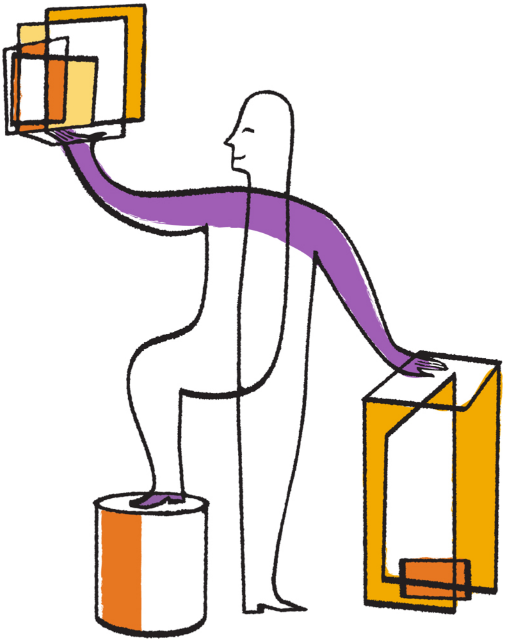
Clustered Data ONTAP® 8.3

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: 215-09137_A0
November 2014

Contents

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.

Privileged user

A privileged user is a domain user account that the Vscan server uses to connect to the SVM. The user account specified in the scanner pool configuration is designated as the privileged user.

Scanner policy

A scanner policy defines when the scanner pool is 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 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 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) is different from `execute` permission on the file.

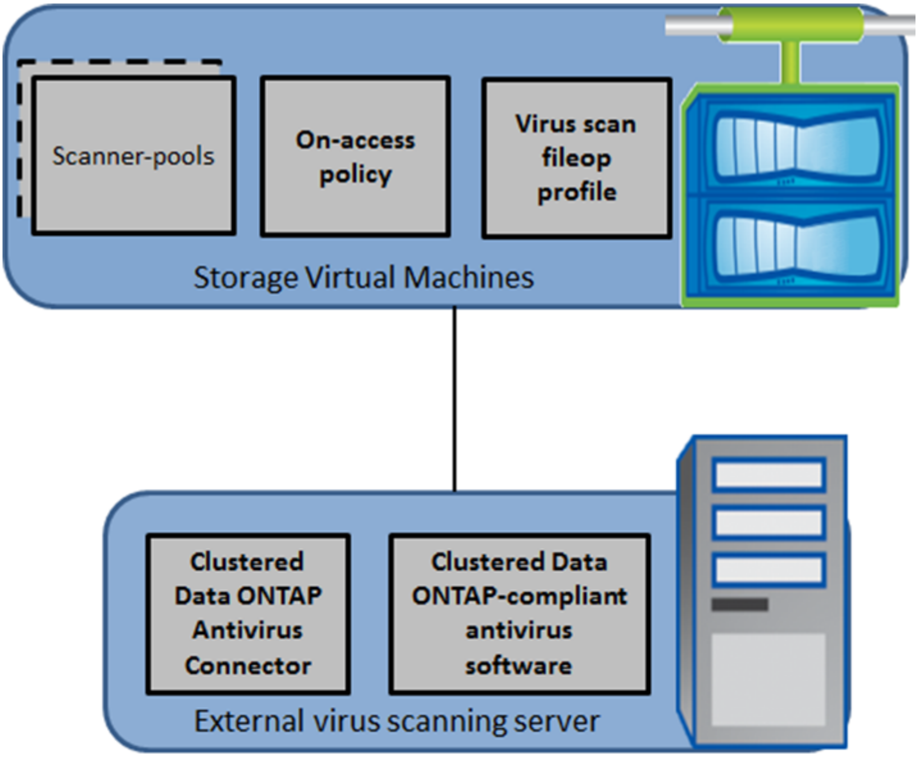
You can also choose not to use any of the filters by setting this parameter to **`"-"`**. This will cause file accesses to be allowed even if the files are not scanned. Also, only read-write volumes are considered for scanning.

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:

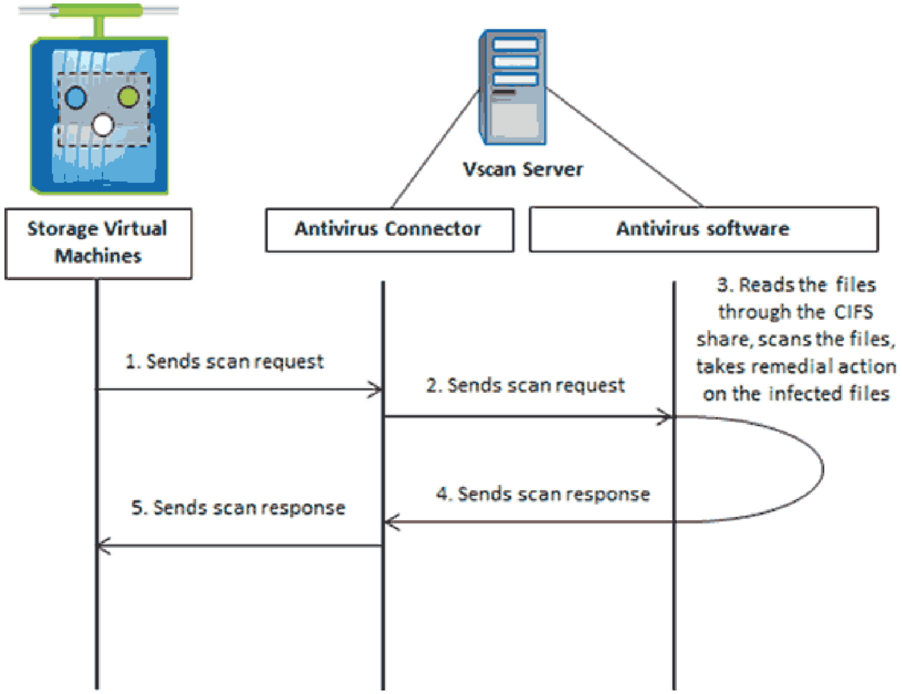
- no-scan: Virus scans are never triggered for this share.
- standard: Virus scans can be triggered by open, close, and rename operations. This is the default profile.
- strict: Virus scans can be triggered by open, read, close, and rename operations. The strict profile provides better security when multiple clients access a file for read and write operations simultaneously while the file is not reopened or closed. This profile makes sure that the read operations trigger virus scanning if the file is modified after it was scanned.
- writes-only: Virus scans can be triggered only when a file that has been modified is closed.


Scanner-pools
On-access policy
Virus scan fileop profile
Storage Virtual Machines
Clustered Data ONTAP Antivirus Connector
Clustered Data ONTAP-compliant antivirus software
External virus scanning server

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):



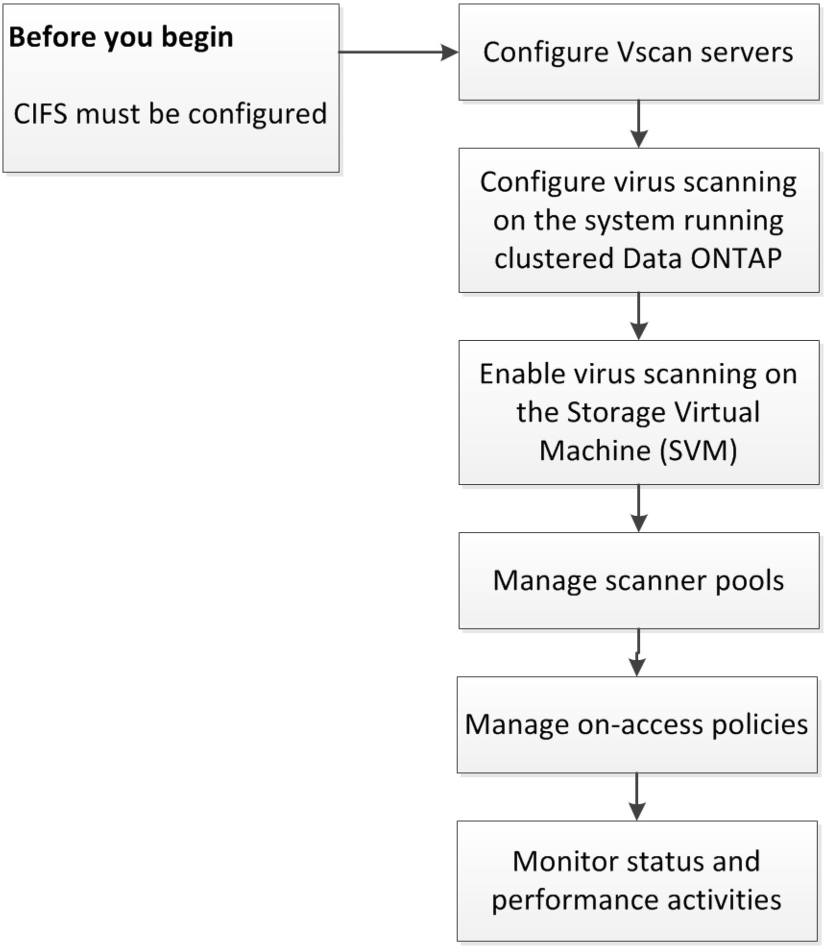
1. When a file is accessed by a client, in a way that it matches the on-access policy that has been set for an SVM and the `Vscan file-operations profile` parameter that has been set for the CIFS shares, a scan request is sent from the SVM to the Vscan server.
2. The Antivirus Connector receives the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



Before you begin
CIFS must be configured
Configure Vscan servers
Configure virus scanning on the system running clustered Data ONTAP
Enable virus scanning on the Storage Virtual Machine (SVM)
Manage scanner pools
Manage on-access policies
Monitor status and performance 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
  - Windows 2012 R2

  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 *mysupport.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. You must follow the specific steps listed in the vendor documentation to configure the antivirus scanning solution for your clustered Data ONTAP environment. If you do not follow the steps mentioned in the vendor documentation, then your antivirus scanning solution might fail or cause performance issues or service disruptions.

Related concepts

Requirements for Vscan servers on page 10

Supported antivirus vendors on page 11

Information about installing and configuring the Antivirus Connector

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

For information about installing and configuring the Antivirus Connector, see the readme file that is provided along with the Antivirus Connector setup.

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.

Configuring virus scanning for a MetroCluster configuration

In a MetroCluster configuration, you must set up and configure Vscan servers separately for both, the local cluster and the partner cluster.

You must create separate scanner pools for the source and destination SVM in the local cluster. You must apply the scanner policy to the scanner pool and specify the cluster on which you want to use the scanner pool by using the `cluster` parameter in the `vserver vscan scanner-pool apply-policy` command. During a disaster, if the local cluster fails, then the partner cluster takes over the operations and uses the scanner pools applied to the destination SVM to allow the Vscan servers and privileged users local to that cluster to access the SVM.

Related tasks

Applying a scanner policy to a scanner pool on page 14

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 the 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 explicitly on each SVM, 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.
- You must add the user, which is used by the vendor's scan engine service, to the list of privileged users of the scanner pool.

- When you are creating a scanner pool for a MetroCluster configuration, you must limit the name of the scanner pool to 200 characters.

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 20

Related tasks

Applying a scanner policy to a scanner pool on page 14

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 21

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.
- When you are creating an on-access policy for a MetroCluster configuration, you must limit the name of the on-access policy to 200 characters.

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 27

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 28

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 is not performed on CIFS shares for which the `continuously-available` parameter is set to `Yes`.

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.

Related information

Clustered Data ONTAP 8.3 File Access Management Guide for CIFS

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 17

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

        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 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 13

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 13

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 21

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 21

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 21

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 21

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 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 15

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 16

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 15

Monitoring Vscan server status

You can monitor the Vscan server status by viewing the information about the Vscan server connection. This information helps you in diagnosing issues related to the Vscan server.

Considerations for working with the Vscan server connection

You have to take into account a list of considerations when you are working with Vscan server connections.

- Before enabling the client access for the Storage Virtual Machine (SVM), you must ensure that at least one Vscan server is connected to SVM on each node that has a LIF. If not, the client access is denied when `scan-mandatory` option is set. If you need to enable Vscan while SVM is serving file-accesses, you must turn off the `scan-mandatory` option and then allow the Vscan server to connect to the clustered Data ONTAP system. You can turn on the `scan-mandatory` option after the Vscan server is connected to the clustered Data ONTAP system.
- Before migrating a LIF, you must ensure that the target LIF does not host all the scanner connections for any SVM. If it does, then the connection between the scanner and the SVM is lost. To ensure that file-accesses are not denied because of non-availability of scanner connections, you must turn off the `scan-mandatory` option from the active on-access policy, disable the LIF, and monitor the vscan connection-status for re-connection of scanners before migrating the LIF.

  Note: It is recommended that Vscan server is connected to clustered Data ONTAP over a separate network than the one used for client access, and each SVM has at least two or more Vscan servers assigned to it.

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`

If you want to...	**Enter the following command...**
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.

Copyright information

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

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

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

Trademark information

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