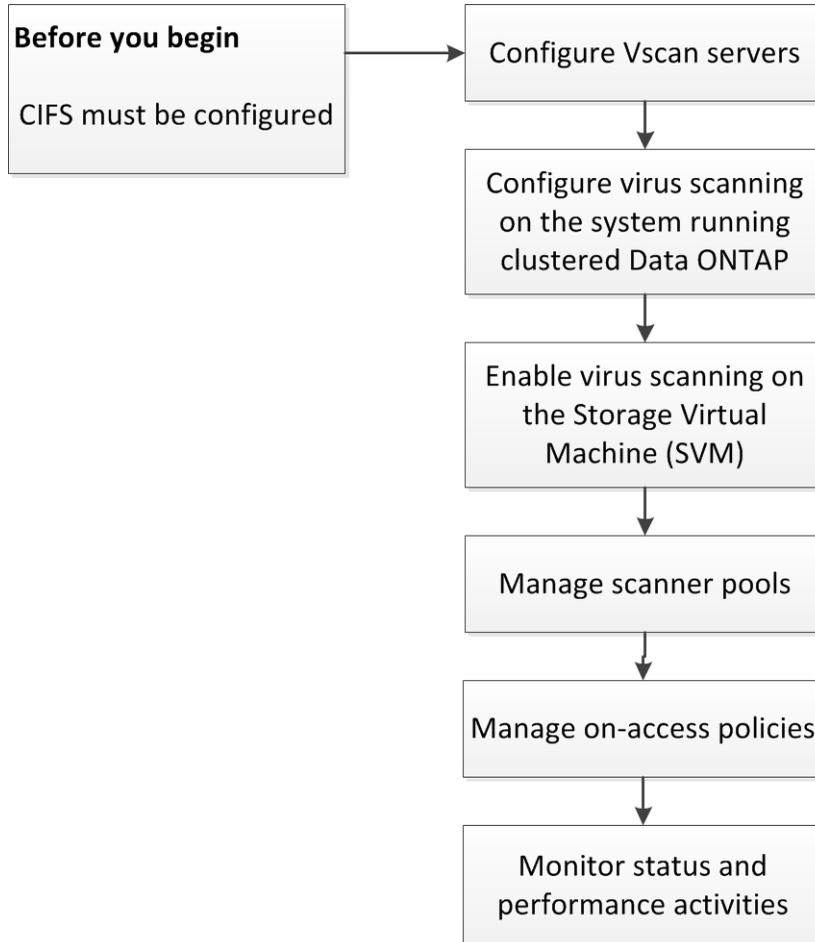
1. When a file is accessed by a client, in a way that it matches the on-access policy that has been set for an SVM and the `Vscan file-operations profile` parameter that has been set for the CIFS shares, a scan request is sent from the SVM to the Vscan server.
2. The Antivirus Connector receives the 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 5

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 5

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

Vscan servers consist of two components, Antivirus Connector and antivirus software. You should ensure that the requirements for the Antivirus Connector and the antivirus software are met before installing them 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

Note: You can install different versions of Windows platforms for different Vscan servers in a cluster.

- .NET 3.0 and later

Note: SMB 2.0 must be enabled on the 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 12

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 Interoperability Matrix at support.netapp.com/matrix.

Related concepts

[Information about installing and configuring the antivirus software](#) on page 12

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 10

[Supported antivirus vendors](#) on page 11

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 NetApp Support Site 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**.
3. In the **Destination Folder** dialog box, perform one of the following operations:
 - Click **Next** to install the Antivirus Connector to the folder that is listed.

- Click **Change** to install to a different folder.

4. In the **ONTAP AV Connector Windows Service Credentials** dialog box, perform one of the following operations:

- Enter your Windows service credentials.
- 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**.

6. In the **Ready to Install the Program** dialog box, click **Install** to begin the installation.

A status box opens and shows the progress of the installation, and then the InstallShield Wizard Completed dialog box opens.

7. Select the **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 Data ONTAP management LIF before the Vscan server can be used.

8. Select the **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 Data ONTAP management LIFs.

Related concepts

[Configuring Antivirus Connector](#) on page 13

[Requirements for Vscan servers](#) on page 10

Related information

[NetApp Support Site: support.netapp.com](http://support.netapp.com)

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 12

Adding an SVM to Antivirus Connector

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

Before you begin

- You must have ensured that the management LIF or the IP address of the 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.

Steps

1. Right-click the **Configure ONTAP Management LIFs for Polling** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **run as administrator**.

The Configure ONTAP Management LIFs for Polling dialog box opens.

2. Perform one of the following actions:

If...	Then...
You have an existing management LIF or IP address	Enter the management LIF or IP address of the SVM that you want to add.
You want to create a management LIF	Create a management LIF with role set to data , data protocol set to none , and firewall policy set to mgmt . For more information about creating a LIF, see the <i>Clustered Data ONTAP Network Management Guide</i> .

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

3. Enter the poll duration, in seconds.

The poll duration is the frequency at which Antivirus Connector checks for changes to the SVMs or to the 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 use the same set of management LIFs.

Related tasks

[Installing Antivirus Connector](#) on page 12

Modifying the details of an SVM connection

You can update the details of a Storage Virtual Machine (SVM) connection, which has been added to the Antivirus Connector, 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.

Steps

1. Right-click the **Configure ONTAP Management LIFs for Polling** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **run as administrator**.

The Configure ONTAP Management LIFs for Polling dialog box opens.

2. Select the IP address of the SVM, and then click **Update**.
3. Update the information, as required.

4. Click **Save** to update the connection details in the registry.
5. Click **Export** if you want to export the list of connections to a registry import/export file.
This is useful if multiple Vscan servers use the same set of management LIFs.

Related tasks

[Adding an SVM to Antivirus Connector](#) on page 14

Removing an SVM connection from Antivirus Connector

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

Steps

1. Right-click the **Configure ONTAP Management LIFs for Polling** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **run as administrator**.
The Configure ONTAP Management LIFs for Polling dialog box opens.
2. Select one or more IP addresses of the SVM, and then click **Remove**.
3. Click **Save** to update the connection details in the registry.
4. Click **Export** if you want to export the list of connections to a registry import/export file.
This is useful if multiple Vscan servers use the same set of management LIFs.

Related tasks

[Adding an SVM to Antivirus Connector](#) on page 14

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, which 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 the SVM named “vs1”:

```
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 24

Related tasks

[Applying a scanner policy to a scanner pool](#) on page 18

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 the SVM only if the IP address and privileged user of the Vscan server 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 the SVM named “vs1”:

```
vserver vscan scanner-pool apply-policy -vserver vs1 -scanner-pool SP1  
-scanner-policy primary
```

Related tasks

[Viewing active scanner pools of SVMs](#) on page 25

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 that must be considered for virus scanning and specify 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 the SVM named “vs1”:

```
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 31

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 each SVM at a time.

Step

1. Use the `vserver vscan on-access-policy enable` command to enable an on-access policy for the 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 the SVM named “vs1”:

```
vserver vscan on-access-policy enable -vserver vs1 -policy-name
Policy1
```

Related tasks

[Disabling an on-access policy](#) on page 32

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) to protect the data.

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 the 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 the 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 virus scanning on the 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 the SVM named “vs1”:

```
vserver vscan enable -vserver vs1
```

Related concepts

[Configuring Vscan servers](#) on page 12

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 the SVM, the SVM is disconnected from all the connected Vscan servers.

Step

1. Use the `vserver vscan disable` command to disable virus scanning on the 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 the SVM named “vs1”:

```
vserver vscan disable -vserver vs1
```

Related tasks

[Enabling virus scanning on an SVM](#) on page 21

Resetting the status of scanned files

You can discard the cached information or reset the status of files that have already been scanned for a Storage Virtual Machine (SVM, formerly known as Vserver) by using the `vserver vscan reset` command. 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.

About this task

After you run the `vserver vscan reset` command, all eligible files will be scanned, the next time they are accessed.

Attention: This command can cause performance degradation because the files will be 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 the 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 the SVM named “vs1”:

```
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
```

Vserver	Scanner Pool	Pool Owner	Servers	Privileged Users	Scanner Policy
vs1	new	vserver	1.1.1.1, 2.2.2.2	cifs\u5	idle
vs1	p1	vserver	3.3.3.3	cifs\u1 cifs\u2	primary

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
```

Vserver	Scanner Pools	Servers	Privileged 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 the 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 the SVM named “vs1”:

```
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 17

Deleting a scanner pool

If you no longer require 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”:

```
vserver vscan scanner-pool delete -vserver vs1 -scanner-pool SP1
```

Related tasks

[Creating a scanner pool](#) on page 17

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 the 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 the SVM named “vs1”:

```
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 25

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”:

```
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 25

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 the 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 the SVM named “vs1”:

```
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 25

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”:

```
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 25

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
```

Vserver	Policy Name	Policy Owner	Protocol	Paths Excluded	File-Ext Excluded	Policy Status
Cluster	default_CIFS	cluster	CIFS	-	-	off
vs1	default_CIFS	cluster	CIFS	-	-	on
vs1	new	vserver	CIFS	\vol\temp	txt	off
vs2	default_CIFS	cluster	CIFS	-	-	on

```
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 redefine the scope of scanning files, when accessed by a client. You can also modify the maximum size of the file that must be considered for virus scanning and modify 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 the 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 19

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 the 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 the SVM named “vs1”:

```
vserver vscan on-access-policy disable -vserver vs1 -policy-name
Policy1
```

Related tasks

[Enabling an on-access policy](#) on page 20

Deleting an on-access policy

If you no longer require 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”:

```
vserver vscan on-access-policy delete -vserver vs1 -policy-name
Policy1
```

Related tasks

[Creating an on-access policy](#) on page 19

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	<code>vserver vscan connection-status show</code>
View detailed information about the connection status	<code>vserver vscan connection-status show-all</code>
View the status of the connections that are available but are not connected	<code>vserver vscan connection-status show-not-connected</code>
View information about the connected Vscan server	<code>vserver vscan connection-status show-connected</code>

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	<code>statistics show -object offbox_vscan</code>
View the list of counters available	<code>statistics catalog counter show -object offbox_vscan</code>

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: vsserver_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 information

Copyright © 1994–2015 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the NetApp logo, Go Further, Faster, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

Cisco and the Cisco logo are trademarks of Cisco in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

How to send your comments

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

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

You can also contact us in the following ways:

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

Index

A

- adding
 - privileged users to a scanner pool [27](#)
 - Vscan servers to a scanner pool [29](#)
- antivirus
 - architecture [5](#)
 - file protection [5](#)
 - supported vendors [11](#)
- Antivirus Connector
 - adding SVMs to [14](#)
 - configuring [13](#)
 - installing [12](#)
 - modifying SVM connection details [15](#)
 - removing SVMs from [16](#)
- antivirus software
 - configuring [12](#)
 - installing [12](#)

C

- CIFS share
 - configuring vscan fileop profile [20](#)
- components
 - of antivirus architecture [5](#)
- configuring
 - Antivirus Connector [13](#)
 - antivirus software [12](#)
 - virus scanning [17](#)
 - vscan fileop profile [20](#)
- creating
 - on-access policies [19](#)
 - scanner pools [17](#)

D

- deleting
 - on-access policy [33](#)
 - privileged users from a scanner pool [27](#)
 - scanner pools [26](#)
 - Vscan servers from a scanner pool [29](#)
- disabling
 - on-access policies [32](#)
 - virus scanning [22](#)

E

- enabling
 - on-access policies [20](#)
 - virus scanning [21](#)

F

- file protection
 - using antivirus [5](#)
- files
 - resetting the status of scanned files [22](#)

H

- how virus scanning works [8](#)

I

- installing
 - Antivirus Connector [12](#)
 - antivirus software [12](#)

M

- managing
 - on-access policies [31](#)
 - scanner pools [24](#)
- managing virus scanning
 - workflow [9](#)
- modifying
 - on-access policies [32](#)
 - scanner pool [25](#)
- monitoring
 - status and performance activities [34](#)

O

- on-access policies
 - creating [19](#)
 - deleting [33](#)
 - disabling [32](#)
 - enabling [20](#)
 - managing [31](#)
 - modifying [32](#)

P

preparing

- setting up Vscan server [10](#)

privileged users

- adding to scanner pool [27](#)
- removing from a scanner pool [27](#)
- viewing, of scanner pool [28](#)

R

removing

- privileged users from a scanner pool [27](#)
- Vscan servers from a scanner pool [29](#)

requirements

- Antivirus Connector [10](#)
- antivirus software [10](#)

resetting

- status of scanned files [22](#)

S

scanned files

- resetting the status of [22](#)

scanner policies

- applying to a scanner pool [18](#)

scanner pools

- adding privileged users [27](#)
- adding Vscan servers [29](#)
- applying a scanner policy [18](#)
- creating [17](#)
- deleting [26](#)
- managing [24](#)
- modifying [25](#)
- removing privileged users [27](#)
- removing Vscan servers [29](#)
- viewing privileged users [28](#)
- viewing Vscan servers [30](#)

setting up virus scanning

- workflow [9](#)

status and performance activities

- monitoring [34](#)

SVMs

- adding to Antivirus Connector [14](#)
- creating on-access policies for [19](#)
- creating scanner pools for [17](#)
- deleting on-access policies [33](#)
- deleting scanner pools [26](#)
- disabling on-access policies on [32](#)
- disabling virus scanning on [22](#)

- enabling on-access policies on [20](#)

- enabling virus scanning on [21](#)

- modifying Antivirus Connector connection details [15](#)

- modifying on-access policies for [32](#)

- modifying scanner pools [25](#)

- removing from Antivirus Connector [16](#)

- resetting the status of scanned files [22](#)

- viewing active scanner pools [25](#)

- viewing on-access policies [31](#)

- viewing scanner pools [24](#)

U

users

- adding privileged users to scanner pools [27](#)

- removing privileged users from scanner pools [27](#)

V

vendors

- supported antivirus software [11](#)

viewing

- active scanner pools of an SVM [25](#)

- connection status of Vscan servers [34](#)

- on-access policies of all SVM [31](#)

- privileged users of a scanner pool [28](#)

- scanner pool of an SVM [24](#)

- Vscan servers of scanner pools [30](#)

- Vscan statistics [34](#)

virus scanning

- configuring [17](#)

- disabling [22](#)

- enabling [21](#)

- how it works [8](#)

Vscan

- viewing statistics [34](#)

Vscan server

Vscan servers

- adding to a scanner pool [29](#)

- Antivirus Connector [10](#)

- antivirus software [10](#)

- commands for viewing connection status [34](#)

- components described [5](#)

- configuring [12](#)

- removing from a scanner pool [29](#)

- viewing, of scanner pool [30](#)

Vservers

- See* SVMs

W

workflow

setting up and managing virus scanning [9](#)