Protect against viruses

ONTAP 9

NetApp
March 08, 2024

Table of Contents

Protect against viruses

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

Vscan partner solutions

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.

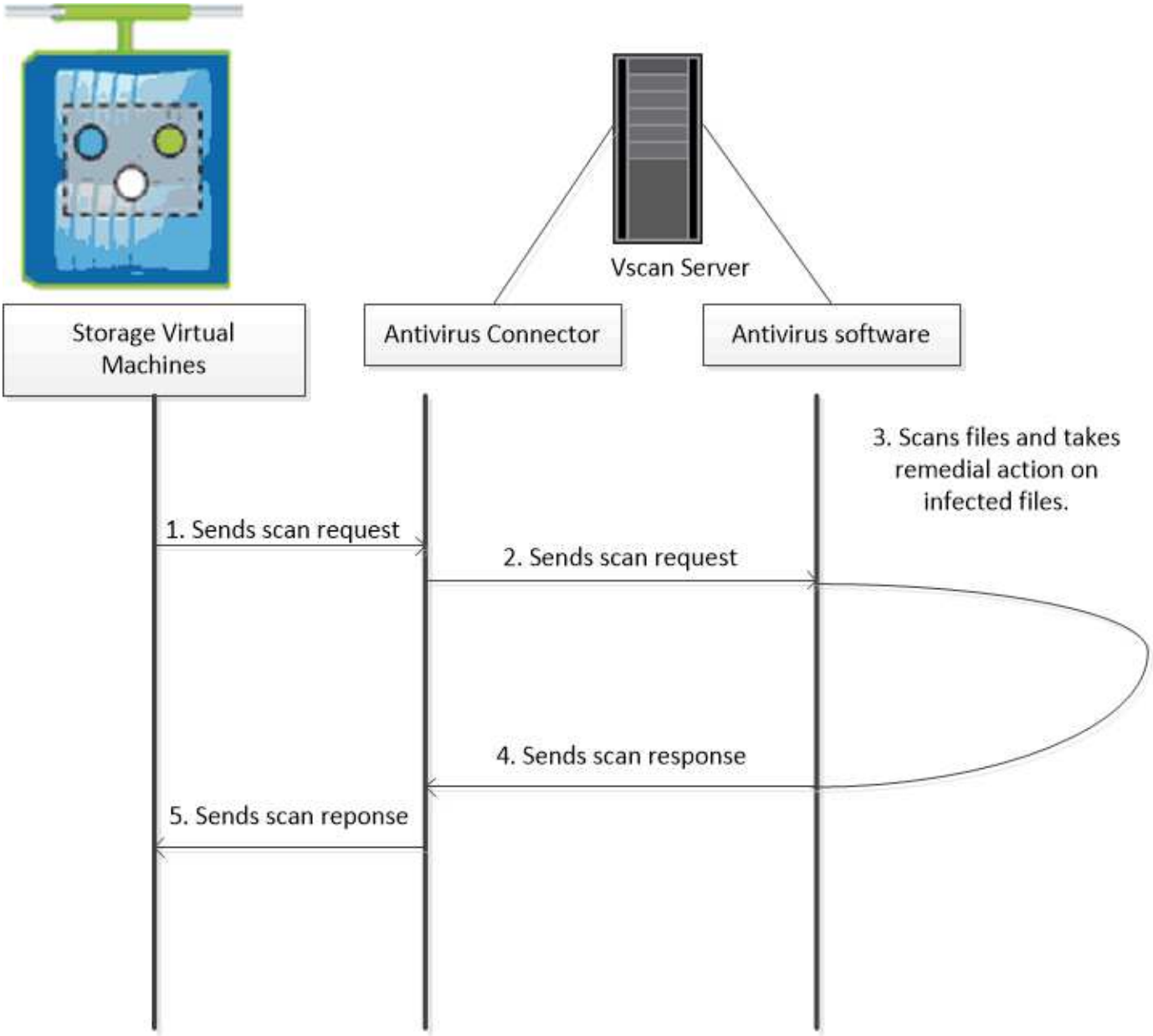
- You can use *on-demand scanning* to check files for viruses immediately or on a schedule. We recommend that on-demand scans run only in off-peak hours to avoid overloading existing AV infrastructure, which is normally sized for on-access scanning. The external server updates the scan status of checked 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

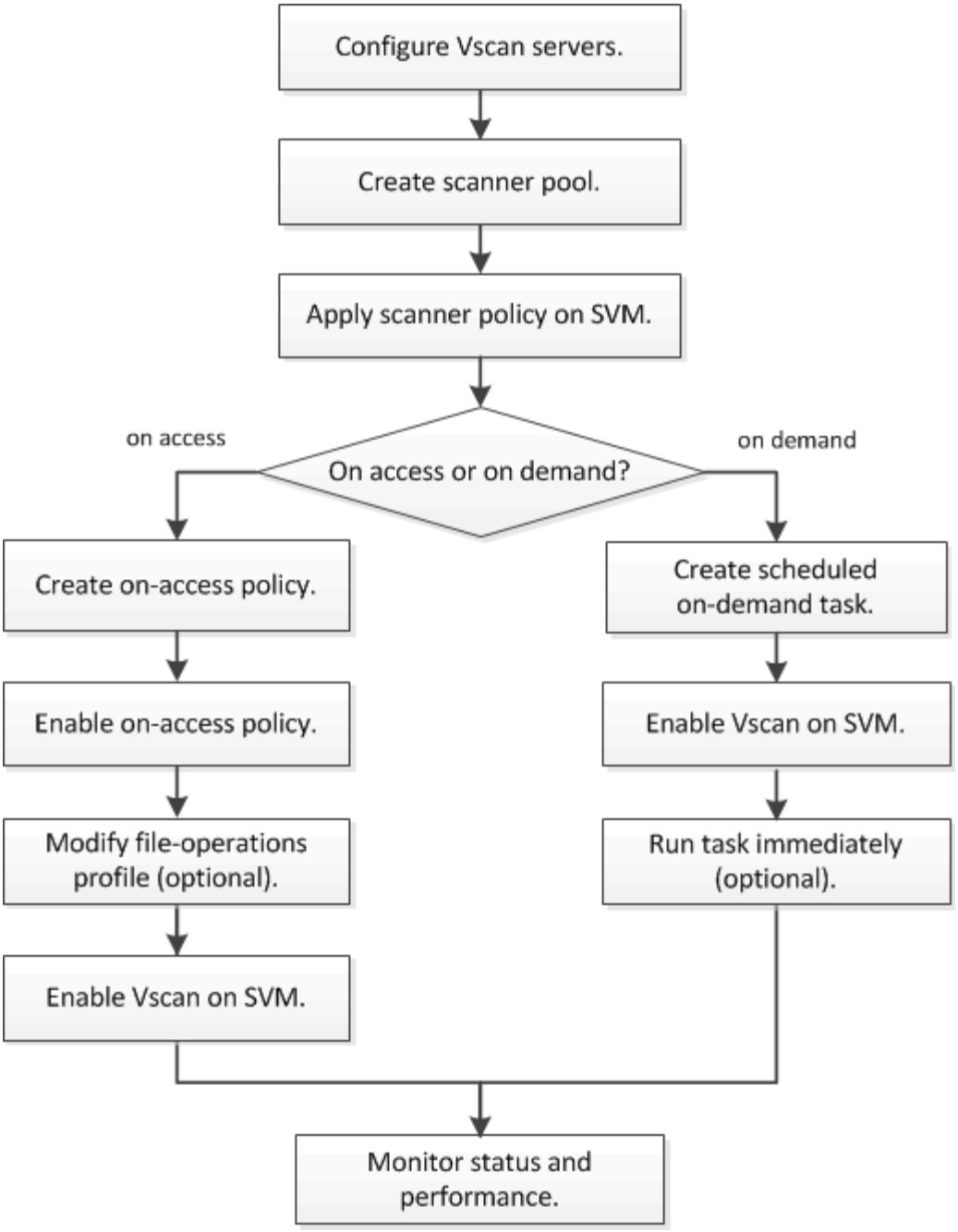
communication between the storage system and the antivirus software.



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.



Next steps

- Create a scanner pool on a single cluster
- Apply a scanner policy on a single cluster
- Create an on-access policy

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	• SentinelOne Singularity Cloud Data Security • SentinelOne support This link requires a user log-in. You can request access from Sentinel One.	

Partner	Solution documentation	Interoperability details
Deep Instinct	Deep Instinct Prevention for Storage • Documentation and Interop This link requires a user log-in. You can request access from Deep Instinct. • Data Sheet	

Vscan server installation and configuration

Vscan server installation and configuration

Set up one or more Vscan servers to ensure that files on your system are scanned for viruses. Follow the instructions provided by your vendor to install and configure the antivirus software on the server.

Follow the instructions in the README file provided by NetApp to install and configure the ONTAP Antivirus Connector. Alternatively, follow the instructions on the Install ONTAP Antivirus Connector page.

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 Vscan partner solutions page.

ONTAP Antivirus Connector requirements

- You can download the ONTAP Antivirus Connector from the **Software Download** page on the NetApp Support Site. NetApp Downloads: Software
- For information about the Windows versions supported by the ONTAP Antivirus Connector and interoperability requirements, see Vscan partner solutions.

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

- .NET 3.0 or later must be installed on the Windows server.
- SMB 2.0 must be enabled on the Windows server.

Install ONTAP Antivirus Connector

Install the ONTAP Antivirus Connector on the Vscan server to enable communication between the system running ONTAP and the Vscan server. When the ONTAP Antivirus Connector is installed, the antivirus software is able to communicate with one or more

storage virtual machines (SVMs).

About this task

- See the Vscan partner solutions page for information about the supported protocols, antivirus vendor software versions, ONTAP versions, interoperability requirements and Windows servers.
- .NET 4.5.1 or later must be installed.
- The ONTAP Antivirus Connector can run on a virtual machine. However, for best performance, NetApp recommends using a dedicated virtual machine for antivirus scanning.
- SMB 2.0 must be enabled on the Windows server on which you are installing and running the ONTAP Antivirus Connector.

Before you begin

- Download the ONTAP Antivirus Connector setup file from the Support Site and save it to a directory on your hard drive.
- Verify that you meet the requirements to install the ONTAP Antivirus Connector.
- Verify that you have administrator privileges to install the Antivirus Connector.

Steps

1. Start the Antivirus Connector installation wizard by running the appropriate setup file.
2. Select *Next*. The Destination Folder dialog box opens.
3. Select *Next* to install the Antivirus Connector to the folder that is listed or select *Change* to install to a different folder.
4. The ONTAP AV Connector Windows Service Credentials dialog box opens.
5. Enter your Windows service credentials or select **Add** to select a user. For an ONTAP system, this user must be a valid domain user and must exist in the scanner pool configuration for the SVM.
6. Select **Next**. The Ready to Install the Program dialog box opens.
7. Select **Install** to begin the installation or select **Back** if you want to make any changes to the settings. A status box opens and charts the progress of the installation, followed by the InstallShield Wizard Completed dialog box.
8. Select the Configure ONTAP LIFs check box if you want to continue with the configuration of ONTAP management or data LIFs. You must configure at least one ONTAP management or data LIF before this Vscan server can be used.
9. Select the Show the **Windows Installer log** check box if you want to view the installation logs.
10. Select **Finish** to end the installation and to close the InstallShield wizard. The **Configure ONTAP LIFs** icon is saved on the desktop to configure the ONTAP LIFs.
11. Add an SVM to the Antivirus Connector. You can add an SVM to the Antivirus Connector by adding either an ONTAP management LIF, which is polled to retrieve the list of data LIFs, or by directly configuring the data LIF or LIFs. You must also provide the poll information and the ONTAP admin account credentials if the ONTAP management LIF is configured.
    - Verify that the management LIF or the IP address of the SVM is enabled for `management-https`. This is not required when you are only configuring data LIFs.
    - Verify that you have created a user account for the HTTP application and assigned a role which has (at least read-only) access to the `/api/network/ip/interfaces` REST API. For more information about creating a user, see the security login role create and security login create ONTAP man pages.

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 ONTAP man page or use the `/api/security/acccounts` and `/api/security/roles` REST APIs to configure the admin account and role.

Steps

a. Right-click on the **Configure ONTAP LIFs** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **Run as Administrator**.

b. In the Configure ONTAP LIFs dialog box, select the preferred configuration type, then perform the following actions:

To create this type of LIF…	Perform these steps…
Data LIF	a. Set "role" to "data" b. Set "data protocol" to "cifs" c. Set "firewall policy" to "data" d. Set "service policy" to "default-data-files"
Management LIF	a. Set "role* to "data" b. Set "data protocol" to "none" c. Set "firewall policy" to "mgmt" d. Set "service policy" to "default-management"

Read more about creating a LIF.

After you create a LIF, enter the data or management LIF or IP address of the SVM that you want to add. You can also enter the cluster management LIF. If you specify the cluster management LIF, all SVMs within that cluster that are serving SMB can use the Vscan server.

When Kerberos authentication is required for Vscan servers, each SVM data LIF must have a unique DNS name, and you must register that name as a server principal name (SPN) with the Windows Active Directory. When a unique DNS name is not available for each data LIF or registered as an SPN, the Vscan server uses the NT LAN Manager mechanism for authentication. If you add or modify the DNS names and SPNs after the Vscan server is connected, you must restart the Antivirus Connector service on the Vscan server to apply the changes.

c. To configure a management LIF, enter the poll duration in seconds. The poll duration is the frequency at which the Antivirus Connector checks for changes to the SVMs or the cluster's LIF configuration. The default poll interval is 60 seconds.

d. Enter the ONTAP admin account name and password to configure a management LIF.

e. Click **Test** to check the connectivity and verify the authentication. Authentication is verified only for a management LIF configuration.

f. Click **Update** to add the LIF to the list of LIFs to poll or to connect to.

g. Click **Save** to save the connection to the registry.

h. Click **Export** if you want to export the list of connections to a registry import or registry export file. This is

useful if multiple Vscan servers use the same set of management or data LIFs.

See the Configure the ONTAP Antivirus Connector page for configuration options.

Configure the ONTAP Antivirus Connector

Configure the ONTAP Antivirus Connector to specify one or more storage virtual machines (SVMs) that you want to connect to by either entering the ONTAP management LIF, poll information, and the ONTAP admin account credentials, or just the data LIF. You can also modify the details of an SVM connection or remove an SVM connection. By default, the ONTAP Antivirus Connector uses REST APIs to retrieve the list of data LIFs if the ONTAP management LIF is configured.

Modify 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 ONTAP management LIF and the poll information. You cannot update data LIFs after they have been added. To update data LIFs you must first remove them and then add them again with the new LIF or IP address.

Before you begin

Verify that you have created a user account for the HTTP application and assigned a role which has (at least read-only) access to the `/api/network/ip/interfaces` REST API. For more information about creating a user, see the security login role create and the security login create commands. 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 ONTAP man page.

Steps

1. Right-click the **Configure ONTAP LIFs** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **Run as Administrator**. The Configure ONTAP LIFs dialog box opens.
2. Select the SVM IP address, 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 or a registry export file. This is useful if multiple Vscan servers use the same set of management or data LIFs.

Remove an SVM connection from the Antivirus Connector

If you no longer require an SVM connection, you can remove it.

Steps

1. Right-click the **Configure ONTAP LIFs** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **Run as Administrator**. The Configure ONTAP LIFs dialog box opens.
2. Select one or more SVM IP addresses, 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 or registry export file. This is useful if multiple Vscan servers use the same set of management or data LIFs.

Troubleshoot

Before you begin

When you are creating registry values in this procedure, use the right-side pane.

You can enable or disable Antivirus Connector logs for diagnostic purposes. By default, these logs are disabled. For enhanced performance, you should keep the Antivirus Connector logs disabled and only enable them for critical events.

Steps

1. Select **Start**, type "regedit" into the search box, and then select `regedit.exe` in the Programs list.
2. In **Registry Editor**, locate the following subkey for the ONTAP Antivirus Connector: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Create registry values by providing the type, name, and values shown in the following table:

Type	Name	Values
String	Tracepath	c:\avshim.log

   This registry value could be any other valid path.

4. Create another registry value by providing the type, name, values, and logging information shown in the following table:

Type	Name	Critical logging	Intermediate logging	Verbose logging
DWORD	Tracelevel	1	2 or 3	4

   This enables Antivirus Connector logs that are saved at the path value provided in the TracePath in Step 3.

5. Disable Antivirus Connector logs by deleting the registry values you created in Steps 3 and 4.
6. Create another registry value of type "MULTI_SZ" with the name "LogRotation" (without quotes). In "LogRotation", provide "logFileSize:1" as an entry for rotation size (where 1 represents 1MB) and in the next line, provide "logFileCount:5" as an entry for rotation limit (5 is the limit).

   These values are optional. If they are not provided, default values of 20MB and 10 files are used for the rotation size and rotation limit respectively. Provided integer values do not provide decimal or fraction values. If you provide values higher than the default values, the default values are used instead.

7. To disable the user-configured log rotation, delete the registry values you created in Step 6.

Customizable Banner

A custom banner allows you to place a legally binding statement and a system access disclaimer on the *Configure ONTAP LIF API* window.

Step

1. Modify the default banner by updating the contents in the `banner.txt` file in the install directory and then saving the changes. You must reopen the Configure ONTAP LIF API window to see the changes reflected in the banner.

Enable Extended Ordinance (EO) mode

You can enable and disable Extended Ordinance (EO) mode for secure operation.

Steps

1. Select **Start**, type "regedit" in the search box, and then select `regedit.exe` in the Programs list.
2. In **Registry Editor**, locate the following subkey for ONTAP Antivirus Connector: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. In the right-side pane, create a new registry value of type "DWORD" with the name "EO_Mode" (without quotes) and value "1" (without quotes) to enable EO Mode or value "0" (without quotes) to disable EO Mode.

> By default, if the `EO_Mode` registry entry is absent, EO mode is disabled. When you enable EO mode, you must configure both the external syslog server and mutual certificate authentication.

Configure the external syslog server

Before you begin

Take note that when you are creating registry values in this procedure, use the right-side pane.

Steps

1. Select **Start**, type "regedit" in the search box, and then select `regedit.exe` in the Programs list.
2. In **Registry Editor**, create the following subkey for ONTAP Antivirus Connector for syslog configuration: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Create a registry value by providing the type, name, and value as shown in the following table:

Type	Name	Value
DWORD	syslog_enabled	1 or 0

   Please note that a "1" value enables the syslog and a "0" value disables it.

4. Create another registry value by providing the information as shown in the following table:

Type	Name
REG_SZ	Syslog_host

   Provide the syslog host IP address or domain name for the value field.

5. Create another registry value by providing the information as shown in the following table:

Type	Name
REG_SZ	Syslog_port

Provide the port number on which the syslog server is running in the value field.

6. Create another registry value by providing the information as shown in the following table:

Type	Name
REG_SZ	Syslog_protocol

Enter the protocol that is in use on the syslog server, either "tcp" or "udp", in the value field.

7. Create another registry value by providing the information as shown in the following table:

Type	Name	LOG_CRIT	LOG_NOTICE	LOG_INFO	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Create another registry value by providing the information as shown in the following table:

Type	Name	Value
DWORD	syslog_tls	1 or 0

Please note that a "1" value enables syslog with Transport Layer Security (TLS) and a "0" value disables syslog with TLS.

Ensure a configured external syslog server runs smoothly

- If the key is absent or has a null value:
  - The protocol defaults to "tcp".
  - The port defaults to "514" for plain "tcp/udp" and defaults to "6514" for TLS.
  - The syslog level defaults to 5 (LOG_NOTICE).
- You can confirm that syslog is enabled by verifying that the `syslog_enabled` value is "1". When the `syslog_enabled` value is "1", you should be able to log in to the configured remote server whether or not EO mode is enabled.
- If EO mode is set to "1" and you change the `syslog_enabled` value from "1" to "0", the following applies:
  - You cannot start the service if syslog is not enabled in EO mode.
  - If the system is running in a steady state, a warning appears that says syslog cannot be disabled in EO mode and syslog is forcefully set to "1", which you can see in the registry. If this occurs, you should disable EO mode first and then disable syslog.
- If the syslog server is unable to run successfully when EO mode and syslog are enabled, the service stops running. This might occur for one of the following reasons:
  - An invalid or no syslog_host is configured.

    - An invalid protocol apart from UDP or TCP is configured.
    - A port number is invalid.
- For a TCP or TLS over TCP configuration, if the server is not listening on the IP port, the connection fails and the service shuts down.

Configure X.509 mutual certificate authentication

X.509 certificate based mutual authentication is possible for the Secure Sockets Layer (SSL) communication between the Antivirus Connector and ONTAP in the management path. If EO mode is enabled and the certificate is not found, the AV Connector terminates. Perform the following procedure on the Antivirus Connector:

Steps

1. The Antivirus Connector searches for the Antivirus Connector client certificate and the certificate authority (CA) certificate for the NetApp server in the directory path from where the Antivirus Connector runs the install directory. Copy the certificates into this fixed directory path.
2. Embed the client certificate and its private key in the PKCS12 format and name it "AV_client.P12".
3. Ensure the CA certificate (along with any intermediate signing authority up to the root CA) used to sign the certificate for the NetApp server is in the Privacy Enhanced Mail (PEM) format and named "Ontap_CA.pem". Place it in the Antivirus Connector install directory. On the NetApp ONTAP system, install the CA certificate (along with any intermediate signing authority up to the root CA) used to sign the client certificate for the Antivirus Connector at "ONTAP" as a "client-ca" type certificate.

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

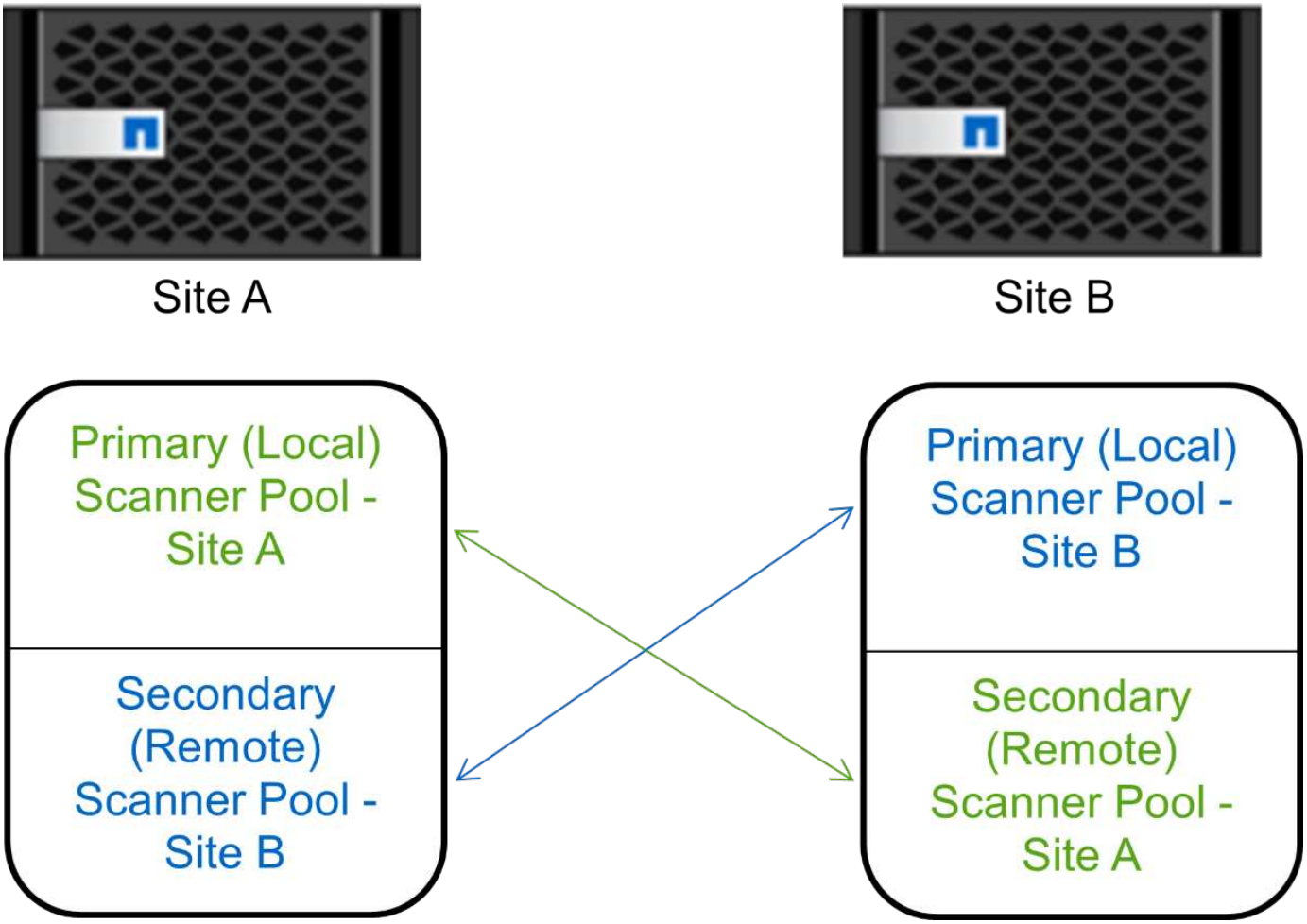
- SVMs and Vscan servers must be in the same domain or in trusted domains.
- For scanner pools defined for an individual SVM, you must have configured ONTAP Antivirus Connector with the SVM management LIF or SVM data LIF.
- For scanner pools defined for all the SVMs in a cluster, you must have configured 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.
- An on-access policy is required for an on-demand scan. To avoid on-access scanning for, you should set `-scan-files-with-no-ext` to false and `-file-ext-to-exclude` to * to exclude all extensions.

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 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.

On-demand scanning does not support scanning of symbolic links or stream files.

To create an on-demand task, there must be at least one on-access policy enabled. It can be the default policy or a user created on-access policy.

Create an on-demand task

An on-demand task defines the scope of the on-demand virus 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.

Before you begin

- You must have created an on-access policy. The policy can be a default or user-created one. Without the on-access policy, you cannot enable the scan.

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 -file-ext-to
-exclude file_extensions -file-ext-to-include file_extensions -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 command reference.

The following command creates an on-demand 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.
```

To view the status of the job, use the `job show` command. The `job pause` and `job resume` commands, respectively pause and restart the job; the `job stop` command terminates 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.

Before you begin

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.

Best practices for configuring the off-box antivirus functionality in ONTAP

Consider the following recommendations for configuring the off-box functionality in ONTAP.

- Restrict privileged users to virus scanning operations. Normal users should be discouraged from using privileged user credentials. This restriction can be achieved by turning off login rights for privileged users on Active Directory.
- Privileged users are not required to be part of any user group that has a large number of rights in the domain, such as the administrators group or the backup operators group. Privileged users must be validated only by the storage system so that they are allowed to create Vscan server connections and access files for virus scanning.
- Use the computers running Vscan servers only for virus scanning purposes. To discourage general use, disable the Windows terminal services and other remote access provisions on these machines, and grant the right to install new software on these machines only to administrators.
- Dedicate the Vscan servers to virus scanning and do not use them for other operations, such as backups. You might decide to run the Vscan server as a virtual machine (VM). If you run the Vscan server as a VM, make sure that the resources allocated to the VM are not shared and are enough to perform virus scanning.
- Provide adequate CPU, memory, and disk capacity to the Vscan server to avoid over allocation of resources. Most Vscan servers are designed to use multiple CPU core servers and to distribute the load across the CPUs.
- NetApp recommends using a dedicated network with a private VLAN for the connection from the SVM to the Vscan server so that the scan traffic is not affected by other client network traffic. Create a separate network interface card (NIC) that is dedicated to the antivirus VLAN on the Vscan server and to the data LIF on the SVM. This step simplifies administration and troubleshooting if network issues arise. The antivirus traffic should be segregated using a private network. The antivirus server should be configured to communicate with the domain controller (DC) and ONTAP in one of the following ways:
  - The DC should communicate to the antivirus servers through the private network that is used to segregate the traffic.
  - The DC and antivirus server should communicate through a different network (not the private network mentioned previously), which is not the same as the CIFS client network.
  - To enable Kerberos authentication for antivirus communication, create a DNS entry for the private LIFs and a service principal name on the DC corresponding to the DNS entry created for the private LIF. Use this name when adding a LIF to the Antivirus Connector. The DNS should be able to return a unique name for each private LIF connected to the Antivirus Connector.

If the LIF for Vscan traffic is configured on a different port than the LIF for client traffic, the Vscan LIF might fail over to another node if a port failure occurs. The change makes the Vscan server not reachable from the new node and the scan notifications for file operations on the node fail. Verify that the Vscan server is reachable through at least one LIF on a node so that it can process scan requests for file operations performed on that node.

- Connect the NetApp storage system and the Vscan server by using at least a 1GbE network.
- For an environment with multiple Vscan servers, connect all servers that have similar high-performing network connections. Connecting the Vscan servers improves performance by allowing load sharing.
- For remote sites and branch offices, NetApp recommends using a local Vscan server rather than a remote

Vscan server because the former is a perfect candidate for high latency. If cost is a factor, use a laptop or PC for moderate virus protection. You can schedule periodic complete file system scans by sharing the volumes or qtrees and scanning them from any system in the remote site.

- Use multiple Vscan servers to scan the data on the SVM for load-balancing and redundancy purposes. The amount of CIFS workload and resulting antivirus traffic vary per SVM. Monitor CIFS and virus-scanning latency on the storage controller. Monitor the trend of the results over time. If CIFS latency and virus-scanning latency increases due to CPU or application queues on the Vscan servers beyond trend thresholds, CIFS clients might experience long wait times. Add additional Vscan servers to distribute the load.
- Install the latest version of ONTAP Antivirus Connector.
- Keep antivirus engines and definitions up to date. Consult partners for recommendations on how often you should update.
- In a multi-tenancy environment, a scanner pool (pool of Vscan servers) can be shared with multiple SVMs provided that the Vscan servers and the SVMs are part of the same domain or trusted domain.
- The antivirus software policy for infected files should be set to "delete" or "quarantine", which is the default value set by most antivirus vendors. If the "vscan-fileop-profile" is set to "write_only", and if an infected file is found, the file remains in the share and can be opened because opening a file does not trigger a scan. The antivirus scan is triggered only after the file is closed.
- The `scan-engine timeout` value should be lesser than the `scanner-pool request-timeout` value. If it is set to a higher value, access to files might be delayed and might eventually time out. To avoid this, configure the `scan-engine timeout` to 5 seconds less than the `scanner-pool request-timeout` value. Refer to the scan engine vendor's documentation for instructions on how to change the `scan-engine timeout` settings. The `scanner-pool timeout` can be changed by using the following command in advanced mode and by providing the appropriate value for the `request-timeout` parameter: `vserver vscan scanner-pool modify`.
- For an environment that is sized for on-access scanning workloads and requires the use of on-demand scanning, NetApp recommends scheduling the on-demand scan job in off-peak hours to avoid additional loads on the existing antivirus infrastructure.

Learn more about best practices specific to partners at Vscan partner solutions.

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.

Before you begin

Advanced privileges are required to view the Vscan event log.

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.
   ```

Monitor and 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`
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 ONTAP man pages.

Troubleshoot virus scanning

For common virus scanning issues, there are possible causes and ways to resolve them. Virus scanning is also known as Vscan.

Issue	How to resolve it
The Vscan servers are not able to connect to the clustered ONTAP storage system.	Check whether the scanner pool configuration specifies the Vscan server IP address. Check also if the allowed privileged users in the scanner pool list are active. To check the scanner pool, run the `vserver vscan scanner-pool show` command on the storage system command prompt. If the Vscan servers still cannot connect, there might be an issue with the network.

Clients observe high latency.	It is probably time to add more Vscan servers to the scanner pool.
Too many scans are triggered.	Modify the value of the `vscan-fileop-profile` parameter to restrict the number of file operations monitored for virus scanning.
Some files are not being scanned.	Check the on-access policy. It is possible that the path for these files has been added to the path-exclusion list or that their size exceeds the configured value for exclusions. To check the on-access policy, run the `vserver vscan on-access-policy show` command on the storage system command prompt.
File access is denied.	Check whether the *scan-mandatory* setting is specified in the policy configuration. This setting denies data access if no Vscan servers are connected. Modify the setting as needed.

Monitor status and performance activities

You can monitor the critical aspects of the Vscan module, such as the Vscan server connection status, the health of the Vscan servers, and the number of files that have been scanned. This information helps you diagnose issues related to the Vscan server.

View Vscan server connection information

You can view the connection status of Vscan servers to manage the connections that are already in use and the connections that are available for use. Various commands display information about the connection status of Vscan servers.

Command…	Information displayed…
`vserver vscan connection-status show`	Summary of the connection status
`vserver vscan connection-status show-all`	Detailed information about the connection status
`vserver vscan connection-status show-not-connected`	Status of the connections that are available but not connected
`vserver vscan connection-status show-connected`	Information about the connected Vscan server

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

View Vscan server statistics

You can view Vscan server–specific statistics to monitor performance and diagnose issues related to virus scanning. You must collect a data sample before you can use the `statistics show` command to display the Vscan server statistics. To complete a data sample, complete the following step:

Step

1. Run the `statistics start` command and the `optional statistics` stop command.

View statistics for Vscan server requests and latencies

You can use ONTAP `offbox_vscan` counters on a per-SVM basis to monitor the rate of Vscan server requests that are dispatched and received per second and the server latencies across all Vscan servers. To view these statistics, complete the following step:

Step

1. Run the statistics show `object offbox_vscan –instance SVM` command with the following counters:

Counter…	Information displayed…
`scan_request_dispatched_rate`	Number of virus-scanning requests sent from ONTAP to the Vscan servers per second
`scan_noti_received_rate`	Number of virus-scanning requests received back by ONTAP from the Vscan servers per second
`dispatch_latency`	Latency within ONTAP to identify an available Vscan server and send the request to that Vscan server
`scan_latency`	Round-trip latency from ONTAP to the Vscan server, including the time for the scan to run

Example of statistics generated from an ONTAP offbox vscan counter

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-------------------------------------------------------------------
```

View statistics for individual Vscan server requests and latencies

You can use ONTAP `offbox_vscan_server` counters on a per-SVM, per–off-box Vscan server, and per-node basis to monitor the rate of dispatched Vscan server requests and the server latency on each Vscan server individually. To collect this information, complete the following step:

Step

1. Run the `statistics show –object offbox_vscan –instance SVM:servername:nodename` command with the following counters:

Counter…	Information displayed…
`scan_request_dispatched_rate`	Number of virus-scanning requests sent from ONTAP
`scan_latency`	Round-trip latency from ONTAP to the Vscan server, including the time for the scan to run to the Vscan servers per second

Example of statistics generated from an ONTAP offbox_vscan_server counter

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-------------------------------------------------------------------
```

View statistics for Vscan server utilization

You can also use ONTAP `offbox_vscan_server` counters to collect Vscan server–side utilization statistics. These statistics are tracked on a per-SVM, per–off-box Vscan server, and per-node basis. They include CPU utilization on the Vscan server, queue depth for scanning operations on the Vscan server (both current and maximum), used memory and used network. These statistics are forwarded by the Antivirus Connector to the statistics counters within ONTAP. They are based on data that is polled every 20 seconds and must be collected multiple times for accuracy; otherwise, the values seen in the statistics reflect only the last polling. CPU utilization and queues are particularly important to monitor and analyze. A high value for an average queue can indicate that the Vscan server has a bottleneck. To collect utilization statistics for the Vscan server on a per-SVM, per–off-box Vscan server, and per-node basis, complete the following step:

Step

1. Collect utilization statistics for the Vscan server

   Run the `statistics show –object offbox_vscan_server –instance SVM:servername:nodename` command with the following `offbox_vscan_server` counters:

Counter…	Information displayed…
`scanner_stats_pct_cpu_used`	CPU utilization on the Vscan server
`scanner_stats_pct_input_queue_avg`	Average queue of scan requests on the Vscan server
`scanner_stats_pct_input_queue_hiwaterma rk`	Peak queue of scan requests on the Vscan server
`scanner_stats_pct_mem_used`	Memory used on the Vscan server
`scanner_stats_pct_network_used`	Network used on the Vscan server

Example of utilization statistics for the Vscan server

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```

Copyright information

Trademark information