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

1 Introduction .............................................................................................................................. 4
   1.1 Audience .......................................................................................................................... 4
   1.2 Purpose and Scope .......................................................................................................... 4

2 Antivirus Solution Architecture .............................................................................................. 5
   2.1 Components of Vscan Server ....................................................................................... 5
   2.2 Components of System Running Clustered Data ONTAP ........................................... 5
   2.3 Workflow for Configuring and Managing Virus Scanning ........................................... 6

3 Vscan Server Requirements ................................................................................................. 7
   3.1 Antivirus Software Requirements ............................................................................... 7
   3.2 Antivirus Connector Requirements .............................................................................. 9

4 Installing and Configuring Antivirus Engine ......................................................................... 9
   4.1 Download Trend Micro ServerProtect for NetApp 5.8 ................................................ 9
   4.2 Configure Firewall Settings for ServerProtect for NetApp ........................................ 9
   4.3 Install ServerProtect for NetApp ............................................................................... 10
   4.4 Install ServerProtect for NetApp 5.8 SP1 Package ................................................... 14
   4.5 Configure ServerProtect for NetApp ....................................................................... 15

5 Installing and Configuring Antivirus Connector ..................................................................... 17
   5.1 Install Antivirus Connector ....................................................................................... 17
   5.2 Add SVMs to Antivirus Connector ............................................................................ 18

6 Configuring Vscan Options in Clustered Data ONTAP ............................................................ 19
   6.1 Create Scanner Pool .................................................................................................. 19
   6.2 Apply Scanner Policy to Scanner Pool ..................................................................... 21
   6.3 Create Vscan Policy ................................................................................................. 21
   6.4 Enable Virus Scanning on SVM .............................................................................. 24

7 Managing Vscan Options in Clustered Data ONTAP .............................................................. 24
   7.1 Modify Vscan File-Operations Profile for CIFS Share ............................................... 24
   7.2 Manage Scanner Pools ............................................................................................. 25
   7.3 Manage On-Access Policies ..................................................................................... 28
   7.4 Manage On-Demand Task ...................................................................................... 29

8 General Best Practices .......................................................................................................... 30
   8.1 Best Practices for Clustered Data ONTAP ............................................................... 30
9  Troubleshooting and Monitoring ........................................................................................................... 32
   9.1 Troubleshooting Virus Scanning ....................................................................................................... 32
   9.2 Monitoring Status and Performance Activities ................................................................................. 33

LIST OF TABLES
Table 1) Installation scenarios on Windows. ................................................................................................. 8
Table 2) Prerequisite for adding a clustered Data ONTAP antivirus shim to ServerProtect .................. 15
Table 3) Prerequisites for installing Antivirus Connector. ......................................................................... 17
Table 4) Prerequisites for adding an SVM to Antivirus Connector .......................................................... 18
Table 5) Prerequisite for configuring a scanner pool for SVMs. ............................................................... 19
Table 6) On-demand task parameters ..................................................................................................... 23
Table 7) Prerequisites for enabling virus scanning on the SVM. ............................................................ 24
Table 8) Prerequisite for modifying the Vscan file-operations profile.................................................... 24
Table 9) Types of file-operations profiles ................................................................................................. 25
Table 10) Prerequisite for adding privileged users to a scanner pool ..................................................... 26
Table 11) Prerequisite for adding Vscan servers to a scanner pool. ......................................................... 27
Table 12) On-demand task parameters ..................................................................................................... 29
Table 13) Common virus-scanning issues ................................................................................................. 29
Table 14) Virus-scanning issues related to ServerProtect for NetApp. .................................................... 33
Table 15) Commands for viewing information about the connection status of Vscan servers. .............. 34
Table 16) offbox_vscan_counters: Vscan server requests and latencies across Vscan servers. ........ 34
Table 17) offbox_vscan_server counters: individual Vscan server requests and latencies .................. 35
Table 18) offbox_vscan_server counters: Vscan server utilization statistics ........................................ 36

LIST OF FIGURES
Figure 1) Antivirus solution architecture. ................................................................................................. 5
Figure 2) Workflow for configuring and managing virus scanning. ....................................................... 7
Figure 3) ServerProtect three-tier architecture (graphic supplied by Trend Micro). ............................... 8
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 Vsan 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 Vsan 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 Vsan 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.
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 Trend Micro ServerProtect for NetApp 5.8. ServerProtect for NetApp protects networks through a three-tier architecture that has the following components:

- The **ServerProtect management console** is a portable console that gives network administrators centralized control of multiple network servers and domains.
- The **information server** is the main communication hub (middleware) between the management console and the normal servers that the information server manages. One information server can manage multiple normal servers.
- The **normal server** can be any server on a network in which ServerProtect is installed. This server is the first line of defense in the ServerProtect architecture and the component where all the action takes place.

Figure 3 shows the relationships between the ServerProtect components.
Figure 3) ServerProtect three-tier architecture (graphic supplied by Trend Micro).

Table 1 presents the Windows platforms that the ServerProtect components support.

Table 1) Installation scenarios on Windows.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Information Server</th>
<th>Normal Server</th>
<th>Management Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2003 family</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32-bit</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Server 2003 family</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64-bit</td>
<td>Yes (WOW64)</td>
<td>Yes</td>
<td>Yes (WOW64)</td>
</tr>
<tr>
<td>Windows Server 2008 family</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32-bit</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Server 2008 family</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64-bit</td>
<td>Yes (WOW64)</td>
<td>Yes</td>
<td>Yes (WOW64)</td>
</tr>
<tr>
<td>Windows Server 2008 Core</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32-bit</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Windows Server 2008 Core</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64-bit</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Windows Server 2012 family</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows XP Professional</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Vista desktop family</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows 7 desktop family</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows 8 desktop family</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note: For more information about the system requirements for Trend Micro ServerProtect for NetApp, see the Getting Started Guide for ServerProtect for NetApp 5.8. SP1.
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

You must install, configure, and run Trend Micro ServerProtect for NetApp 5.8 on the Vscan servers for files stored on the system running clustered Data ONTAP to be scanned and cleaned.

4.1 Download Trend Micro ServerProtect for NetApp 5.8

To download Trend Micro ServerProtect for NetApp 5.8 Service Pack 1 (SP1), complete the following step:

1. Navigate to the [Trend Micro Software Download Center](#) page and download the following materials:
   - Installation package for ServerProtect for NetApp 5.8
   - Installation package for ServerProtect for NetApp 5.8 SP1
   - Getting Started Guide for ServerProtect for NetApp 5.8 SP1
   - Readme file for ServerProtect for NetApp 5.8 SP1

4.2 Configure Firewall Settings for ServerProtect for NetApp

Before you can install ServerProtect for NetApp, you must configure your firewall settings.

Firewall Settings for Machine Running Management Console

- Open ports 1000 through 1009 for TCP.
  
  Ports 1000 to 1009 are used by the management console to receive event response messages from the information server.

  The management console listens to port 1000 during startup. If this port is being used by another program, the management console listens to ports 1001 through 1009 until it finds an available port.

Firewall Settings for Information Server

- Open ports 5005 through 5014 for TCP.

  Port 5005 is used to receive commands from the management console. Normally, port 5005 must be opened. If this port is being used by another program, find an available port between ports 5006 and 5014 and open the firewall.

- Open ports 3000 through 3009 for UDP.

  Port 3000 is used to receive broadcast messages. If port 3000 is being used by another program, find an available port between ports 3001 and 3009 and open the firewall.
- Open ports 137 through 139 for Remote Procedure Call (RPC) over named pipes:
  - 137 (UDP)
  - 138 (UDP)
  - 139 (TCP)
- Open port 3628 for TCP.
  Port 3628 is used to receive event response messages.
- Open port 1921 for SPX or TCP with NetWare.
  Port 1921 is used to communicate with NetWare by using SPX or TCP.

**Firewall Settings for Windows on Normal Server**

- Open port 5168 for listening to RPC over TCP/IP from the information server.
  Port 5168 is used to receive commands from the information server.
- Open ports 137 through 139 for named pipes:
  - 137 (UDP)
  - 138 (UDP)
  - 139 (TCP)

### 4.3 Install ServerProtect for NetApp

ServerProtect for NetApp 5.8 is composed of three components. These components can be installed either on one machine or on different machines. This procedure explains how to install the components on one machine.

**Note:** For information about how to install the components separately, how to install them remotely, or how to install them in silent mode, see the Getting Started Guide for ServerProtect for NetApp 5.8 SP1 that you downloaded with the installation package.

To install all ServerProtect for NetApp components on the same machine, complete the following steps:

1. Extract the ServerProtect for NetApp GM package that you downloaded to a temporary folder to start the ServerProtect installation wizard.
2. On the Welcome page of the wizard, click Next.
3. Read and accept the software license agreement. Click Yes.

4. ServerProtect checks the boot sector of the storage hardware for viruses. Click OK to continue.
5. On the User Information page, provide your user information, including the product’s serial number. Click Next.

**Note:** If you do not provide the serial number, the installation wizard installs a trial version of ServerProtect. The trial license is valid for 30 days. If you enter an invalid serial number, the wizard prompts you to reenter the correct serial number.

6. On the Select Components page, make the following selections and then click Next:
   a. Select the checkboxes for the components that you want to install. Select all components that are appropriate for the desired setup.
   b. Select a destination folder. The default installation path is `<drive>:\Program Files\Trend\SProtect`, but you can choose hidden shared storage devices, such as `C$` or `D$`, as destination folders.
7. If you chose to install either a normal server or an information server, the next wizard page is the Input Logon Information page. Enter the domain name, user name, and password of the administrator account for the target server. Confirm the password and click Next.
8. After you complete the installation, go to the desktop and double-click the shortcut to the ServerProtect for NetApp management console. The information server and the normal server should be listed in the management console window.

   **Note:** The build number of the normal server is 1075.

### 4.4 Install ServerProtect for NetApp 5.8 SP1 Package

To install the ServerProtect for NetApp 5.8 SP1 package, complete the following steps:

1. If the management console is running, close it before you proceed with the ServerProtect for NetApp 5.8 SP1 installation.
2. Copy the ServerProtect for NetApp 5.8 SP 1 installation file that you previously downloaded to a temporary folder.
3. Run the patch file.
4. Read the software license agreement:
   - If you disagree with the terms of the agreement, select I Do Not Agree with the Terms of the Legal Agreement and click Cancel to cancel the installation.
   - Otherwise, select I Accept the Terms of the Legal Agreement and click Next.
5. The installation program opens the readme file. Read it carefully and click Install. The information server deploys the patch to the normal servers 30 seconds after the installation is completed and then restarts the ServerProtect services.
6. Go to the desktop and double-click the shortcut to the ServerProtect for NetApp management console. The information server and the normal server should be listed in the management console window.

   **Note:** The build number of the normal server should have changed from 1075 to the SP1 build number. In this example, the SP1 build number is 1151.
4.5 Configure ServerProtect for NetApp

A normal server can protect multiple clustered Data ONTAP antivirus shims at the same time. Use the ServerProtect management console to add clustered Data ONTAP antivirus shims to a normal server. Before you can add a clustered Data ONTAP antivirus shim to ServerProtect for NetApp, the prerequisite in Table 2 must be in place.

Table 2) Prerequisite for adding a clustered Data ONTAP antivirus shim to ServerProtect.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have an account that is part of the list of privileged users in all clustered Data ONTAP systems that are managed by the antivirus shim.</td>
</tr>
</tbody>
</table>

To add a clustered Data ONTAP antivirus shim to ServerProtect for NetApp, complete the following steps:

1. Open the management console.

2. Right-click a normal server and select Filer List on the domain browser tree.

3. In the Filer List dialog box, click Add.

4. In the Add Filer dialog box, specify the following information and then click OK:
   a. From the Filer Mode drop-down list, select Cluster-Mode AVShim.
   b. In the Domain Name box, type the name of the domain in which the clustered Data ONTAP antivirus shim is located.
   c. In the User Name and Password boxes, type your clustered Data ONTAP antivirus shim login credentials.
Best Practice

Install the clustered Data ONTAP antivirus shim on the same machine as the normal server. Ensure that the antivirus shim and the clustered Data ONTAP storage system are correctly configured before you add the antivirus shim to ServerProtect for NetApp. For more information about configuring the antivirus shim and the clustered Data ONTAP system, see the Clustered Data ONTAP 8.2 Antivirus Configuration Guide.

**Note:** If a clustered Data ONTAP antivirus shim manages multiple clustered Data ONTAP systems, the login account must be one of the privileged users on all clustered Data ONTAP systems that are managed by the antivirus shim. For more information, see the Clustered Data ONTAP 8.2 Antivirus Configuration Guide.

5. Click OK in the message that confirms that the antivirus shim was added successfully.
Verify that the clustered Data ONTAP antivirus shim and the clustered Data ONTAP system that is managed by the antivirus shim are listed in the Filer List dialog box.

Note: For more information about how to configure ServerProtect for NetApp, see the Getting Started Guide for ServerProtect for NetApp 5.8 SP1 that you downloaded with the installation package.

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 3 must be in place.

Table 3) Prerequisites for installing Antivirus Connector.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have downloaded the Antivirus Connector setup file from the NetApp Support site and saved it to a directory on your hard drive.</td>
</tr>
<tr>
<td>You have verified that the requirements to install Antivirus Connector are met.</td>
</tr>
<tr>
<td>You have administrator privileges to install Antivirus Connector.</td>
</tr>
</tbody>
</table>

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.
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 Vsct 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 4 must be in place.

Table 4) Prerequisites for adding an SVM to Antivirus Connector.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have verified that the cluster management LIF or the IP address of the SVM is enabled for ontapi.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
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.

   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 5 must be in place.

Table 5) Prerequisite for configuring a scanner pool for SVMs.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVMs and Vscan servers must be in the same domain or in trusted domains.</td>
</tr>
</tbody>
</table>
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 <server 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.

```bash
vserver vsan 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 is 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 vsan 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`:

   ```bash
   vserver vsan 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 vsan 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 Trend Micro.

**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`:

   ```bash
   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`:

   ```bash
   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 <extensions> -max-file-size 10GB
```

Table 6 describes the parameters used in the command.

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

Table 7) Prerequisites for enabling virus scanning on the SVM.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have created one or more scanner pools and applied a scanner policy to them.</td>
</tr>
<tr>
<td>You have created an on-access policy and enabled it on the SVM.</td>
</tr>
<tr>
<td>You have configured the Vscan file-operations profile parameter.</td>
</tr>
<tr>
<td>You have verified that the Vscan servers are available.</td>
</tr>
</tbody>
</table>

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 8 must be in place.

Table 8) Prerequisite for modifying the Vscan file-operations profile.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have created a CIFS share.</td>
</tr>
</tbody>
</table>

**Note:** Virus scanning is not performed on CIFS shares for which the `-continuously-available` parameter is set to `yes`. 
Table 9 lists the file-operations profile types and the file operations that they monitor.

Table 9) Types of file-operations profiles.

<table>
<thead>
<tr>
<th>Profile Type</th>
<th>File Operations That Trigger Scanning</th>
</tr>
</thead>
<tbody>
<tr>
<td>no_scan</td>
<td>None</td>
</tr>
<tr>
<td>standard</td>
<td>Open, close, and rename</td>
</tr>
<tr>
<td>strict</td>
<td>Open, read, close, and rename</td>
</tr>
<tr>
<td>writes_only</td>
<td>Close (only for newly created or modified files)</td>
</tr>
</tbody>
</table>

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 any users to the scanner pool, the prerequisite in Table 10 must be in place.

Table 10) Prerequisite for adding privileged users to a scanner pool.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have created a scanner pool for the SVM.</td>
</tr>
</tbody>
</table>

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\texttt{vserver vscan scanner-pool privileged-users remove} command.

   \textbf{Note:} For information about the parameters that you can use with this command, see the\texttt{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\texttt{vserver vscan scanner-pool privileged-users show} command.

   \textbf{Note:} For information about the parameters that you can use with this command, see the\texttt{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 11 must be in place.

\begin{table}[h]
\centering
\begin{tabular}{|l|}
\hline
\textbf{Description} \\
You have created a scanner pool for the SVM. \\
\hline
\end{tabular}
\caption{Prerequisite for adding Vscan servers to a scanner pool.}
\end{table}

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

1. Run the\texttt{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:

   \texttt{vserver vscan scanner-pool servers add -vserver vs1 -scanner-pool SP1 -servers 10.10.10.10,11.11.11.11}

   \textbf{Note:} For information about the parameters that you can use with this command, see the\texttt{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\texttt{vserver vscan scanner-pool servers remove} command.

   \textbf{Note:} For information about the parameters that you can use with this command, see the\texttt{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\texttt{vserver vscan scanner-pool servers show} command.

   \textbf{Note:} For information about the parameters that you can use with this command, see the\texttt{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 vservex CIFS \vol\temp txt off
vs2 default_cluster CIFS - - on
CIFS
4 entries were displayed.
Cluster::> vserver vscan on-access-policy show -instance -vservex
vs1 -policynamel new
Vserver: vs1
Policy: new
Policy Status: off
Policy Config Owner: vservex
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.
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:

```bash
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:

```bash
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 12 lists the parameters contained in the reports. You can generate reports based on these parameters.

Table 12) On-demand task parameters.

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

### 8.1 Best Practices for Clustered Data ONTAP

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 Trend Micro 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 Trend Micro 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.

- To size an AV solution, use the NetApp SPM (System Performance Modeler) tool.
- 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 Trend Micro 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:

```bash
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.

### 8.2 Best Practices for Trend Micro ServerProtect for NetApp

Consider the following recommendations when configuring Trend Micro ServerProtect for NetApp:

- Trend Micro recommends allocating more than two Vscan servers per storage system. If a single Vscan server is allocated to the storage system, all I/O file operations will be blocked if any exception occurs on the server.
- By default, the number of scan threads for scan requests from the clustered Data ONTAP system is determined by the number of CPU cores according to the following formula:
  
  \[
  \text{Number of scan threads} = (\text{number of CPU cores} \times 2) + 2
  \]

To increase the number of scan threads and improve scan performance, complete the following steps on the Vscan server:

1. Run Regedit.
2. Browse to the following key:
   
   `SOFTWARE\TrendMicro\ServerProtect\CurrentVersion\Engine\FileServer\`.
3. Set the value data to the desired thread number in the `ScanThreadsNumberForCMode` key whose type is DWORD.

- To scan a compressed file, the Vscan server copies the whole file from the storage system to the local machine. This process might consume a lot of time and affect performance. NetApp recommends that you scan read-only compressed files in advance and then add them to the exclusion list.

### 9 Troubleshooting and Monitoring

#### 9.1 Troubleshooting Virus Scanning

Table 13 lists common virus-scanning issues, their possible causes, and ways to resolve them.

<table>
<thead>
<tr>
<th>Issue</th>
<th>How to Resolve It</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Vscan servers are not able to connect to the clustered Data ONTAP storage system.</td>
<td>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 <code>vserver vscan scanner-pool show</code> command on the storage system command prompt. If the Vscan servers still cannot connect, there might be an issue with the network.</td>
</tr>
<tr>
<td>Clients observe high latency.</td>
<td>It is probably time to add more Vscan servers to the scanner pool.</td>
</tr>
<tr>
<td>Too many scans are triggered.</td>
<td>Modify the value of the <code>vscan-fileop-profile</code></td>
</tr>
<tr>
<td>Issue</td>
<td>How to Resolve It</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Some files are not being scanned.</td>
<td>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 <code>vserver vscan on-access-policy show</code> command on the storage system command prompt.</td>
</tr>
<tr>
<td>File access is denied.</td>
<td>Check whether the <code>scan-mandatory</code> setting is specified in the policy configuration. This setting denies data access if no Vscan servers are connected. Modify the setting as appropriate.</td>
</tr>
</tbody>
</table>

Table 14 lists additional virus-scanning issues related to ServerProtect for NetApp and how to resolve them.

Table 14) Virus-scanning issues related to ServerProtect for NetApp.

<table>
<thead>
<tr>
<th>Issue</th>
<th>How to Resolve It</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus Connector is online, but the clustered Data ONTAP system is offline.</td>
<td>Check that the same domain account was used to register Antivirus Connector and run the Antivirus Connector service. This domain account must have been added to the active scanner pool.</td>
</tr>
</tbody>
</table>
| Large files are not being scanned successfully. | This issue occurs when the scan exceeds the scan timeout period (24 seconds by default) because the file size is too large. Extend the timeout period between the storage system and the Vscan server by completing the following steps on the Vscan server:  
1. Run Regedit.  
2. Browse to the following key: \HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ServerProtect\Current Version\Engine\Filers  
3. Set the value data to the desired timeout period in the key `ScanFilerTimeOut` whose type is DWORD. The time unit for `ScanFilerTimeOut` is seconds. |

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 15 lists the commands that display information about the connection status of Vscan servers.
Table 15) Commands for viewing information about the connection status of Vscan servers.

<table>
<thead>
<tr>
<th>Command</th>
<th>Information Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>vserver vscan connection-status show</td>
<td>Summary of the connection status</td>
</tr>
<tr>
<td>vserver vscan connection-status show-all</td>
<td>Detailed information about the connection status</td>
</tr>
<tr>
<td>vserver vscan connection-status show-not-connected</td>
<td>Status of the connections that are available but not connected</td>
</tr>
<tr>
<td>vserver vscan connection-status show-connected</td>
<td>Information about the connected Vscan server</td>
</tr>
</tbody>
</table>

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 16.

Table 16) `offbox_vscan` counters: Vscan server requests and latencies across Vscan servers.

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

Example:

Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
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 17.

### Table 17) `offbox_vscan_server` counters: individual Vscan server requests and latencies.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Information Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>scan_request_dispatched_rate</code></td>
<td>Number of virus-scanning requests sent from Data ONTAP to the Vscan servers per second</td>
</tr>
<tr>
<td><code>scan_latency</code></td>
<td>Round-trip latency from Data ONTAP to the Vscan server, including the time for the scan to run</td>
</tr>
</tbody>
</table>

**Example:**

```
Object: offbox_vscan_server
Instance: SVM:vserv_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)
---------------------------------- -------------------------------
scan_request_dispatched_rate        291
scan_noti_received_rate             292
dispatch_latency                    43986us
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 18.
<table>
<thead>
<tr>
<th>Counter</th>
<th>Information Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>scanner_stats_pct_cpu_used</td>
<td>CPU utilization on the Vscan server</td>
</tr>
<tr>
<td>scanner_stats_pct_input_queue_avg</td>
<td>Average queue of scan requests on the Vscan server</td>
</tr>
<tr>
<td>scanner_stats_pct_input_queue_hiwatermark</td>
<td>Peak queue of scan requests on the Vscan server</td>
</tr>
<tr>
<td>scanner_stats_pct_mem_used</td>
<td>Memory used on the Vscan server</td>
</tr>
<tr>
<td>scanner_stats_pct_network_used</td>
<td>Network used on the Vscan server</td>
</tr>
</tbody>
</table>

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)  

<table>
<thead>
<tr>
<th>Counter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>scanner_stats_pct_cpu_used</td>
<td>51</td>
</tr>
<tr>
<td>scanner_stats_pct_dropped_requests</td>
<td>0</td>
</tr>
<tr>
<td>scanner_stats_pct_input_queue_avg</td>
<td>91</td>
</tr>
<tr>
<td>scanner_stats_pct_input_queue_hiwatermark</td>
<td>100</td>
</tr>
<tr>
<td>scanner_stats_pct_mem_used</td>
<td>95</td>
</tr>
<tr>
<td>scanner_stats_pct_network_used</td>
<td>4</td>
</tr>
</tbody>
</table>
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.

Copyright Information

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

Trademark Information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Fitness, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, SnapCenter, SnapCopy, Snap Creator, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, StorageGRID, Tech OnTap, Unbound Cloud, WAFL, and other names are trademarks or registered trademarks of NetApp Inc., in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at http://www.netapp.com/us/legal/netapptmlist.aspx. TR-4312-0716