Technical Report

Antivirus Solution Guide for Clustered Data ONTAP: Sophos

Saurabh Singh and Brahmanna Chowdary Kodavali, NetApp
July 2016 | TR-4309

Abstract

An antivirus solution is key for enterprises to be able to protect their data from viruses and malware. Storage systems running the NetApp® clustered Data ONTAP® 8.2.1 operating system can be protected through an off-box antivirus solution. This document covers deployment procedures for the components of the solution, including the antivirus software, along with best practices for the configuration of each component.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

The off-box antivirus feature provides virus-scanning support to the NetApp clustered Data ONTAP operating system. In this architecture, virus scanning is performed by external servers that host antivirus software from third-party vendors. This feature offers antivirus functionality that is similar to the functionality currently available in Data ONTAP operating in 7-Mode.

The off-box antivirus feature provides two modes of scanning:

- **On-access scanning**. Triggers in-band notifications to the external virus-scanning servers during various file operations, such as open, close, rename, and write operations. Due to the in-band nature of these notifications, the client's file operation is suspended until the file scan status is reported back by the virus-scanning server, a Windows Server instance that is referred to as Vscan server.
- **On-demand scanning**. Introduced in ONTAP 9, this feature enables AV scanning whenever required on files/folders in a specific path through a scheduled job. It leverages the existing AV servers configured for on-access AV scanning to run the scanning job. The on-demand job updates the "scan status" of the files and reduces an additional scan on the same files when accessed next unless the files are modified. It can be used to scan volumes that cannot be configured for on-access scanning, such as NFS exports.

The Vscan server, upon receiving a notification for a scan, retrieves the file through a privileged CIFS share and scans the file contents. If the antivirus software encounters an infected file, it attempts to perform remedial operations on the file. The remedial operations are determined by the settings that are configured in the antivirus software.

After completing all necessary operations, the Vscan server reports the scan status to clustered Data ONTAP. Depending on the scan status, clustered Data ONTAP allows or denies the file operation requested by the client.

On-access scan for clustered Data ONTAP is currently available only for the CIFS-related traffic. This feature is similar to the antivirus feature in the 7-Mode implementation with the following key enhancements:

- **Granular scan exclusion.** Clustered Data ONTAP gives you the ability to exclude files from virus scanning based on file size and location (path) or to scan only the files that are opened with execute permissions.
- **Support for updates to the antivirus software.** Clustered Data ONTAP supports rolling updates of the antivirus software and maintains information about the software running version along with the scan status of files. If the antivirus software running in a single server in a scanner pool is updated to a later version, the scan status of all files that have already been scanned is not discarded.
- **Security enhancements.** Clustered Data ONTAP validates incoming connection requests sent by the Vscan server. Before the server is allowed to connect, the connection request is compared to the privileged users and IP addresses defined in the scanner pools to verify that it is originating from a valid Vscan server.

1.1 Audience

The target audience for this document is customers who want to implement virus scanning for clustered Data ONTAP storage systems that use the CIFS protocol.

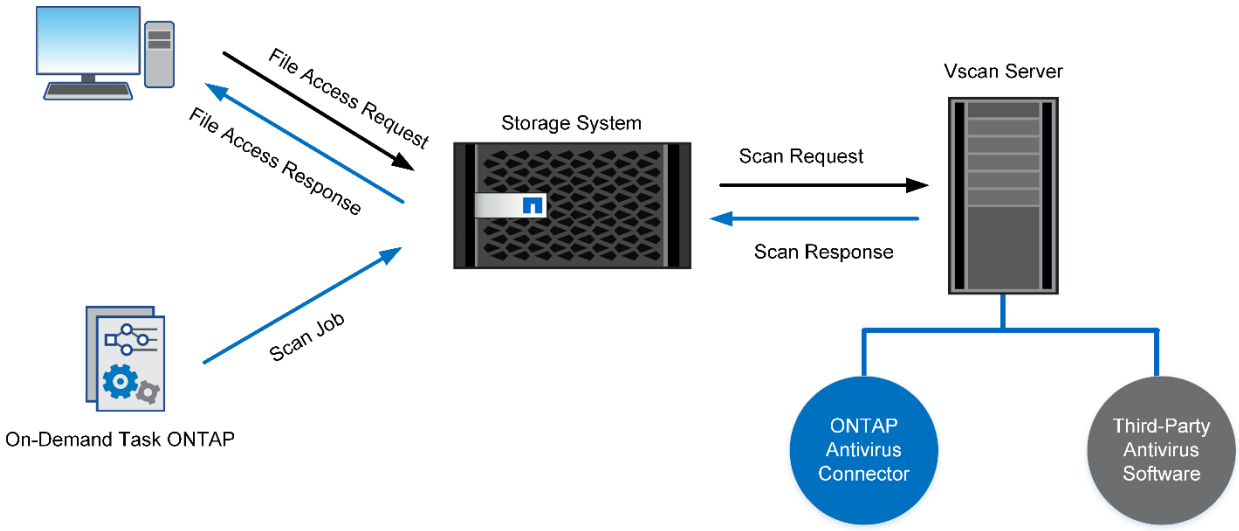
1.2 Purpose and Scope

The purpose of this document is to provide an overview of the antivirus solution on clustered Data ONTAP, with deployment steps and best practices.

2 Antivirus Solution Architecture

The antivirus solution consists of the following components: the third-party antivirus software, clustered Data ONTAP Antivirus Connector, and the clustered Data ONTAP virus-scanning settings. You must install both the antivirus software and Antivirus Connector on the Vscan server. Figure 1 shows the architecture of the antivirus solution.

Figure 1) Antivirus solution architecture.



2.1 Components of Vscan Server

Antivirus Software

The antivirus software is installed and configured on the Vscan server to scan files for viruses or other malicious data. The antivirus software must be compliant with clustered Data ONTAP. You must specify the remedial actions to be taken on infected files in the configuration of the antivirus software.

Antivirus Connector

Antivirus Connector is installed on the Vscan server to process scan requests and provide communication between the antivirus software and the storage virtual machines (SVMs; formerly called Vservers) in the storage system running clustered Data ONTAP.

2.2 Components of System Running Clustered Data ONTAP

Scanner Pool

A scanner pool is used to validate and manage the connection between the Vscan servers and the SVMs. You can create a scanner pool for an SVM to define the list of Vscan servers and privileged users that can access and connect to that SVM and to specify a timeout period for scan requests. If the response to a scan request is not received within the timeout period, file access is denied in mandatory scan cases.

Scanner Policy

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

Note: All scanner policies are system defined; you cannot create a customized scanner policy.

A scanner policy can have one of the following values:

- **Primary.** Makes the scanner pool always active.
- **Secondary.** Makes the scanner pool active only when none of the primary Vscan servers is connected.
- **Idle.** Makes the scanner pool always inactive.

On-Access Policy

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

On-Demand Task

The on-demand scan, introduced in ONTAP 9, runs the AV scanning job on files/folders in a specific path through a scheduled job whenever required. It leverages the existing AV servers configured for on-access AV scanning to run the scanning job.

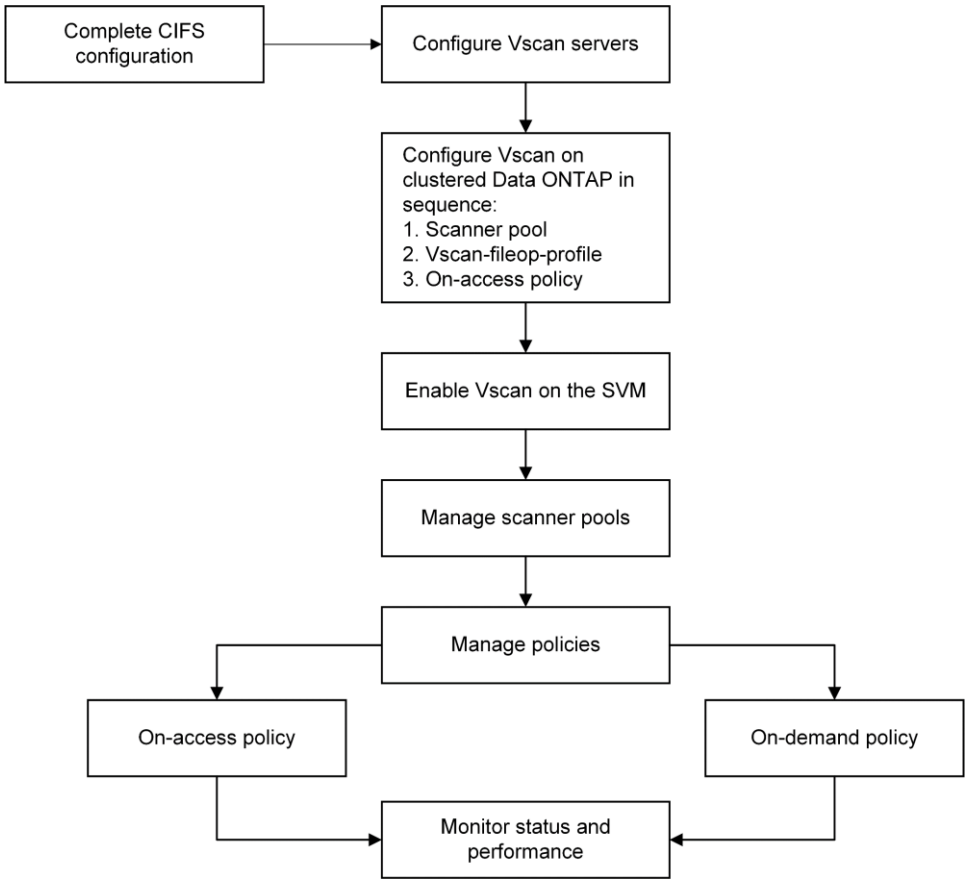
Vscan File-Operations Profile

The Vscan file-operations profile parameter (`-vscan-fileop-profile`) defines which file operations on the CIFS share can trigger virus scanning. You must configure this parameter when you create or modify a CIFS share.

2.3 Workflow for Configuring and Managing Virus Scanning

Figure 2 shows a workflow with the high-level steps that you must perform to configure and manage virus-scanning activities.

Figure 2) Workflow for configuring and managing virus scanning.



3 Vscan Server Requirements

You must set up one or more Vscan servers for files on your system to be scanned for viruses and malware. To set up a Vscan server, you must install and configure the antivirus software provided by the vendor and Antivirus Connector.

3.1 Antivirus Software Requirements

The antivirus engine featured in this document is Sophos Anti-Virus for NetApp Storage Systems. For information about the system requirements for Sophos Anti-Virus for NetApp, see the Sophos KB 118633 article: System Requirements for Antivirus Protection for Network Storage.

3.2 Antivirus Connector Requirements

Antivirus Connector has the following system requirements:

- It must be installed on one of the following Windows platforms:
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
  - Windows Server 2008

  Note: You can install different versions of the Windows platform on different Vscan servers scanning the same SVM.

Note: You must enable SMB 2.0 on the Windows Server instance (Vscan server) on which you install and run Antivirus Connector.

- .NET 3.0 or later must be enabled on Windows Server.

4 Installing and Configuring Antivirus Engine

Sophos Anti-Virus for NetApp Storage Systems uses the scanning capabilities of Sophos Endpoint Security and Control to scan files for viruses. You must install, configure, and run both Sophos Endpoint Security and Control and Sophos Anti-Virus for NetApp on the Vscan servers so that files stored on the system running clustered Data ONTAP can be scanned and cleaned.

Sophos Anti-Virus for NetApp is configured and managed from a Microsoft Management Console (MMC) snap-in.

4.1 Sophos Anti-Virus for NetApp Preinstallation Tasks

Before installing Sophos Anti-Virus for NetApp, you must complete the following tasks:

- Download and install Sophos Endpoint Security and Control (antivirus component only) on the computer you want to use as the Vscan server.
- Configure Sophos Endpoint Security and Control for use with a NetApp storage system.
- Configure Windows security options on the Vscan server.

Download and Install Sophos Endpoint Security and Control

The following steps explain how to configure a standalone installation of Sophos Endpoint Security and Control. If you are using Sophos Enterprise Console to manage antivirus software on endpoint computers, you can create a managed installation of Sophos Endpoint Security and Control as described in the Sophos Anti-Virus for NetApp Storage Systems User Guide.

To download software from the Sophos website, you must have a MySophos account and associate your software license credentials with it. For more information, see the Sophos KB 111195 article: How to Create a MySophos Login to Download Your Sophos Software.

To download and install Sophos Endpoint Security and Control, complete the following steps:

1. Navigate to the Sophos Download page and type your MySophos user name and password. After you log in, the webpage displays your license or licenses.
2. Under your license name, find the Standalone Installers downloads. Download the Anti-Virus Only installer for Windows.
3. Verify that you are logged in as an administrator in the Windows computer that you want to use as the Vscan server.
4. If you have other security software installed on this computer, verify the following items:
   a. Ensure that the security software user interface is closed.
   b. Ensure that the firewall and host-based intrusion prevention system (HIPS) software is turned off or configured to allow the Sophos installer to run.
5. Locate the installer that you downloaded and double-click it.
6. In the installer window, click Install. A wizard guides you through the installation steps. Accept the default options, except for the following items:
   a. On the Update Source page, enter the location from which Endpoint Security and Control will download updates. Sophos recommends that you set the following options now:
   – In the Address box, select Sophos or, if you download updates to your website or network, type the relevant web address or network address.

- In the Username box, type the user name that is required to access the update source.
- In the Password and Confirm Password boxes, type and confirm the password that is required to access the update source.

Note: If you access the Internet through a proxy, select the Access the Update Source via a Proxy checkbox.

b. On the Remove Third-Party Security Software page, select the Remove Third-Party Security Software checkbox if you have other antivirus software installed on the computer.

Note: Third-party security software removal does not, by default, remove any associated update tools because other security software might still be using them. If these update tools are not being used, you can remove them by using Control Panel.

7. On the last page of the wizard, choose whether to restart the computer. Click Finish.

Note: You must restart the computer to complete the removal of third-party security software.

8. The installation is complete when the Sophos Endpoint Security and Control icon is displayed in the notification area:

Configure Sophos Endpoint Security and Control

You must configure Sophos Endpoint Security and Control to perform the following tasks:

- Scan files when they are copied, moved, or opened (on read).
- Scan files with an unknown file name extension.
- Scan remote files.
- Move all infected files to a quarantine folder.
- Move all suspicious files to a quarantine folder.
- Not display messages on the screen when scanning files.

Best Practice

If you specify virus-scanning exclusions in a clustered Data ONTAP on-access policy that applies to a storage system that you want to scan, NetApp recommends specifying the same exclusions in Sophos Endpoint Security and Control on the Vscan server. For details about supported exclusions, see the Sophos Endpoint Security and Control help.

To configure Sophos Endpoint Security and Control, complete the following steps:

9. On the Vscan server, in the notification area, right-click the Endpoint Security and Control icon and select Open Sophos Endpoint Security and Control.
10. In the Sophos Endpoint Security and Control window, from the Configure menu, select Anti-Virus > On-Access Scanning.
11. In the On-access Scan Settings for This Computer dialog box, configure the following settings:
    a. Click the Scanning tab and verify that the Read checkbox is selected. If the checkbox is not selected, no files will be scanned.
    b. Click the Extensions tab. Click Add. In the extensions list box, type `???` and press Enter.
    c. Click the Exclusions tab. Verify that the exclusions list does not contain the item called All Remote Files.

d. Click the Cleanup tab:

- Verify that the Automatically Clean Up Items That Contain Virus/Spyware checkbox is not selected.
- Click Deny Access and Move To. Click Browse and specify the path of the folder to which infected files will be moved. The folder must be on this computer and should preferably be accessible only by antivirus administrators.
- Under the Suspicious Files pane, click Deny Access and Move To. Click Browse and specify the path of the folder to which suspicious files will be moved. The folder must be on this computer and should preferably be accessible only by antivirus administrators.

12. Click OK to close the On-Access Scan Settings for This Computer dialog box.
13. From the Configure menu, select Anti-Virus > Messaging.
14. In the Messaging dialog box, click the Desktop Messaging tab and clear the Enable Desktop Messaging checkbox. Click OK.

Configure Windows Security Options on Vscan Server

To configure Windows security options on the Vscan server, complete the following steps:

1. On the taskbar of the Vscan server, click Start, point to Administrative Tools, and select Local Security Policy.
2. In the left pane of the Local Security Policy window, double-click the Local Policies folder to expand it. Select Security Options.
3. Enable the Network Access: Let Everyone Permissions Apply to Anonymous Users option.
4. Restart the computer.

4.2 Install Sophos Anti-Virus for NetApp

Sophos Anti-Virus for NetApp has two components:

- The Sophos Anti-Virus for NetApp service
- An MMC snap-in, which is used to manage the Sophos Anti-Virus for NetApp service

You can install the components on the same computer or on separate computers.

Best Practice

To ensure that virus scanning can be carried out even when the Vscan server is unavailable (for example, while Sophos Endpoint Security and Control is updating), install Sophos Endpoint Security and Control and Sophos Anti-Virus for NetApp on additional computers to create additional Vscan servers. NetApp recommends adding at least two Vscan servers to a scanner pool.

NetApp also recommends creating a backup scanner pool and assigning a secondary scanner policy to it. If none of the Vscan servers in the primary scanner pool are available, then the secondary scanner pool becomes active.

To install Sophos Anti-Virus for NetApp, complete the following steps:

1. Navigate to the Sophos Download page and type your MySophos user name and password. After you log in, the webpage displays your license or licenses.
2. Under your license name, find the Groupware and Network Storage Protection downloads. Download the Anti-Virus for Network Storage installer.
3. On the Windows computer on which you are installing Sophos Anti-Virus for NetApp, verify that you are logged in as an administrator.

Note: If you are installing the Sophos Anti-Virus for NetApp service (that is, if this computer will be a Vscan server), this section assumes that you have already installed and configured Sophos Endpoint Security and Control.

4. Locate the installer that you downloaded and double-click it.
5. In the installer window, click Install.
6. On the Welcome page of the installation wizard, click Next.
7. On the End-user License Agreement page, read and accept the license agreement. Click Next.
8. On the Custom Setup page, select the features to install. This selection depends on how you will use this computer:
   - To use the computer as a Vscan server and to manage Sophos Anti-Virus for NetApp from MMC, click Next and continue to step 9.
   - To use the computer only as a Vscan server, click the drop-down arrow next to MMC Snap-in and select Entire Feature Will Be Unavailable. Click Next and continue to step 9.
   - To use the computer only to manage Sophos Anti-Virus for NetApp from MMC, click the drop-down arrow next to Anti-Virus Service and select Entire Feature Will Be Unavailable. Click Next and go to step 10.
9. On the Filer Mode page, select Clustered Data ONTAP. Click Next.
10. On the Account Information page, enter the details of an account in the domain that contains the storage system or systems that this computer is serving. The account must be a privileged user in the scanner pool. Click Next.

    Note: If the installation wizard displays a warning that the account details are invalid, verify that the Network Access: Sharing and Security Model for Local Accounts local security setting is set to Classic - Local Users Authenticate as Themselves.
11. On the Ready to Install page, click Install to begin the installation.
12. On the last page of the wizard, click Finish.

Note: To install the Sophos Anti-Virus for NetApp service and/or the MMC snap-in on another computer, repeat the steps in this section.

4.3 Configure Sophos Anti-Virus for NetApp

To configure Sophos Anti-Virus for NetApp from MMC, you must complete the following tasks:

- Snap in Sophos Anti-Virus for NetApp to MMC.
- Add a Vscan server or servers to MMC.
- Specify the storage system or systems that will be scanned by the Vscan server.

Snap In Sophos Anti-Virus for NetApp to MMC

To snap in Sophos Anti-Virus for NetApp to MMC, complete the following steps:

1. In the computer on which you installed the MMC snap-in, double-click the Sophos AV Machines shortcut on the desktop.
2. Alternatively, click Start on the taskbar and then click Run. If the computer is running a 32-bit version of Windows, type `mmc` in the Run dialog box. Otherwise, type `mmc /32`. Click OK.
3. In the Console1 console, from the File menu, select Add/Remove Snap-in.
4. In the Add or Remove Snap-ins dialog box, select Sophos Anti-Virus for NetApp Storage Systems in the Available Snap-ins list box. Click Add.
5. Click OK to return to the Console1 console.
6. From the File menu, select Save. In the Save As dialog box, choose a location and type a file name for the console settings. Click Save.

Add Vscan Server to MMC

To add a Vscan server to MMC, complete the following steps:

1. In the console tree, double-click Sophos Anti-Virus for NetApp.
2. Click the AV Machines folder. From the Action menu, select Add AV Machine.
3. In the Add Sophos Anti-Virus Server dialog box, click Browse.
4. In the Browse for Computer dialog box, locate the Vscan server and click OK.
5. In the Add Sophos Anti-Virus Server dialog box, type a location and a description for the Vscan server and click OK. The Vscan server is displayed in the right pane of the AV Machines console, with the status of the Sophos Anti-Virus for NetApp service shown in the Status column as `running`.
6. Repeat steps 1 to 5 to add another Vscan server.

Specify Storage System to Be Scanned by Vscan Server

To specify which storage system or systems will be scanned by the Vscan server, complete the following steps:

1. In the right pane of the AV Machines console, right-click the name of the Vscan server and select Properties to open the Administer AV Machine dialog box.
2. In the dialog box, click the Filers tab, and then click Add Filer. Fill in the storage system details.
3. Repeat steps 1 and 2 to add another storage system.

4.4 Monitor Antivirus Software

To monitor the status of the Vscan server in Sophos Anti-Virus for NetApp from MMC, complete the following steps:

1. In the computer on which you installed the MMC snap-in, double-click the Sophos AV Machines shortcut on the desktop.
2. Alternatively, click Start on the taskbar and then click Run. If the computer is running a 32-bit version of Windows, type `mmc` in the Run dialog box. Otherwise, type `mmc /32`. Click OK.
3. In the console tree, double-click Sophos Anti-Virus for NetApp.
4. Click the AV Machines folder. In the right pane of the AV Machines console, right-click the name of the Vscan server and select Properties to open the Administer AV Machine dialog box.
5. In the dialog box, review the status of the antivirus service and the statistics for the Vscan server.

   Note: To learn more about the statistics, see the Sophos KB 58736 article: Sophos Anti-Virus for NetApp Storage Systems: Overview of Properties, Statistics, and Options.

4.5 View Detected Malware Threats

To view which malware threats have been detected, complete the following steps:

1. Open Sophos Endpoint Security and Control on the Vscan server.
2. Double-click the Sophos Endpoint Security and Control icon in the notification area.
3. In the right pane of the Sophos Endpoint Security and Control window, under Anti-Virus and HIPS, click Manage Quarantine Items.
4. Review the list of detected threats displayed by Quarantine Manager.
5. To find out more information about a specific threat, click its name, which is displayed in the Name column in Quarantine Manager. Clicking the threat name will connect you to the Sophos website.
6. Alternatively, navigate to the Threat Analysis page on the Sophos website. Under Browse Threat Analysis, click the link for the type of item you want to find (for example, viruses and spyware) and

either type the name of the detected item in the search box or look for it in the list of latest items of its type.

4.6 Verify Firewall Requirements

A firewall on a Vscan server or on the computer running the MMC snap-in can block communication between the Vscan server and the storage system or between the computer running the snap-in and the Vscan server.

Ensure that the Sophos Anti-Virus for NetApp Storage Systems executables `savnaser.exe` and `savnammc.dll` have access to all Vscan servers, the storage system, and the computer running the snap-in.

5 Installing and Configuring Antivirus Connector

To enable the antivirus engine to communicate with one or more SVMs, you must install Antivirus Connector and configure it to connect to the SVMs.

5.1 Install Antivirus Connector

Before you can install Antivirus Connector, the prerequisites in Table 1 must be in place.

Table 1) Prerequisites for installing Antivirus Connector.

Description
You have downloaded the Antivirus Connector setup file from the NetApp Support site and saved it to a directory on your hard drive.
You have verified that the requirements to install Antivirus Connector are met.
You have administrator privileges to install Antivirus Connector.

To install Antivirus Connector, complete the following steps:

1. Run the setup file for Antivirus Connector to start the installation wizard.
2. On the Welcome page of the wizard, click Next.
3. On the Destination Folder page, either keep the Antivirus Connector installation in the suggested folder or click Change to install to a different folder. Click Next.
4. On the Data ONTAP AV Connector Windows Service Credentials page, enter your Windows service credentials or click Add to select a user. Click Next.

   Note: This user must be a valid domain user and must exist in the SVM's scanner pool.

Best Practices
• You must add the credentials used as service accounts to run the Antivirus Connector service as privileged users in the scanner pool. • The same service account must be used to run the antivirus engine service.

5. On the Ready to Install the Program page, click Back to make any changes to the settings or click Install to begin the installation. A status box opens and charts the installation progress.
6. On the InstallShield Wizard Completed page, select the Configure ONTAP Management LIFs checkbox if you want to continue with the configuration of the Data ONTAP management LIFs.

Best Practices

- Credentials used for polling must have at least read access to the network interface.
- For security purposes, consider using a separate user to poll the Data ONTAP management LIFs. The preferred accounts are `cluster admin` and `vsadmin`.

7. Select the Show the Windows Installer Log checkbox if you want to view the installation logs.
8. Click Finish to end the installation and close the wizard. The Configure ONTAP Management LIFs for Polling icon is saved on your desktop for you to configure the Data ONTAP management LIFs.

Important

By default, the ONTAP AV Connector service does not have logging enabled. To enable logging, add the following two values to the Vscan server registry:

- The `TracePath` string value (gives the local path to the logging file; for example, `c:\folder\avshim.log`)
- The `TraceLevel` DWORD value (controls the logging level; level 2 is verbose and 3 is debug)

You must add the registry values to one of the following locations:

- `HKLM\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
- `HKLM \SOFTWARE\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`

For more details, see the NetApp KB 2018449 article: Troubleshooting Workflow: Clustered Data ONTAP Antivirus Connector (Offbox\Offboard AV).

5.2 Add SVMs to Antivirus Connector

To send files for virus scanning, you must configure Antivirus Connector to connect to one or more SVMs by entering the Data ONTAP management LIF, the poll information, and the account credentials. The management LIF is polled to retrieve the list of data LIFs. Before you can add SVMs to Antivirus Connector, the prerequisites in Table 2 must be in place.

Table 2) Prerequisites for adding an SVM to Antivirus Connector.

Description
You have verified that the cluster management LIF or the IP address of the SVM is enabled for `ontapi`.
You have created a user with at least read-only access to the `network interface` command directory for `ontapi`. For more information about creating a user, see the `security login role create` and `security login create` man pages. **Note:** You can also use the domain user as an account by adding an authentication tunnel SVM for an administrative SVM. For more information, see the `security login domain tunnel` man page.

To add an SVM to Antivirus Connector, complete the following steps:

1. Right-click the Configure ONTAP Management LIFs for Polling icon, which was saved on your desktop when you completed the Antivirus Connector installation. Select Run as Administrator.
2. In the Configure Data ONTAP Management LIFs for Polling dialog box, configure the following settings:
   a. Specify the management LIF of the SVM:
   – If you have an existing management LIF or IP address, enter the management LIF or IP address of the SVM that you want to add.

– If you want to create a management LIF, create one with the role set to `data`, the data protocol set to `none`, and the firewall policy set to `mgmt`. For more information about creating a LIF, see the Clustered Data ONTAP 8.2 Network Management Guide.

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

b. Enter the poll duration, in seconds.

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

c. Enter the account name and password.

d. Click Test to verify connectivity and authenticate the connection.

e. Click Update to add the management LIF to the list of management LIFs to poll.

f. Click Save to save the connection to the registry.

g. Click Export if you want to export the list of connections to a registry import/export file.

Note: Exporting the list of connections to a file is useful if multiple Vscan servers use the same set of management LIFs.

6 Configuring Vscan Options in Clustered Data ONTAP

After you set up the Vscan servers, you must configure scanner pools and on-access policies on the storage system running clustered Data ONTAP. You must also configure the Vscan file-operations profile parameter (`-vscan-fileop-profile`) before you enable virus scanning on an SVM.

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

6.1 Create Scanner Pool

You must create a scanner pool for an SVM or a cluster to define the list of Vscan servers and privileged users that are allowed to access and connect to that SVM or cluster. Before you can configure a scanner pool, the prerequisite in Table 3 must be in place.

Table 3) Prerequisite for configuring a scanner pool for SVMs.

Description
SVMs and Vscan servers must be in the same domain or in trusted domains.

Scanner pools have the following characteristics and limits:

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

Best Practices

- Ensure that you have added all Vscan servers for serving the SVM to the scanner pool. NetApp recommends having at least two servers per scanner pool. Having more than one Vscan server improves fault tolerance and allows regular maintenance.
- The number of Vscan servers to be connected per SVM depends on the size of the environment.
- To enable multi-tenancy compliance in a secure multi-tenancy architecture, you must use different privileged users for different SVMs.

Configure Scanner Pool for SVM

To configure a scanner pool for an SVM, complete the following step:

1. Run the `vserver vscan scanner-pool create` command.

   This example shows how to create a scanner pool named `SP1` on the SVM named `vs1`:

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

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

Configure One Scanner Pool for Use with Multiple SVMs

You can configure virus scanning to leverage the same pool of Vscan servers for all SVMs instead of using a separate pool for each SVM.

NetApp recommends that you use the domain account for the Vscan servers as the privileged access credentials in the scanner pool configuration. Using this account makes the configuration less complex and easier to troubleshoot for authentication issues.

Cluster-Scoped Configuration

In a cluster-scoped configuration, the pool of Vscan servers is used for scanning all SVMs in the cluster. To configure a cluster-scoped scanner pool, complete the following steps:

1. Create a scanner pool with the cluster scope.

```
vserver vscan scanner-pool create -vserver <cserver name> -scanner-pool <scanner pool name> -
servers <vscan server ip> -privileged-users <domain\username>
```

2. Configure Antivirus Connector with the cluster management LIF.
3. Apply a scanner policy to the scanner pool, enable the on-access policy, and enable virus scanning for each SVM.

SVM-Scoped Configuration

In an SVM-scoped configuration, the pool of Vscan servers is used for scanning specific SVMs in the cluster. To configure an SVM-scoped scanner pool, complete the following steps:

1. Create a scanner pool with the SVM scope. Create the same configuration on all SVMs.

```
vserver vscan scanner-pool create -vserver <vserver name> -scanner-pool <scanner pool name> -
servers <vscan server ip> -privileged-users <domain\username>
```

2. Configure Antivirus Connector with the SVM management LIF or the data LIF.
3. Apply a scanner policy to the scanner pool, enable the on-access policy, and enable virus scanning for each SVM.

Note: Due to the trust relationship between domains, the authentication request to be sent to the corresponding domain.

6.2 Apply Scanner Policy to Scanner Pool

You must apply a scanner policy to every scanner pool defined on an SVM. The scanner policy defines when the scanner pool is active. A Vscan server is allowed to connect to the SVM only if the IP address and privileged user of the Vscan server are part of the active scanner pool list for that SVM.

You can apply only one scanner policy per scanner pool at a time. By default, the scanner policy has the value `idle`. Scanner policies can have two other values, `primary` and `secondary`. The primary policy always takes effect, whereas the secondary policy takes effect only if the primary policy fails.

Best Practice

Verify that you applied a primary policy to a primary scanner pool and a secondary policy to the backup scanner pool.

To apply a scanner policy to a scanner pool, complete the following step:

1. Run the `vserver vscan scanner-pool apply-policy` command.

   This example shows how to apply the scanner policy named `primary` to a scanner pool named `SP1` on the SVM named `vs1`:

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

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

6.3 Create Vscan Policy

A Vscan policy needs to be created to define the purview under which the Vscan acts. There are two ways in which Vscan can be used. These define the policies of Vscan.

- On-access policy
- On-demand policy

On-Access Policy

You must create an on-access policy for an SVM or for a cluster to define the scope of virus scanning. In the policy, you can specify the maximum file size for files to be considered for scanning and the file extensions and file paths to exclude from scanning:

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

Best Practices

- Consider excluding large files (file size can be specified) from virus scanning because they might result in a slow response or a scan request timeout 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 that you specify the same set of exclusions on the antivirus engine. For more information about supported exclusions, contact Sophos.

Create On-Access Policy

To create an on-access policy, complete the following step:

1. Run the `vserver vscan on-access-policy create` command.

   This example shows how to create an on-access policy named `Policy1` on the SVM named `vs1`:

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

Note: By default, the `scan-mandatory` filter is enabled if other filters are not specified. Use double quotes ("" or "-") to disable filters. For information about the parameters that you can use with the `vserver vscan on-access-policy create` command, see the command's man page.

Enable On-Access Policy

After you create an on-access scan policy, you must enable it for an SVM. You can enable only one on-access policy of a specified protocol for each SVM at a time.

To enable an on-access policy for the SVM, complete the following step:

1. Run the `vserver vscan on-access-policy enable` command.

   This example shows how to enable an on-access policy named `Policy1` on the SVM named `vs1`:

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

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

On-Demand Policy

To run an on-demand scan, you must create and schedule an on-demand task. There are parameters that needs to be defined when creating an on-demand task such as task name, maximum file size for files to be considered for scanning, file extensions, file paths to exclude from scanning and so on.

- An on-demand task needs be created for individual SVMs
- A maximum of 10 on-demand tasks can be created for each SVM, but only one can be scheduled or run at a time
- An on-demand task creates a report, which has information regarding the statistics related to the scans. This report can be accessed by either using a command (specified later in this document) or by downloading the report file created by the task at the location defined.

Create On-Demand Task

To create an on-demand task, complete the following step.

1. Run the `vscan on-demand-task create` command.

The following example shows how to create an on-demand task:

```
vscan on-demand-task create -vserver <vserver_name> -task-name <task name> -scan-paths
/vol1,/vol2 -report-path <path-to-store-reports> -request-timeout <timeout value> -cross-junction
true –directory-recursion true -scan-priority normal -paths-to-exclude <path-name> -file-ext-to-
exclude <extentions> -max-file-size 10GB
```

Table 12 describes the parameters used in the command.

Table 4) On-demand task parameters.

Parameter	Description
`vserver`	The Vserver on which the on-demand scanning is configured. On a secure multi-tenant environment, `vserver` implicitly points to the Vserver on which Vserver admin is working. This attribute defines the scope of scanning.
`task-name`	The name of the on-demand task.
`scan-paths`	A list of paths of the files or directory that need to be scanned. The path must be provided in UNIX format and from the root of the Vserver.
`report-directory`	The path to the directory where the report file is created. The path must be provided in UNIX format and from the root of the Vserver.
`schedule`	The schedule according to which the on-demand task should be run. The schedule can be created from set of commands in the job `schedule` directory.
`max-file-size`	The maximum file size for scanning. If a value is not provided, all files, irrespective of their sizes, are considered for scanning.
`paths-to-exclude`	A comma-separated list of paths to exclude from the scan.
`file-ext-to-exclude`	A comma-separated list of file extensions to exclude from the scan. This can also contain regular expression such ass `?` and `*`.
`file-ext-to-include`	A comma-separated list of file extensions to include in the scan. This can also contain regular expression such as `?` and `*`. The default value is `*`.
`scan-files-with-no-ext`	Specifies whether a file without an extension need to be scanned or not.
`request-timeout`	The total request service time limit in seconds.
`cross-junction`	Specifies whether the on-demand task is allowed to cross volume junctions. If the parameter is set to `false`, crossing junctions is not allowed. The default value is `true`.
`directory-recursion`	Determines whether the on-demand task is allowed to recursively scan through subdirectories. If the parameter is set to false, recursive scanning is not allowed. The default value `is` true.
`scan-priority`	The priority of the on-demand scan requests generated by this task.
`report-log-level`	The verbosity of the report file.

Run an On-Demand Task

After an on-demand task is created, it can be run immediately or you can wait for the task to run according to the schedule.

1. To run the task at any given point, run the following command:

```
vscan on-demand-task run -vserver <vserver name> -task-name <task name>
```

For more details on on-demand task, see section “ Manage On-Demand Task.”

6.4 Enable Virus Scanning on SVM

After you configure the scanner pool, the on-access policy, and the Vscan file-operations profile parameter, you must enable virus scanning on the SVM to protect the data. When virus scanning is enabled on the SVM, the SVM connects to the Vscan servers that are listed in the active scanner pool for that SVM. Before you can enable virus scanning on the SVM, the prerequisites in Table 5 must be in place.

Table 5) Prerequisites for enabling virus scanning on the SVM.

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

To enable virus scanning on the SVM, complete the following step:

1. Run the `vserver vscan enable` command.

   This example shows how to enable virus scanning on the SVM named `vs1`:

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

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

7 Managing Vscan Options in Clustered Data ONTAP

7.1 Modify Vscan File-Operations Profile for CIFS Share

When you create a CIFS share, you must configure the `-vscan-fileop-profile` parameter to specify which operations performed on the CIFS share can trigger virus scanning. By default, the parameter is set to `standard`. You can use the default value or change it by running the `vserver cifs share modify` command.

Before you can modify the Vscan file-operations profile for a CIFS share, the prerequisite in Table 6 must be in place.

Table 6) Prerequisite for modifying the Vscan file-operations profile.

Description
You have created a CIFS share. **Note:** Virus scanning is not performed on CIFS shares for which the `-continuously-available` parameter is set to `Yes`.

Table 7 lists the file-operations profile types and the file operations that they monitor.

Table 7) Types of file-operations profiles.

Profile Type	File Operations That Trigger Scanning
`no_scan`	None
`standard`	Open, close, and rename
`strict`	Open, read, close, and rename
`writes_only`	Close (only for newly created or modified files)

Best Practices

- Use the default, `standard` profile.
- To further restrict scanning options, use the `strict` profile. However, using this profile generates more scan requests and affects performance.
- To maximize performance with liberal scanning, use the `writes_only` profile. This profile scans only the files that have been modified and closed.

To modify the value of the `-vscan-fileop-profile` parameter, complete the following step:

1. Run the `vserver cifs share modify` command.

   Note: For more information about modifying the CIFS shares, see the Clustered Data ONTAP 8.2 File Access Management Guide for CIFS.

7.2 Manage Scanner Pools

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

View Scanner Pools of SVMs

To view information about all scanner pools belonging to all SVMs or about one scanner pool that belongs to a specific SVM, complete the following step:

1. Run the `vserver vscan scanner-pool show` command.

   These examples show how to view the list of scanner pools of all SVMs and a scanner pool of a specific SVM:

```
Cluster::> vserver vscan scanner-pool show
Scanner Pool Privileged Scanner
Vserver Pool Owner Servers Users Policy
-------------------------------------------------------------
vs1 new vserver 1.1.1.1, 2.2.2.2 cifs\u5 idle
vs1 p1 vserver 3.3.3.3 cifs\u1 primary
cifs\u2
2 entries were displayed.
Cluster::> vserver vscan scanner-pool show -vserver vs1 -scannerpool
new
Vserver: vs1
Scanner Pool: new
Applied Policy: idle
Current Status: off
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 1.1.1.1, 2.2.2.2
List of Privileged Users: cifs\u5
```

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

View Active Scanner Pools of SVMs

You can view the list of active scanner pools belonging to all SVMs. The list of active scanner pools is derived by merging the information about the active scanner pools on all SVMs.

To view the list of active scanner pools of all SVMs, complete the following step:

1. Run the `vserver vscan scanner-pool show-active` command.

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

Modify Scanner Pool

You can update the scanner pool information to modify the list of Vscan servers and privileged users that can connect to the SVM and the request and response timeout period.

To modify the scanner pool information, complete the following step:

1. Run the `vserver vscan scanner-pool modify` command.

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

Delete Scanner Pool

If you no longer need an unused scanner pool, you can delete it. To delete a scanner pool, complete the following step:

1. Run the `vserver vscan scanner-pool delete` command.

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

Add Privileged Users to Scanner Pool

You can add one or more privileged users to a scanner pool to define the privileged users who can connect to an SVM. Before you can add privileged users to the scanner pool, the prerequisite in Table 8 must be in place.

Table 8) Prerequisite for adding privileged users to a scanner pool.

Description
You have created a scanner pool for the SVM.

To add one or more privileged users to a scanner pool, complete the following step:

1. Run the `vserver vscan scanner-pool privileged-users add` command.

   This example shows how to add the privileged users named `cifs\u2` and `cifs\u3` to a scanner pool named `SP1` on the SVM named `vs1`:

```
vserver vscan scanner-pool privileged-users add -vserver vs1 -scannerpoolSP1 -privileged-users
cifs\u2,cifs\u3
```

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

Remove Privileged Users from Scanner Pool

If you no longer require privileged users, you can remove them from the scanner pool. To remove one or more privileged users from a scanner pool, complete the following step:

1. Run the `vserver vscan scanner-pool privileged-users remove` command.

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

View Privileged Users of All Scanner Pools

To view the list of privileged users of all scanner pools, complete the following step:

1. Run the `vserver vscan scanner-pool privileged-users show` command.

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

Add Vscan Servers to Scanner Pool

You can add one or more Vscan servers to a scanner pool to define the Vscan servers that can connect to an SVM. Before you can add Vscan servers to the scanner pool, the prerequisite in Table 9 must be in place.

Table 9) Prerequisite for adding Vscan servers to a scanner pool.

Description
You have created a scanner pool for the SVM.

To add one or more Vscan servers to a scanner pool, complete the following step:

1. Run the `vserver vscan scanner-pool servers add` command.

   This example shows how to add a list of Vscan servers to a scanner pool named `SP1` on the SVM named `vs1`:

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

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

Remove Vscan Servers from Scanner Pool

If you no longer require a Vscan server, you can remove it from the scanner pool. To remove one or more Vscan servers from a scanner pool, complete the following step:

1. Run the `vserver vscan scanner-pool servers remove` command.

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

View Vscan Servers of All Scanner Pools

You can view the list of Vscan servers of all scanner pools to manage the Vscan server connections. To view the Vscan servers of all scanner pools, complete the following step:

1. Run the `vserver vscan scanner-pool servers show` command.

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

7.3 Manage On-Access Policies

You can manage on-access policies to define the scope of scanning when files are accessed by a client. You can modify the maximum file size that is allowed for virus scanning and the file extensions and file

paths to be excluded from scanning. You can also delete and disable an on-access policy if it is no longer required.

View On-Access Policies of SVMs

You can view information about all on-access policies belonging to all SVMs or one on-access policy belonging to one SVM to manage on-access policies. To view on-access policies, complete the following step:

1. Run the `vserver vscan on-access-policy show` command.

   These examples show how to view the list of on-access policies of all SVMs and the on-access policy of one SVM:

```
Cluster::> vserver vscan on-access-policy show
Policy Policy File-Ext Policy
Vserver Name Owner Protocol Paths Excluded Excluded Status
---------------------------------------------------------------------
Cluster default_ cluster CIFS - - off
CIFS
vs1 default_ cluster CIFS - - on
CIFS
vs1 new vserver CIFS \vol\temp txt off
vs2 default_ cluster CIFS - - on
CIFS
4 entries were displayed.
Cluster::> vserver vscan on-access-policy show -instance -vserver
vs1 -policyname new
Vserver: vs1
Policy: new
Policy Status: off
Policy Config Owner: vserver
File-Access Protocol: CIFS
Filters: scan-ro-volume
Max File Size Allowed for Scanning: 4GB
File-Paths Not to Scan: \vol\temp
File-Extensions Not to Scan: txt
```

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

Modify On-Access Policy

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

To modify an on-access policy, complete the following step:

1. Run the `vserver vscan on-access-policy modify` command.

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

Disable On-Access Policy

To disable an on-access policy for an SVM, complete the following step:

1. Run the `vserver vscan on-access-policy disable` command.

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

Delete On-Access Policy

If you no longer require an on-access policy, you can delete it. To delete an on-access policy, complete the following step:

1. Run the `vserver vscan on-access-policy delete` command.

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

7.4 Manage On-Demand Task

View On-Demand Task Information

To view an on-demand task, complete the following step:

1. Run the `vscan on-demand-task show` command.

Manage On-Demand Task Schedule

1. You can create a schedule for an on-demand task during the task creation or define it by running the following command:

```
vscan on-demand-task schedule -vserver <vserver name> -task-name <task name> -schedule daily
```

2. To remove schedule for a task, run the following command:

```
vscan on-demand-task unschedule -vserver <vserver name> -task-name <task name>
```

On-Demand Task Report

Each on-demand task creates a report that contains results of the scan job. Table 10 lists the parameters contained in the reports. You can generate reports based on these parameters.

Table 10) On-demand task parameters.

Parameter	Description
`task-name`	Name of the task.
`job-id`	ID of the on-demand scan job.
`job-duration`	Time taken by the job to complete the on-demand task.
`report-file`	Path of the report file from root of the Vserver.
`attempted-scans`	Total number of attempted scans.
`skipped-scans`	Total number of files that were not scanned due of the configured scope of scanning.
`already-scanned-files`	Total number of files that were already scanned by a valid virus scanner.
`successful-scans`	Total number of files that were successfully scanned.
`failed-scans`	Total number of failed scans.
`timedout-scans`	Total number of scans that were timed out.
`files-cleaned`	Total number of files that were marked clean by the virus scanner.
`files-infected`	Total number of files that were marked infected by the virus scanner.
`internal-error`	Total number of internal error occurred while running the task.
`scan-retries`	Total number of scans that were retried because of an internal error.
`job-start-time`	On-demand task start time.
`job-end-time`	On-demand task end time.

To generate the reports, complete the following step:

1. Run the following command:

```
vscan_on_demand_report
```

Delete On-Demand Task

To delete an on-demand task, complete the following step:

1. Run the following command:

```
vscan on-demand-task delete –task-name <task-name> -vserver <vserver name>
```

Manage On-demand Task Job

To check the job status for an on-demand task, complete the following steps:

1. Run the following command:

```
job show –name *on-demand*
```

2. To stop the job, run the following command:

```
job stop –id <job-id>
```

8 General Best Practices

Consider the following recommendations for configuring the off-box antivirus functionality in clustered Data 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 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 this is the case, ensure that the resources allocated to the VM are not shared and are enough to perform virus scanning. Consult Sophos for guidance on antivirus engine requirements.
- Provide adequate CPU, memory, and disk capacity to the Vscan server to avoid resource bottlenecks. Most Vscan servers are designed to use multiple CPU core servers and to distribute the load across the CPUs. Consult Sophos for guidance on antivirus engine requirements.
- 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 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 AV traffic should be segregated using a private network. The AV server should be configured to communicate with domain controller (DC) and clustered Data ONTAP in one the following ways:

  – The DC should communicate to the AV servers through the private network that is used to segregate the traffic.

- The DC and AV server should communicate through a different network (not the private network mentioned previously), which is not the same as the CIFS client network.

For Kerberos authentication to work for the AV 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 AV Connector. The DNS should be able to return a unique name for each private LIF connected to the AV Connector.

Important

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 in case of a port failure. The change will make the Vscan server not reachable from the new node and the scan notifications for file operations on the node will fail.

Ensure 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 latencies on the storage controller. Trend the results over time. If CIFS latencies and virus-scanning latencies increase due to CPU or application bottlenecks 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 Antivirus Connector. For detailed information about supportability, see the NetApp Interoperability Matrix Tool (IMT).
- Keep antivirus engines and definitions up to date. Consult Sophos for recommendations on update frequency.
- 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 of a trusted domain.
- The AV software policy for infected files should be set to delete or quarantine, which is the default value set by most AV vendors. In case 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 since opening a file will not trigger a scan. The AV scan is triggered only after the file is closed.
- The `scan-engine timeout` value should always be lesser than the `scanner-pool request-timeout` value. If it is set to a higher value, access to files might be delayed and may eventually time out.

  To avoid this, configure the `scan-engine timeout` to 5 seconds lesser than the `scanner-pool request-timeout` value. See 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 workload and requiring the use of on-demand scanning, it is recommended to schedule the on-demand scan job in off-peak hours to avoid additional load on the existing AV infrastructure.

9 Troubleshooting and Monitoring

9.1 Troubleshooting Virus Scanning

Table 11 lists common virus-scanning issues, their possible causes, and ways to resolve them.

Table 11) Common virus-scanning issues.

Issue	How to Resolve It
The Vscan servers are not able to connect to the clustered Data 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 appropriate.

9.2 Monitoring 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. Table 12 lists the commands that display information about the connection status of Vscan servers.

Table 12) Commands for viewing information about the connection status of Vscan servers.

Command	Information Displayed
`vserver vscan connection-status show`	Summary of the connection status

Command	Information Displayed
`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

Note: For more information about these commands, see their respective 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 collect a data sample, complete the following step:

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

   Note: For more information about these commands, see the Clustered Data ONTAP 8.2 System Administration Guide for Cluster Administrators.

View Statistics for Vscan Server Requests and Latencies

You can use Data 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 collect this information, complete the following step:

1. Run the `statistics show –object offbox_vscan –instance SVM` command with the counters listed in Table 13.

Table 13) `offbox_vscan` counters: Vscan server requests and latencies across Vscan servers.

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

Example:

```
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 Data 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:

1. Run the `statistics show –object offbox_vscan –instance SVM:servername:nodename` command with the counters listed in Table 14.

Table 14) `offbox_vscan_server` counters: individual Vscan server requests and latencies.

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

Example:

```
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 Data 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 Antivirus Connector to the statistics counters within Data 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:

1. Run the `statistics show –object offbox_vscan_server –instance SVM:servername:nodename` command with the counters listed in Table 15.

Table 15) `offbox_vscan_server` counters: Vscan server utilization statistics.

Counter	Information Displayed
`scanner_stats_pct_cpu_used`	CPU utilization on the Vscan server

Counter	Information Displayed
scanner_stats_pct_input_queue_avg	Average queue of scan requests on the Vscan server
scanner_stats_pct_input_queue_hiwatermark	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:

```
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
-------------------------------- --------------------------------
```

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.