Antivirus configuration

ONTAP 9

NetApp
July 19, 2023

Table of Contents

Antivirus configuration

Antivirus configuration overview

Vscan is an antivirus scanning solution developed by NetApp that allows customers to protect their data from being compromised by viruses or other malicious code.

Vscan performs virus scans when clients access files over SMB. You can configure Vscan to scan on-demand or on a schedule. You can interact with Vscan using the ONTAP command-line interface (CLI) or ONTAP application programming interfaces (APIs).

Related information

Trellix (formerly McAfee) Endpoint Security Storage Protection

Symantec Protection Engine

NetApp Technical Report 4312: Antivirus Solution for Clustered Data ONTAP Trend Micro

About NetApp antivirus protection

About NetApp virus scanning

Vscan is an antivirus scanning solution developed by NetApp that allows customers to protect their data from being compromised by viruses or other malicious code. It combines partner-provided antivirus software with ONTAP features to give customers the flexibility they need to manage file scanning.

How virus scanning works

Storage systems offload scanning operations to external servers hosting antivirus software from third-party vendors.

Based on the active scanning mode, ONTAP sends scan requests when clients access files over SMB (on-access) or access files in specific locations, on a schedule or immediately (on-demand).

- You can use *on-access scanning* to check for viruses when clients open, read, rename, or close files over SMB. File operations are suspended until the external server reports the scan status of the file. If the file has already been scanned, ONTAP allows the file operation. Otherwise, it requests a scan from the server.

  On-access scanning is not supported for NFS.

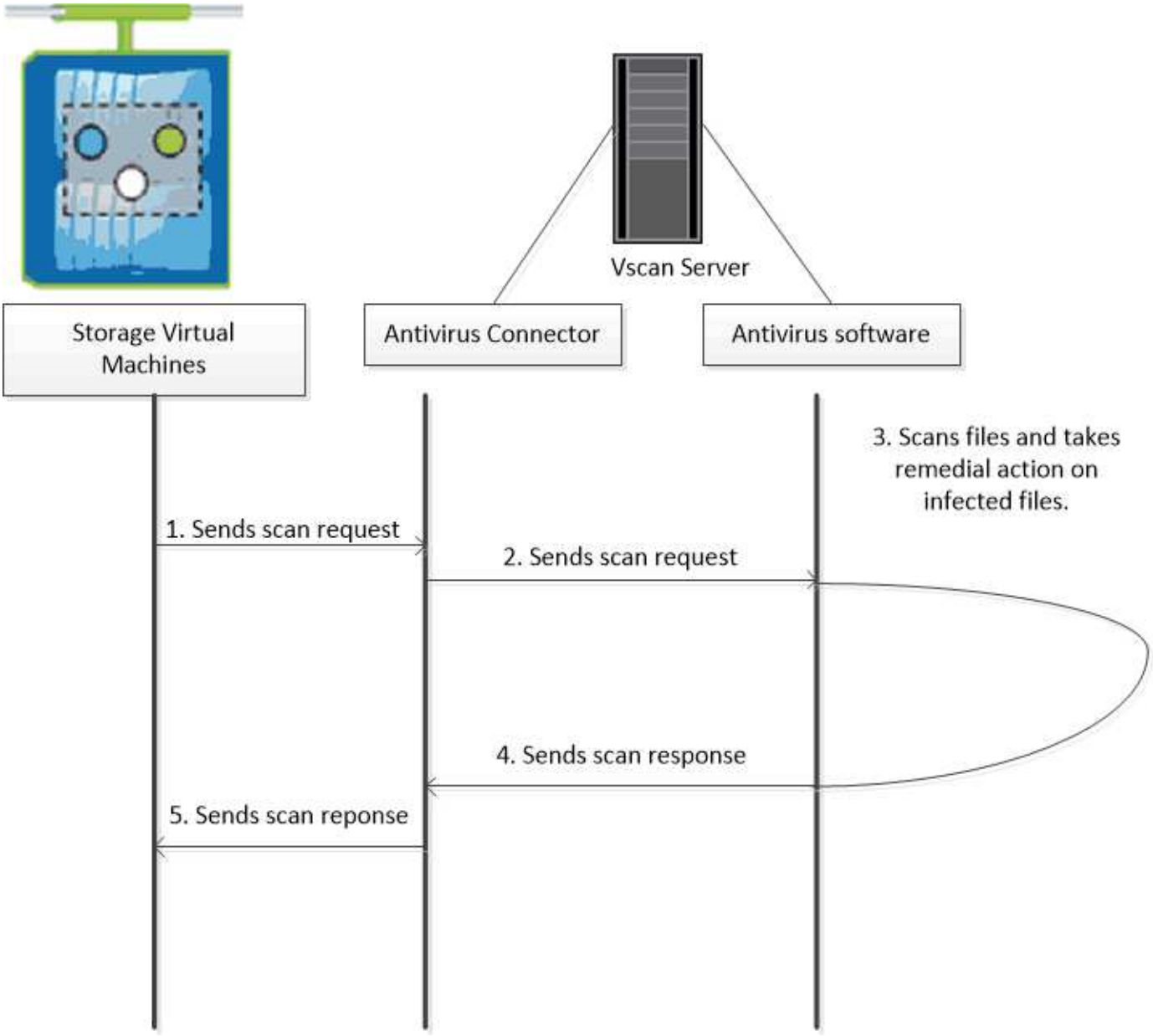
- You can use *on-demand scanning* to check files for viruses immediately or on a schedule. We recommend that on-demand scans run only in off-peak hours to avoid overloading existing AV infrastructure, which is normally sized for on-access scanning. The external server updates the scan status of checked files, so that file-access latency is reduced over SMB. If there were file modifications or software version updates, it requests a new file scan from the external server.

  You can use on-demand scanning for any path in the SVM namespace, even for volumes that are exported only through NFS.

You typically enable both on-access and on-demand scanning modes on an SVM. In either mode, the antivirus

software takes remedial action on infected files based on your software settings.

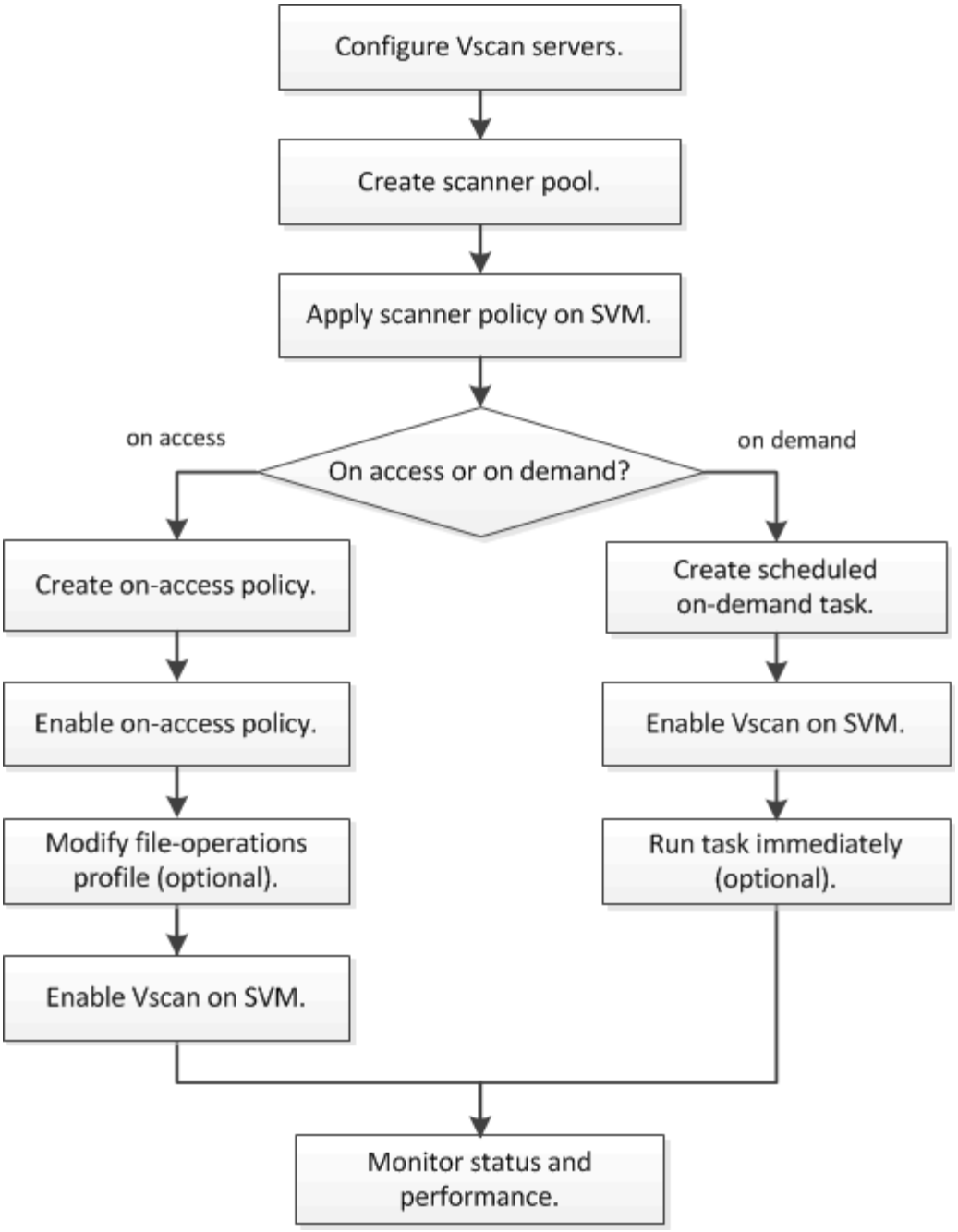
The ONTAP Antivirus Connector, provided by NetApp and installed on the external server, handles communication between the storage system and the antivirus software.



Virus scanning workflow

You must create a scanner pool and apply a scanner policy before you can enable scanning. You typically enable both on-access and on-demand scanning modes on an SVM.

You must have completed the CIFS configuration.



Antivirus architecture

The NetApp antivirus architecture consists of Vscan server software and associated settings.

Vscan server software

You must install this software on the Vscan server.

- **ONTAP Antivirus Connector**

  This is NetApp-provided software that handles scan request and response communication between the SVMs and antivirus software. It can run on a virtual machine, but for best performance use a physical machine. You can download this software from the NetApp Support Site (requires login).

- **Antivirus software**

  This is partner-provided software that scans files for viruses or other malicious code. You specify the remedial actions to be taken on infected files when you configure the software.

Vscan software settings

You must configure these software settings on the Vscan server.

- **Scanner pool**

  This setting defines the Vscan servers and privileged users that can connect to SVMs. It also defines a scan request timeout period, after which the scan request is sent to an alternative Vscan server if one is available.

  > ⓘ You should set the timeout period in the antivirus software on the Vscan server to five seconds less than the scanner-pool scan-request timeout period. This will avoid situations in which file access is delayed or denied altogether because the timeout period on the software is greater than the timeout period for the scan request.

- **Privileged user**

  This setting is a domain user account that a Vscan server uses to connect to the SVM. The account must exist in the list of privileged users in the scanner pool.

- **Scanner policy**

  This setting determines whether a scanner pool is active. Scanner policies are system-defined, so you cannot create custom scanner policies. Only these three policies are available:

  - `Primary` specifies that the scanner pool is active.
  - `Secondary` specifies that the scanner pool is active, only when none of the Vscan servers in the primary scanner pool are connected.
  - `Idle` specifies that the scanner pool is inactive.

- **On-access policy**

  This setting defines the scope of an on-access scan. You can specify the maximum file size to scan, file extensions and paths to include in the scan, and file extensions and paths to exclude from the scan.

  By default, only read-write volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with execute access:

  - `scan-ro-volume` enables scanning of read-only volumes.
  - `scan-execute-access` restricts scanning to files opened with execute access.

    > ⓘ “Execute access” is different from “execute permission.” A given client will have “execute access” on an executable file only if the file was opened with “execute intent.”

  You can set the `scan-mandatory` option to off to specify that file access is allowed when no Vscan servers are available for virus scanning. Within on-access mode you can choose from these two mutually-exclusive options:

- Mandatory: With this option, Vscan tries to deliver the scan request to the server until the timeout period expires. If the scan request is not accepted by the server, then the client access request is denied.
- Non-Mandatory: With this option, Vscan always allows client access, whether or not a Vscan server was available for virus scanning.

- **On-demand task**

  This setting defines the scope of an on-demand scan. You can specify the maximum file size to scan, file extensions and paths to include in the scan, and file extensions and paths to exclude from the scan. Files in subdirectories are scanned by default.

  You use a cron schedule to specify when the task runs. You can use the `vserver vscan on-demand-task run` command to run the task immediately.

- **Vscan file-operations profile (on-access scanning only)**

  The `vscan-fileop-profile` parameter for the `vserver cifs share create` command defines which SMB file operations trigger virus scanning. By default, the parameter is set to `standard`, which is NetApp best practice. You can adjust this parameter as necessary when you create or modify an SMB share:

  - `no-scan` specifies that virus scans are never triggered for the share.
  - `standard` specifies that virus scans are triggered by open, close, and rename operations.
  - `strict` specifies that virus scans are triggered by open, read, close, and rename operations.

    The `strict` profile provides enhanced security for situations in which multiple clients access a file simultaneously. If one client closes a file after writing a virus to it, and the same file remains open on a second client, `strict` ensures that a read operation on the second client triggers a scan before the file is closed.

    You should be careful to restrict the `strict` profile to shares containing files that you anticipate will be accessed simultaneously. Since this profile generates more scan requests, it may impact performance.

  - `writes-only` specifies that virus scans are triggered only when modified files are closed.

    Since `writes-only` generates fewer scan requests, it typically improves performance.

    If you use this profile, the scanner must be configured to delete or quarantine unrepairable infected files, so they cannot be accessed. If, for example, a client closes a file after writing a virus to it, and the file is not repaired, deleted, or quarantined, any client that accesses the file `without` writing to it will be infected.

> If a client application performs a rename operation, the file is closed with the new name and is not scanned. If such operations pose a security concern in your environment, you should use the `standard` or `strict` profile.

Vscan partner solutions

NetApp collaborates with Trellix, Symantec, Trend Micro, and Sentinel One to deliver

industry-leading anti-malware and anti-virus solutions that build upon ONTAP Vscan technology. These solutions help you scan files for malware and remediate any affected files.

As shown in the table below, interoperability details for Trellix, Symantec and Trend Micro are maintained on the NetApp Interoperability Matrix. Interoperability details for Trellix and Symantec can also be found on the partner websites. Interoperability details for Sentinel One and other new partners will be maintained by the partner on their websites.

Partner	Solution documentation	Interoperability details
Trellix (Formerly McAfee)	Trellix Product Documentation	• NetApp Interoperability Matrix Tool • Supported platforms for Endpoint Security Storage Protection (trellix.com)
Symantec	Symantec Protection Engine 9.0.0	• NetApp Interoperability Matrix Tool • Support Matrix for Partner Devices Certified with Symantec Protection Engine (SPE) for Network Attached Storage (NAS) 8.x (broadcom.com)
Trend Micro	Trend Micro ServerProtect for Storage 6.0 Getting Started Guide	NetApp Interoperability Matrix Tool
Sentinel One	Sentinel One support This link requires a user log-in. You can request access from Sentinel One.	

Vscan server installation and configuration

You must set up and configure one or more Vscan servers to enable antivirus scanning.

- To install and configure the antivirus software on the server, follow the instructions provided by your vendor.
- To install and configure the ONTAP Antivirus Connector, follow the instructions in the `README.txt` file available on the NetApp support site.

For disaster recovery and MetroCluster configurations, you must set up and configure separate Vscan servers for the primary/local and secondary/partner ONTAP clusters.

Antivirus software requirements

- For information about antivirus software requirements, see the vendor documentation.
- For information about the vendors, software, and versions supported by Vscan, see the NetApp Interoperability Matrix Tool (IMT).

ONTAP Antivirus Connector requirements

- You can download this software from the NetApp Support Site (requires login).
- For information about software version support, see the NetApp Interoperability Matrix Tool (IMT).

Vscan server configuration requirements

- You must install .NET 3.0 or later and you must enable SMB 2.0 on the Vscan server. For SMB servers with an export policy, you must add all Vscan servers to the policy.
- You can install different versions of Windows Server OS on different Vscan servers in a cluster. At a minimum, ONTAP Antivirus Connector requires Windows Server 2008.

Configure scanner pools

Configure scanner pools overview

A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. A scanner policy determines whether a scanner pool is active.

If you use an export policy on an SMB server, you must add each Vscan server to the export policy.

Create a scanner pool on a single cluster

A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. You can create a scanner pool for an individual SVM or for all the SVMs in a cluster.

What you'll need

- SVMs and Vscan servers must be in the same domain or in trusted domains.
- For scanner pools defined for an individual SVM, you must have configured ONTAP Antivirus Connector with the SVM management LIF or SVM data LIF.
- For scanner pools defined for all the SVMs in a cluster, you must have configured ONTAP Antivirus Connector with the cluster management LIF.
- The list of privileged users must include the domain user account the Vscan server uses to connect to the SVM.
- Once the scanner pool is configured, check the connection status to the servers.

Steps

1. Create a scanner pool:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
privileged_users
```

   - Specify a data SVM for a pool defined for an individual SVM, and specify a cluster admin SVM for a pool defined for all of the SVMs in a cluster.
   - Specify an IP address or FQDN for each Vscan server host name.

◦ Specify the domain and user name for each privileged user. For a complete list of options, see the man page for the command.

The following command creates a scanner pool named `SP` on the `vs1` SVM:

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2
```

2. Verify that the scanner pool was created:

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `SP` scanner pool:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                               Scanner Pool: SP
                             Applied Policy: idle
                             Current Status: off
          Cluster on Which Policy Is Applied: -
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                     List of Privileged Users: cifs\u1, cifs\u2
```

   You can also use the `vserver vscan scanner-pool show` command to view all of the scanner pools on an SVM. For complete command syntax, see the man page for the command.

Create scanner pools in MetroCluster configurations

You must create primary and secondary scanner pools on each cluster in a MetroCluster configuration, corresponding to the primary and secondary SVMs on the cluster.

What you'll need

- SVMs and Vscan servers must be in the same domain or in trusted domains.
- For scanner pools defined for an individual SVM, you must have configured ONTAP Antivirus Connector with the SVM management LIF or SVM data LIF.
- For scanner pools defined for all the SVMs in a cluster, you must have configured ONTAP Antivirus Connector with the cluster management LIF.

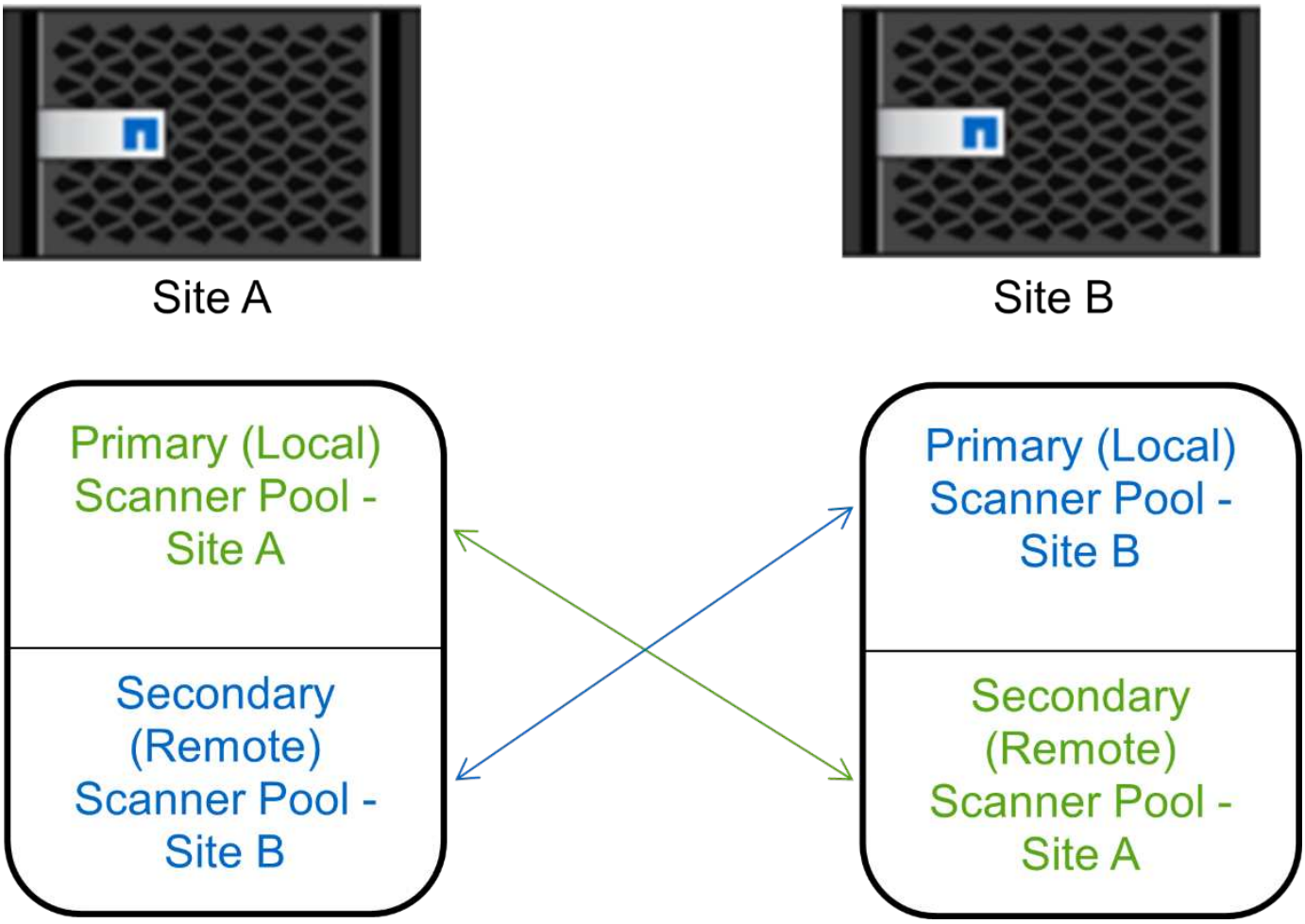
- The list of privileged users must include the domain user account the Vscan server uses to connect to the SVM.
- Once the scanner pool is configured, check the connection status to the servers.

About this task

MetroCluster configurations protect data by implementing two physically separate mirrored clusters. Each cluster synchronously replicates the data and SVM configuration of the other. A primary SVM on the local cluster serves data when the cluster is online. A secondary SVM on the local cluster serves data when the remote cluster is offline.

This means that you must create primary and secondary scanner pools on each cluster in a MetroCluster configuration, The secondary pool becomes active when the cluster begins serving data from the secondary SVM. For Disaster Recovery (DR) the configuration is similar to MetroCluster.

This figure shows a typical MetroCluster/DR configuration.



Steps

1. Create a scanner pool:

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - Specify a data SVM for a pool defined for an individual SVM, and specify a cluster admin SVM for a

pool defined for all the SVMs in a cluster.

- Specify an IP address or FQDN for each Vscan server host name.
- Specify the domain and user name for each privileged user.

> You must create all scanner pools from the cluster containing the primary SVM.

For a complete list of options, see the man page for the command.

The following commands create primary and secondary scanner pools on each cluster in a MetroCluster configuration:

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Verify that the scanner pools were created:

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   For a complete list of options, see the man page for the command.

   The following command displays the details for the scanner pool `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: idle
                              Current Status: off
         Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

You can also use the `vserver vscan scanner-pool show` command to view all of the scanner pools on an SVM. For complete command syntax, see the man page for the command.

Apply a scanner policy on a single cluster

A scanner policy determines whether a scanner pool is active. You must activate a scanner pool before the Vscan servers that it defines can connect to an SVM.

About this task

- You can apply only one scanner policy to a scanner pool.
- If you created a scanner pool for all the SVMs in a cluster, you must apply a scanner policy on each SVM individually.

Steps

1. Apply a scanner policy:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   A scanner policy can have one of the following values:

   - `Primary` specifies that the scanner pool is active.
   - `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool are connected.
   - `Idle` specifies that the scanner pool is inactive.

   The following example shows that the scanner pool named `SP` on the `vs1` SVM is active:

   ```
   cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
   -scanner-pool SP  -scanner-policy primary
   ```

2. Verify that the scanner pool is active:

   ```
   vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool
   ```

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `SP` scanner pool:

   ```
   cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
   SP

                                       Vserver: vs1
                                  Scanner Pool: SP
                                Applied Policy: primary
                                Current Status: on
            Cluster on Which Policy Is Applied: cluster1
                     Scanner Pool Config Owner: vserver
           List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
   List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
   27.fsct.nb
                      List of Privileged Users: cifs\u1, cifs\u2
   ```

   You can use the `vserver vscan scanner-pool show-active` command to view the active scanner pools on an SVM. For the complete command syntax, see the man page for the command.

Apply scanner policies in MetroCluster configurations

A scanner policy determines whether a scanner pool is active. You must apply a scanner policy to the primary and secondary scanner pools on each cluster in a MetroCluster configuration.

About this task

- You can apply only one scanner policy to a scanner pool.
- If you created a scanner pool for all the SVMs in a cluster, you must apply a scanner policy on each SVM individually.
- For disaster recovery and MetroCluster configurations, you must apply a scanner policy to every scanner pool in the local cluster and remote cluster.
- In the policy that you create for the local cluster, you must specify the local cluster in the `cluster` parameter. In the policy that you create for the remote cluster, you must specify the remote cluster in the `cluster` parameter. The remote cluster can then take over virus scanning operations in case of a disaster.

Steps

1. Apply a scanner policy:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   ```

cluster_to_apply_policy_on

A scanner policy can have one of the following values:

- `Primary` specifies that the scanner pool is active.
- `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool are connected.
- `Idle` specifies that the scanner pool is inactive.

> You must apply all scanner policies from the cluster containing the primary SVM.

The following commands apply scanner policies to the primary and secondary scanner pools on each cluster in a MetroCluster configuration:

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster
cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. Verify that the scanner pool is active:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

For a complete list of options, see the man page for the command.

The following command displays the details for the scanner pool `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: primary
                              Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                   Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

You can use the `vserver vscan scanner-pool show-active` command to view the active scanner pools on an SVM. For complete command syntax, see the man page for the command.

Commands for managing scanner pools

You can modify and delete scanner pools, and manage privileged users and Vscan servers for a scanner pool. You can also view summary information about the scanner pool.

If you want to…	Enter the following command…
Modify a scanner pool	`vserver vscan scanner-pool modify`
Delete a scanner pool	`vserver vscan scanner-pool delete`
Add privileged users to a scanner pool	`vserver vscan scanner-pool privileged-users add`
Delete privileged users from a scanner pool	`vserver vscan scanner-pool privileged-users remove`
Add Vscan servers to a scanner pool	`vserver vscan scanner-pool servers add`
Delete Vscan servers from a scanner pool	`vserver vscan scanner-pool servers remove`
View summary and details for a scanner pool	`vserver vscan scanner-pool show`
View privileged users for a scanner pool	`vserver vscan scanner-pool privileged-users show`

View Vscan servers for all scanner pools	`vserver vscan scanner-pool servers show`

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

Configure on-access scanning

Create an on-access policy

An on-access policy defines the scope of an on-access scan. You can create an on-access policy for an individual SVM or for all the SVMs in a cluster. If you created an on-access policy for all the SVMs in a cluster, you must enable the policy on each SVM individually.

About this task

- You can specify the maximum file size to scan, file extensions and paths to include in the scan, and file extensions and paths to exclude from the scan.
- You can set the `scan-mandatory` option to off to specify that file access is allowed when no Vscan servers are available for virus scanning.
- By default, ONTAP creates an on-access policy named "default_CIFS" and enables it for all the SVMs in a cluster.
- Any file that qualifies for scan exclusion based on the `paths-to-exclude`, `file-ext-to-exclude`, or `max-file-size` parameters is not considered for scanning, even if the `scan-mandatory` option is set to on. (Check this troubleshooting section for connectivity issues related to the `scan-mandatory` option.)
- By default, only read-write volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with execute access.
- Virus scanning is not performed on an SMB share for which the continuously-available parameter is set to Yes.
- See the Antivirus architecture section for details about the *Vscan file-operations profile*.
- You can create a maximum of ten (10) on-access policies per SVM. However, you can enable only one on-access policy at a time.
  - You can exclude a maximum of one hundred (100) paths and file extensions from virus scanning in an on-access policy.
- Some file exclusion recommendations:
  - Consider excluding large files (file size can be specified) from virus scanning because they can result in a slow response or scan request timeouts for CIFS users. The default file size for exclusion is 2GB.
  - Consider excluding file extensions such as `.vhd` and `.tmp` because files with these extensions might not be appropriate for scanning.
  - Consider excluding file paths such as the quarantine directory or paths in which only virtual hard drives or databases are stored.
  - Verify that all exclusions are specified in the same policy, because only one policy can be enabled at a time. NetApp highly recommends having the same set of exclusions specified in the antivirus engine.

Steps

1. Create an on-access policy:

`vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM -policy-name policy_name -protocol CIFS -max-file-size max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access] -file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to -exclude paths_of_files_to_exclude -scan-mandatory on|off`

- Specify a data SVM for a policy defined for an individual SVM, a cluster admin SVM for a policy defined for all the SVMs in a cluster.
- The `-file-ext-to-exclude` setting overrides the `-file-ext-to-include` setting.
- Set `-scan-files-with-no-ext` to true to scan files without extensions. The following command creates an on-access policy named `Policy1` on the `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
-file-ext-to-include “mp*”,"tx*" -file-ext-to-exclude "mp3","txt" -scan
-files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
```

2. Verify that the on-access policy has been created: `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name policy_name`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `Policy1` policy:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: off
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

Enable an on-access policy

An on-access policy defines the scope of an on-access scan. You must enable an on-access policy on an SVM before its files can be scanned.

If you created an on-access policy for all the SVMs in a cluster, you must enable the policy on each SVM individually. You can enable only one on-access policy on an SVM at a time.

Steps

1. Enable an on-access policy:

   `vserver vscan on-access-policy enable -vserver data_SVM -policy-name policy_name`

   The following command enables an on-access policy named `Policy1` on the `vs1` SVM:

   ```
   cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
   -name Policy1
   ```

2. Verify that the on-access policy is enabled:

   `vserver vscan on-access-policy show -instance *data_SVM* -policy-name *policy_name*`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `Policy1` on-access policy:

   ```
   cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
   -name Policy1

                               Vserver: vs1
                                Policy: Policy1
                         Policy Status: on
                  Policy Config Owner: vserver
                File-Access Protocol: CIFS
                               Filters: scan-ro-volume
                        Mandatory Scan: on
   Max File Size Allowed for Scanning: 3GB
               File Paths Not to Scan: \vol\a b\, \vol\a,b\
          File Extensions Not to Scan: mp3, txt
              File Extensions to Scan: mp*, tx*
         Scan Files with No Extension: false
   ```

Modify the Vscan file-operations profile for an SMB share

The *Vscan file-operations profile* for an SMB share defines the operations on the share that can trigger scanning. By default, the parameter is set to `standard`. You can adjust the parameter as necessary when you create or modify an SMB share.

See the Antivirus architecture section for details about the *Vscan file-operations profile*.

Virus scanning is not performed on an SMB share that has the `continuously-available` parameter set to `Yes`.

Step

1. Modify the value of the Vscan file-operations profile for an SMB share:

   `vserver cifs share modify -vserver` *`data_SVM`* `-share-name` *`share`* `-path` *`share_path`* `-vscan-fileop-profile no-scan|standard|strict|writes-only`

   For a complete list of options, see the man page for the command.

   The following command changes the Vscan file operations profile for an SMB share to `strict`:

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

Commands for managing on-access policies

You can modify, disable, or delete an on-access policy. You can view a summary and details for the policy.

If you want to…	Enter the following command…
Create an on-access policy	`vserver vscan on-access-policy create`
Modify an on-access policy	`vserver vscan on-access-policy modify`
Enable an on-access policy	`vserver vscan on-access-policy enable`
Disable an on-access policy	`vserver vscan on-access-policy disable`
Delete an on-access policy	`vserver vscan on-access-policy delete`
View summary and details for an on-access policy	`vserver vscan on-access-policy show`
Add to the list of paths to exclude	`vserver vscan on-access-policy paths-to-exclude add`
Delete from the list of paths to exclude	`vserver vscan on-access-policy paths-to-exclude remove`
View the list of paths to exclude	`vserver vscan on-access-policy paths-to-exclude show`

Add to the list of file extensions to exclude	`vserver vscan on-access-policy file-ext-to-exclude add`
Delete from the list of file extensions to exclude	`vserver vscan on-access-policy file-ext-to-exclude remove`
View the list of file extensions to exclude	`vserver vscan on-access-policy file-ext-to-exclude show`
Add to the list of file extensions to include	`vserver vscan on-access-policy file-ext-to-include add`
Delete from the list of file extensions to include	`vserver vscan on-access-policy file-ext-to-include remove`
View the list of file extensions to include	`vserver vscan on-access-policy file-ext-to-include show`

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

Configure on-demand scanning

Configure on-demand scanning overview

You can use on-demand scanning to check files for viruses immediately or on a schedule.

You might want to run scans only in off-peak hours, for example, or you might want to scan very large files that were excluded from an on-access scan. You can use a cron schedule to specify when the task runs.

About this topic

- You can assign a schedule when you create a task.
- Only one task can be scheduled at a time on an SVM.
- On-demand scanning does not support scanning of symbolic links or stream files.

Create an on-demand task

An on-demand task defines the scope of an on-demand scan. You can specify the maximum size of the files to be scanned, the extensions and paths of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan. Files in subdirectories are scanned by default.

About this task

- A maximum of ten (10) on-demand tasks can exist for each SVM, but only one can be active.
- An on-demand task creates a report, which has information regarding the statistics related to the scans. This report is accessible with a command or by downloading the report file created by the task at the location defined.

Steps

1. Create an on-demand task:

   ```
   vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
   -scan-paths paths_of_files_to_scan -report-directory report_directory_path
   -report-expiry-time expiration_time_for_report -schedule cron_schedule -max
   -file-size max_size_of_files_to_scan -paths-to-exclude
   paths_of_files_to_exclude -file-ext-to-exclude extensions_of_files_to_exclude
   -file-ext-to-include extensions_of_files_to_include -scan-files-with-no-ext
   true|false -directory-recursion true|false
   ```

   - The `-file-ext-to-exclude` setting overrides the `-file-ext-to-include` setting.
   - Set `-scan-files-with-no-ext` to true to scan files without extensions.

   For a complete list of options, see the man page for the command.

   The following command creates an on-access task named `Task1` on the `vs1` SVM:

   ```
   cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
   Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
   -schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
   -file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
   -scan-files-with-no-ext false
   [Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
   command to view the status.
   ```

   > You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job.

2. Verify that the on-demand task has been created:

   ```
   vserver vscan on-demand-task show -instance data_SVM -task-name task_name
   ```

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `Task1` task:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

After you finish

You must enable scanning on the SVM before the task is scheduled to run.

Schedule an on-demand task

You can create a task without assigning a schedule and use the `vserver vscan on-demand-task schedule` command to assign a schedule; or add a schedule while creating the task.

About this task

The schedule assigned with the `vserver vscan on-demand-task schedule` command overrides a schedule already assigned with the `vserver vscan on-demand-task create` command.

Steps

1. Schedule an on-demand task:

   ```
   vserver vscan on-demand-task schedule -vserver data_SVM -task-name task_name
   -schedule cron_schedule
   ```

   The following command schedules an on-access task named `Task2` on the `vs2` SVM:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

> You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job.

2. Verify that the on-demand task has been scheduled:

   `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   For a complete list of options, see the man page for the command.

   The following command displays the details for the `Task 2` task:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                          Vserver: vs2
                        Task Name: Task2
               List of Scan Paths: /vol1/, /vol2/cifs/
            Report Directory Path: /report
                     Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
           File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: info
```

After you finish

You must enable scanning on the SVM before the task is scheduled to run.

Run an on-demand task immediately

You can run an on-demand task immediately, whether or not you have assigned a schedule.

What you'll need

You must have enabled scanning on the SVM.

Step

1. Run an on-demand task immediately:

   `vserver vscan on-demand-task run -vserver data_SVM -task-name task_name`

   The following command runs an on-access task named `Task1` on the `vs1` SVM:

   ```
   cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
   Task1
   [Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
   command to view the status.
   ```

   You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job.

Commands for managing on-demand tasks

You can modify, delete, or unschedule an on-demand task. You can view a summary and details for the task, and manage reports for the task.

If you want to…	Enter the following command…
Create an on-demand task	`vserver vscan on-demand-task create`
Modify an on-demand task	`vserver vscan on-demand-task modify`
Delete an on-demand task	`vserver vscan on-demand-task delete`
Run an on-demand task	`vserver vscan on-demand-task run`
Schedule an on-demand task	`vserver vscan on-demand-task schedule`
Unschedule an on-demand task	`vserver vscan on-demand-task unschedule`
View summary and details for an on-demand task	`vserver vscan on-demand-task show`
View on-demand reports	`vserver vscan on-demand-task report show`
Delete on-demand reports	`vserver vscan on-demand-task report delete`

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

Enable virus scanning on an SVM

You must enable virus scanning on an SVM before an on-access or on-demand scan can run.

Steps

1. Enable virus scanning on an SVM:

   `vserver vscan enable -vserver data_SVM`

   > You can use the `vserver vscan disable` command to disable virus scanning, if necessary.

   The following command enables virus scanning on the `vs1` SVM:

   ```
   cluster1::> vserver vscan enable -vserver vs1
   ```

2. Verify that virus scanning is enabled on the SVM:

   `vserver vscan show -vserver data_SVM`

   For a complete list of options, see the man page for the command.

   The following command displays the Vscan status of the `vs1` SVM:

   ```
   cluster1::> vserver vscan show -vserver vs1

                               Vserver: vs1
                          Vscan Status: on
   ```

Reset the status of scanned files

Occasionally, you might want to reset the scan status of successfully scanned files on an SVM by using the `vserver vscan reset` command to discard the cached information for the files. You might want to use this command to restart the virus scanning processing in case of a misconfigured scan, for example.

About this task

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

> This command can affect performance adversely, depending on the number and size of the files to be rescanned.

What you'll need

Advanced privileges are required for this task.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Reset the status of scanned files:

   ```
   vserver vscan reset -vserver data_SVM
   ```

   The following command resets the status of scanned files on the `vs1` SVM:

   ```
   cluster1::> vserver vscan reset -vserver vs1
   ```

View Vscan event log information

You can use the `vserver vscan show-events` command to view event log information about infected files, updates to Vscan servers, and the like. You can view event information for the cluster or for given nodes, SVMs, or Vscan servers.

What you'll need

Advanced privileges are required for this task.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. View Vscan event log information:

   ```
   vserver vscan show-events
   ```

   For a complete list of options, see the man page for the command.

   The following command displays event log information for the cluster `cluster1`:

```
cluster1::*> vserver vscan show-events

Vserver     Node              Server          Event Type         Event Time
----------- ---------------- --------------- -----------------
-----------------
vs1         Cluster-01      192.168.1.1     file-infected      9/5/2014
11:37:38
vs1         Cluster-01      192.168.1.1     scanner-updated    9/5/2014
11:37:08
vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

Troubleshoot connectivity issues

Potential connectivity issues involving the scan-mandatory option

You can use the `vserver vscan connection-status show` commands to view information about Vscan server connections that you might find helpful in troubleshooting connectivity issues.

By default, the `scan-mandatory` option for on-access scanning denies file access when a Vscan server connection is not available for scanning. Although this option offers important safety features, it can lead to problems in a few situations.

- Before enabling client access, you must ensure that at least one Vscan server is connected to an SVM on each node that has a LIF. If you need to connect servers to SVMs after enabling client access, you must turn off the `scan-mandatory` option on the SVM to ensure that file access is not denied because a Vscan server connection is not available. You can turn the option back on after the server has been connected.
- If a target LIF hosts all the Vscan server connections for an SVM, the connection between the server and the SVM will be lost if the LIF is migrated. To ensure that file access is not denied because a Vscan server connection is not available, you must turn off the `scan-mandatory` option before migrating the LIF. You can turn the option back on after the LIF has been migrated.

Each SVM should have at least two Vscan servers assigned to it. It is a best practice to connect Vscan servers to the storage system over a different network from the one used for client access.

Commands for viewing Vscan server connection status

You can use the `vserver vscan connection-status show` commands to view summary and detailed information about Vscan server connection status.

If you want to…	Enter the following command…
View a summary of Vscan server connections	`vserver vscan connection-status show`

If you want to…	Enter the following command…
View details for Vscan server connections	`vserver vscan connection-status show-all`
View details for connected Vscan servers	`vserver vscan connection-status show-connected`
View details for available Vscan servers that are not connected	`vserver vscan connection-status show-not-connected`

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

Copyright information

Trademark information