Technical Report

# Antivirus Solution Guide for Clustered Data ONTAP 8.2.1: Trend Micro

Brahmanna Chowdary Kodavali, NetApp

June 2014 | TR-4312

## Abstract

An antivirus solution is key for enterprises to be able to protect their data from viruses and malware. An off-box antivirus solution has been introduced to protect storage systems running the clustered Data ONTAP® 8.2.1 operating system. 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 virus-scanning support by triggering 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.

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. In clustered Data ONTAP 8.2.1, virus scanning is available only for CIFS-related traffic.

The off-box antivirus feature for clustered Data ONTAP is similar to the antivirus feature in the 7-Mode implementation, but some key enhancements have been added:

- **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.

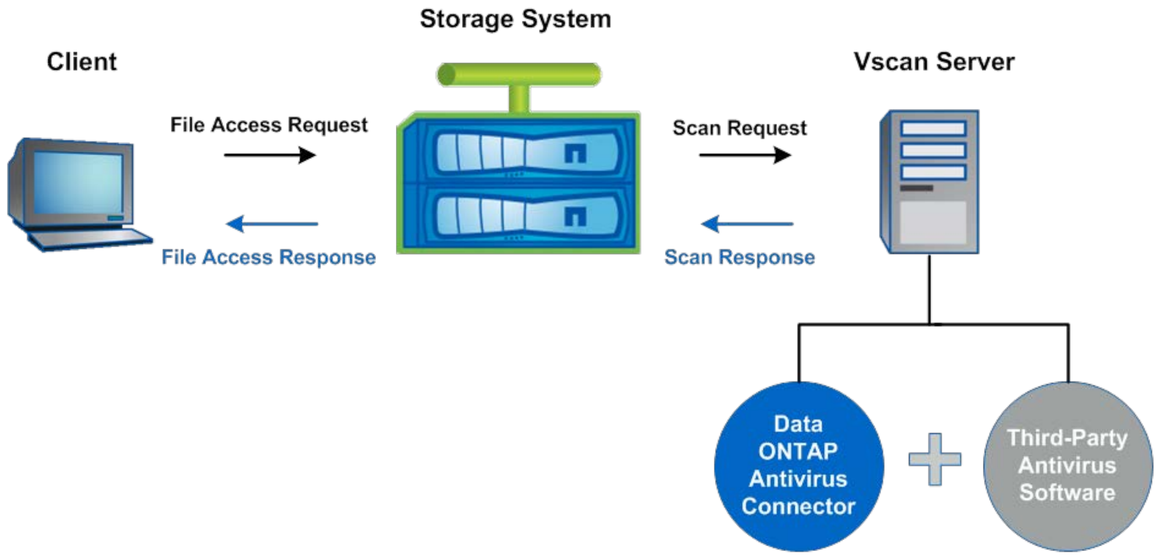
## 1.2 Purpose and Scope

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 server 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 from the available set of filters to define the scope of scanning.

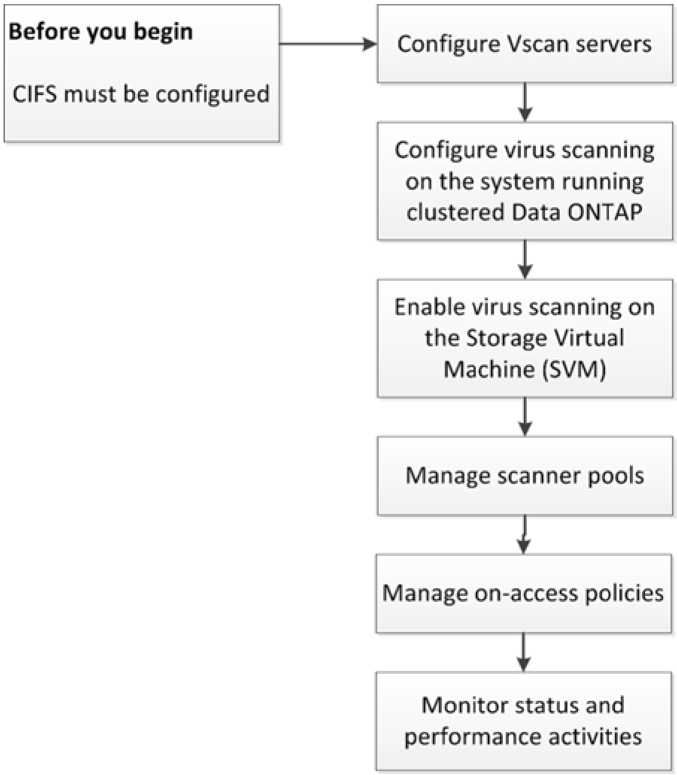
### Vscan File-Operations Profile

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 that specifies the high-level steps that you must perform to configure and manage virus scanning activities.

Figure 2) Workflow for configuring and managing virus scanning.


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

# 3 Vscan Server Requirements

You must set up one or more Vscan servers so that files on your system are 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).

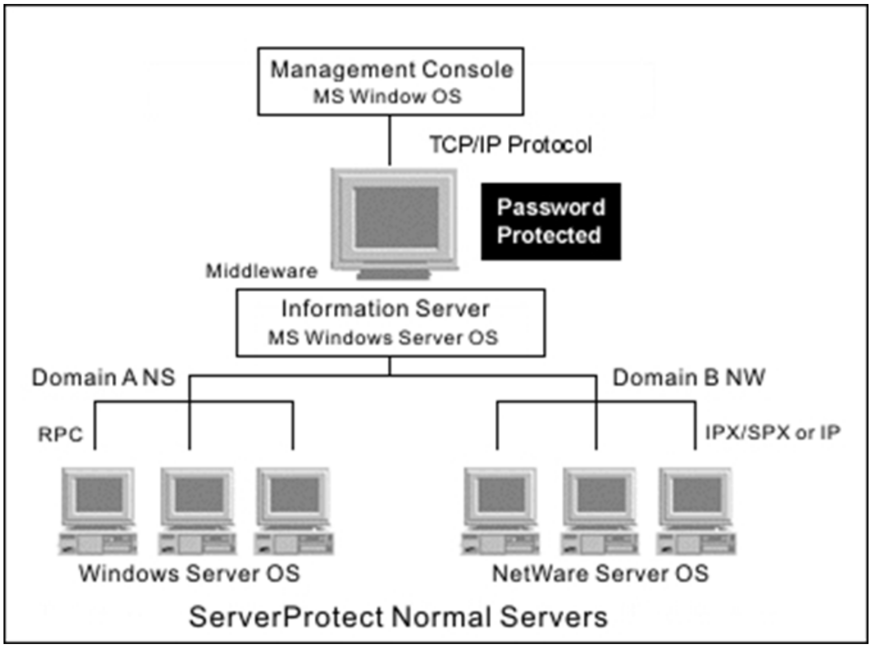


Table 1 presents the Windows® platforms that the ServerProtect components support.

Table 1) Installation scenarios on Windows.

| Operating System | Information Server | Normal Server | Management Console |
|---|---|---|---|
| Windows Server 2003 family 32-bit | Yes | Yes | Yes |
| Windows Server 2003 family 64-bit | Yes (WOW64) | Yes | Yes (WOW64) |
| Windows Server 2008 family 32-bit | Yes | Yes | Yes |
| Windows Server 2008 family 64-bit | Yes (WOW64) | Yes | Yes (WOW64) |

| Operating System | Information Server | Normal Server | Management Console |
|---|---|---|---|
| Windows 2008 Server Core 32-bit | No | Yes | No |
| Windows 2008 Server Core 64-bit | No | Yes | No |
| Windows Server 2012 family | Yes | Yes | Yes |
| Windows XP Professional | No | No | Yes |
| Windows Vista® desktop family | No | No | Yes |
| Windows 7 desktop family | No | No | Yes |
| Windows 8 desktop family | No | No | Yes |

**Note:** For more information about the system requirements for Trend Micro ServerProtect for NetApp, refer to 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 so that files stored on the system running clustered Data ONTAP can 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

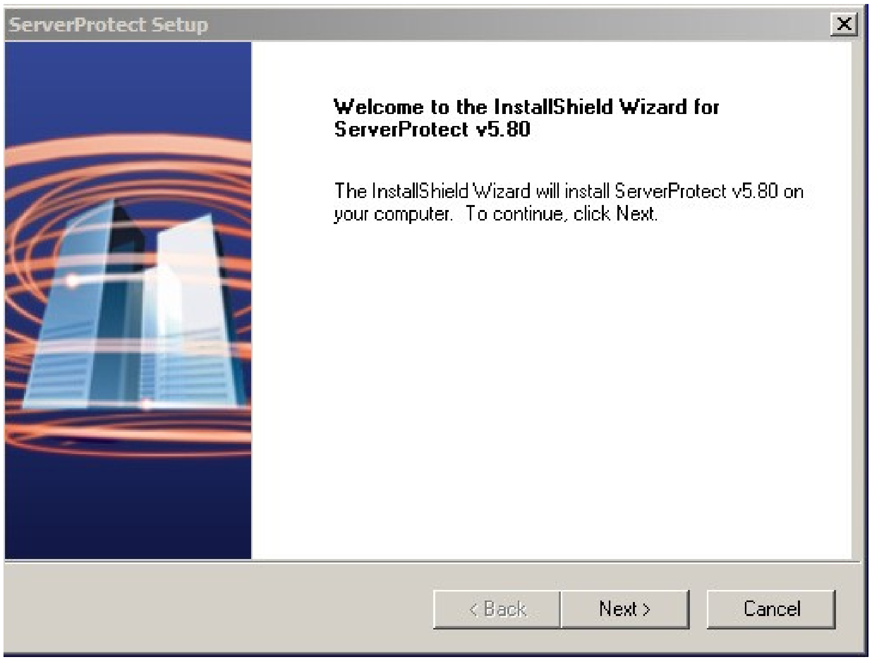
ServerProtect for NetApp 5.8 is composed of three components. These components can be installed either on one machine or on different machines. This procedure explains how to install the components on one machine.

**Note:** For information about how to install the components separately, how to install them remotely, or how to install them in silent mode, refer to 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.

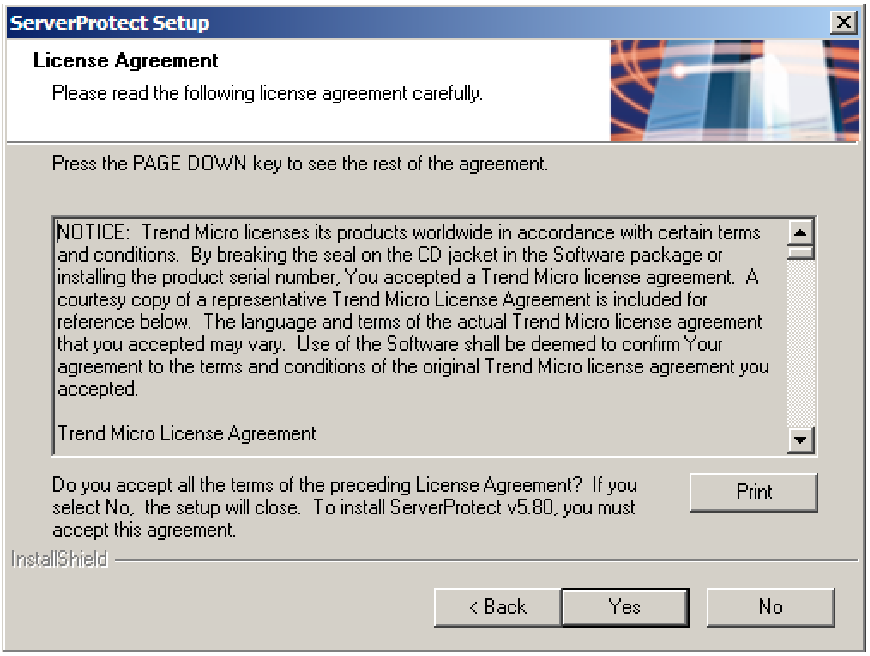
2. On the Welcome page, click Next.



**Welcome to the InstallShield Wizard for ServerProtect v5.80**

The InstallShield Wizard will install ServerProtect v5.80 on your computer. To continue, click Next.

3. Read and accept the software license agreement. Click Yes.



**License Agreement**

Please read the following license agreement carefully.

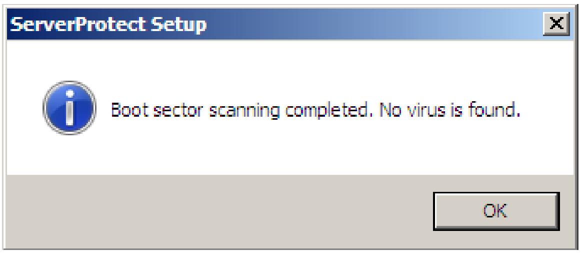
Press the PAGE DOWN key to see the rest of the agreement.

NOTICE: Trend Micro licenses its products worldwide in accordance with certain terms and conditions. By breaking the seal on the CD jacket in the Software package or installing the product serial number, You accepted a Trend Micro license agreement. A courtesy copy of a representative Trend Micro License Agreement is included for reference below. The language and terms of the actual Trend Micro license agreement that you accepted may vary. Use of the Software shall be deemed to confirm Your agreement to the terms and conditions of the original Trend Micro license agreement you accepted.

Trend Micro License Agreement

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install ServerProtect v5.80, you must accept this agreement.

4. ServerProtect checks the boot sector of the storage hardware for viruses. Click OK to continue.

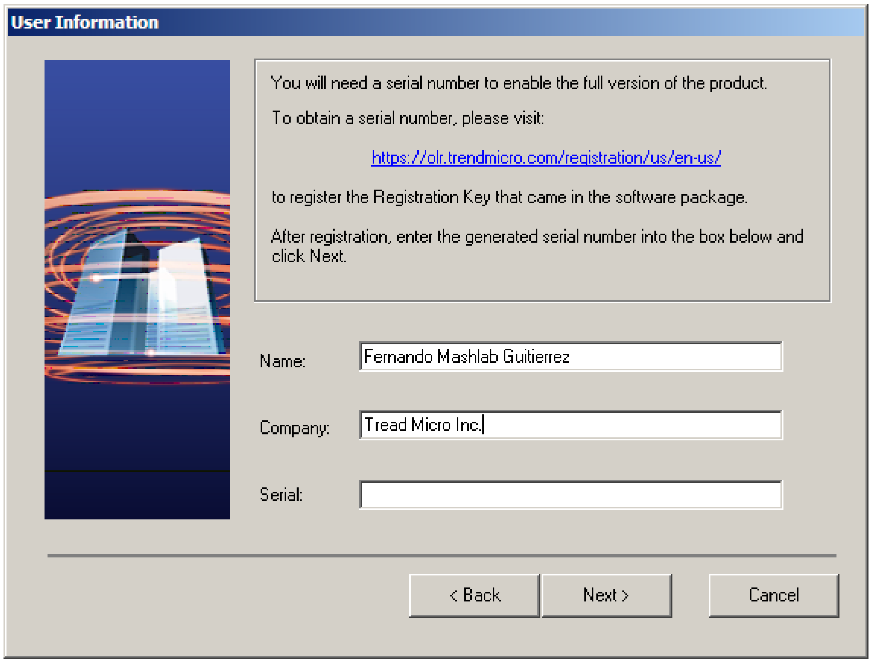


ServerProtect Setup

Boot sector scanning completed. No virus is found.

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.



User Information

You will need a serial number to enable the full version of the product.

To obtain a serial number, please visit:

https://olr.trendmicro.com/registration/us/en-us/

to register the Registration Key that came in the software package.

After registration, enter the generated serial number into the box below and click Next.

Name: Fernando Mashlab Guitierrez

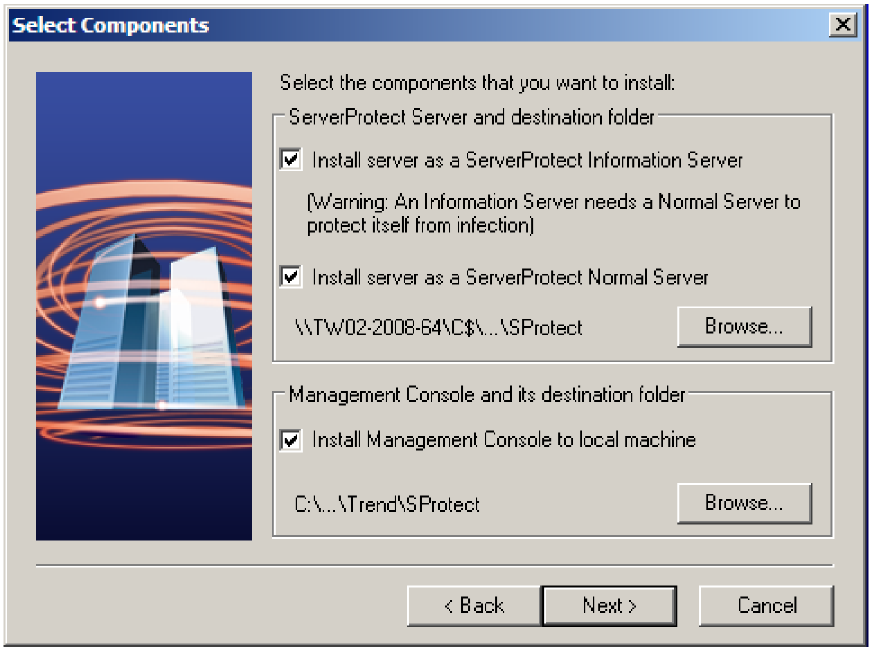
Company: Tread Micro Inc.

Serial:

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. Make sure that you select the 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.



**Select Components**

Select the components that you want to install:

ServerProtect Server and destination folder

☑ Install server as a ServerProtect Information Server

(Warning: An Information Server needs a Normal Server to protect itself from infection)

☑ Install server as a ServerProtect Normal Server

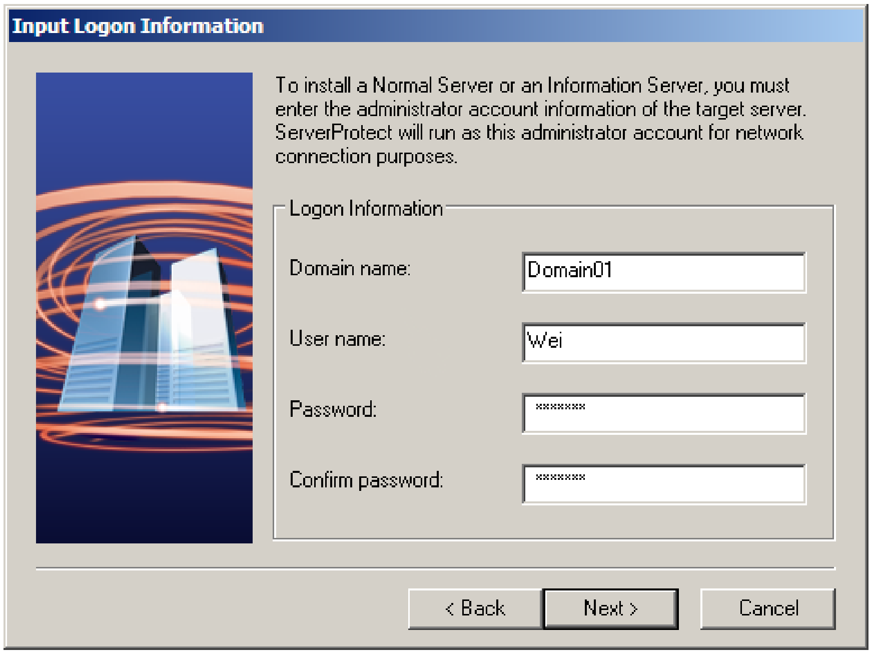
\\TW02-2008-64\C$\...\SProtect

Management Console and its destination folder

☑ Install Management Console to local machine

C:\...\Trend\SProtect

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.



**Input Logon Information**

To install a Normal Server or an Information Server, you must enter the administrator account information of the target server. ServerProtect will run as this administrator account for network connection purposes.

Logon Information

Domain name: Domain01

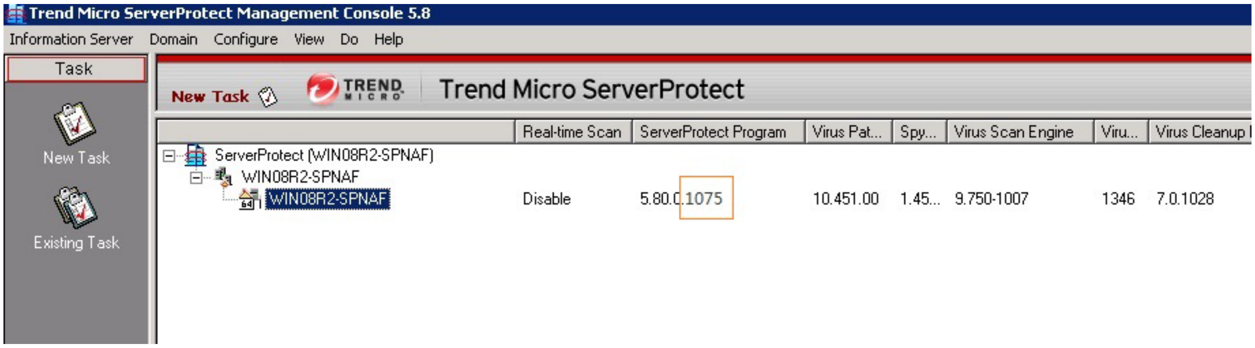
User name: Wei

Password: ********

Confirm password: ********

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.



Trend Micro ServerProtect Management Console 5.8

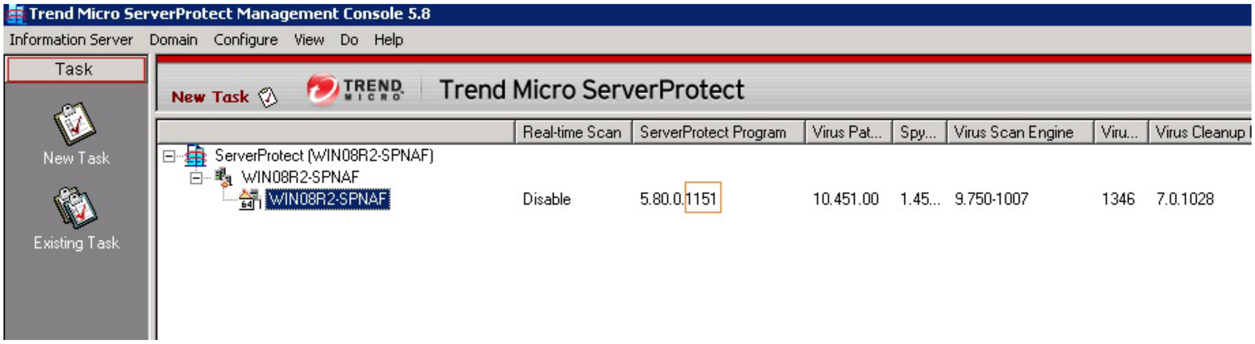
| | Real-time Scan | ServerProtect Program | Virus Pat... | Spy... | Virus Scan Engine | Viru... | Virus Cleanup I |
|---|---|---|---|---|---|---|---|
| ServerProtect (WIN08R2-SPNAF) | | | | | | | |
| WIN08R2-SPNAF | | | | | | | |
| WIN08R2-SPNAF | Disable | 5.80.0.1075 | 10.451.00 | 1.45... | 9.750-1007 | 1346 | 7.0.1028 |

## 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.



Trend Micro ServerProtect Management Console 5.8

| | Real-time Scan | ServerProtect Program | Virus Pat... | Spy... | Virus Scan Engine | Viru... | Virus Cleanup I |
|---|---|---|---|---|---|---|---|
| ServerProtect (WIN08R2-SPNAF) | | | | | | | |
| WIN08R2-SPNAF | | | | | | | |
| WIN08R2-SPNAF | Disable | 5.80.0.1151 | 10.451.00 | 1.45... | 9.750-1007 | 1346 | 7.0.1028 |

## 4.5 Configure ServerProtect for NetApp

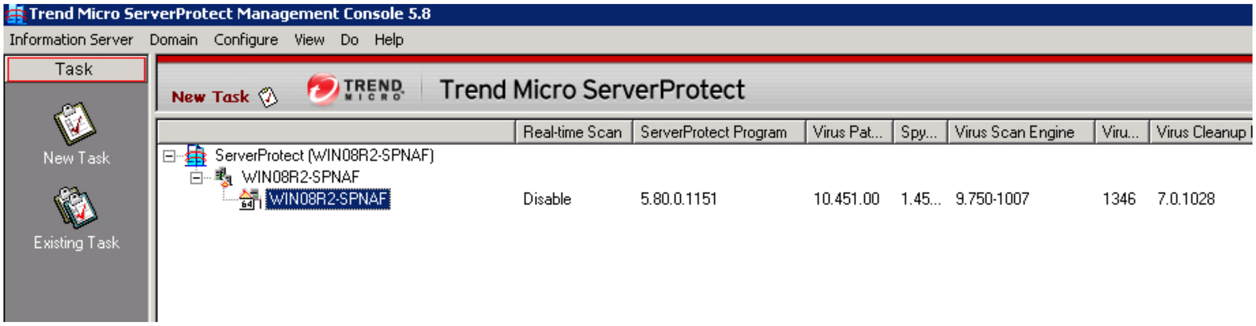
A normal server can protect multiple clustered Data ONTAP antivirus shims at the same time. Use the ServerProtect management console to add clustered Data ONTAP antivirus shims to a normal server. Before you can add a clustered Data ONTAP antivirus shim to ServerProtect for NetApp, the prerequisite in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

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

| Description |
|---|
| 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. |

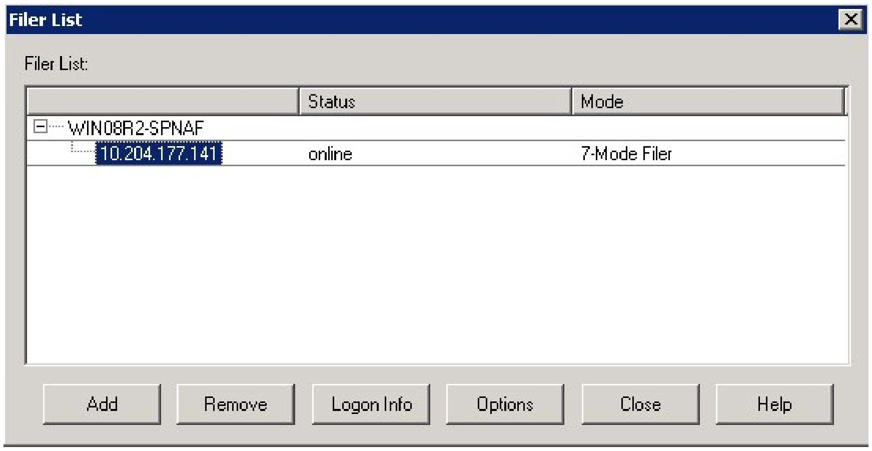
To add a clustered Data ONTAP antivirus shim to ServerProtect for NetApp, complete the following steps:

1. Open the management console.



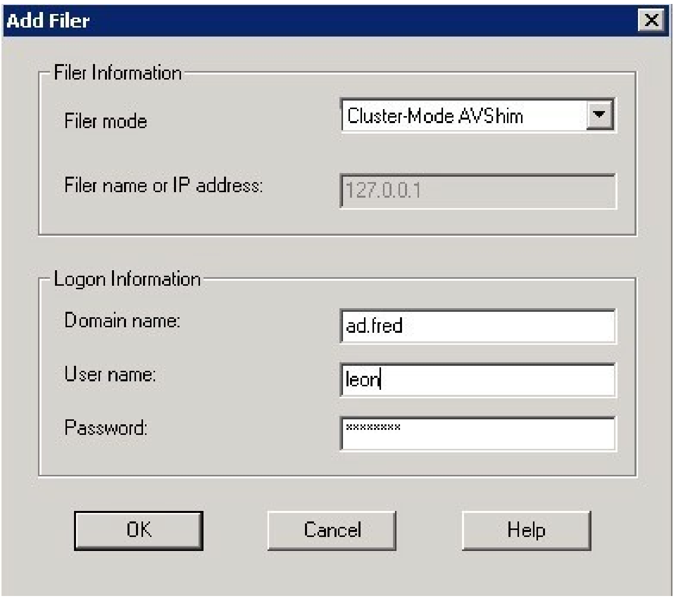
| | Real-time Scan | ServerProtect Program | Virus Pat... | Spy... | Virus Scan Engine | Viru... | Virus Cleanup I |
|---|---|---|---|---|---|---|---|
| ServerProtect (WIN08R2-SPNAF) | | | | | | | |
| WIN08R2-SPNAF | | | | | | | |
| WIN08R2-SPNAF | Disable | 5.80.0.1151 | 10.451.00 | 1.45... | 9.750-1007 | 1346 | 7.0.1028 |

2. Right-click a normal server and select Filer List on the domain browser tree.
3. In the Filer List dialog box, click Add.



| | Status | Mode |
|---|---|---|
| WIN08R2-SPNAF | | |
| 10.204.177.141 | online | 7-Mode Filer |

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.



Filer Information

Filer mode: Cluster-Mode AVShim

Filer name or IP address: 127.0.0.1

Logon Information

Domain name: ad.fred

User name: leon

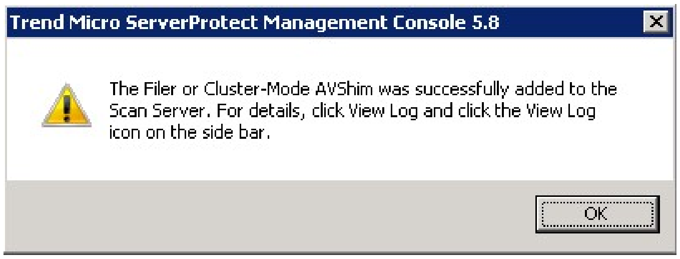
Password: *********

## Best Practice

Install the clustered Data ONTAP antivirus shim on the same machine as the normal server. Make sure 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, refer to the Clustered Data ONTAP 8.2 Antivirus Configuration Guide.

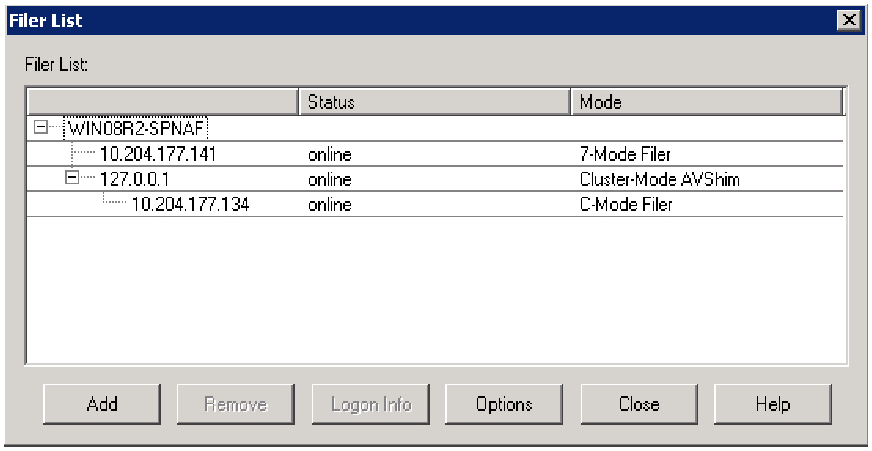
**Note:** If a clustered Data ONTAP antivirus shim manages multiple clustered Data ONTAP systems, the login account must be one of the privileged users on all clustered Data ONTAP systems that are managed by the antivirus shim. For more information, refer to the Clustered Data ONTAP 8.2 Antivirus Configuration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

5. Click OK in the message that confirms that the antivirus shim was added successfully.



The Filer or Cluster-Mode AVShim was successfully added to the Scan Server. For details, click View Log and click the View Log icon on the side bar.

6. 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.



Filer List:

| | Status | Mode |
|---|---|---|
| WIN08R2-SPNAF | | |
| 10.204.177.141 | online | 7-Mode Filer |
| 127.0.0.1 | online | Cluster-Mode AVShim |
| 10.204.177.134 | online | C-Mode Filer |

**Note:** For more information about how to configure ServerProtect for NetApp, refer to 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.**

| 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 |
|---|
| • Credentials used as service accounts to run the Antivirus Connector service must be added as privileged users in the scanner pool.<br>• 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.<br>• 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 the desktop for you to configure the Data ONTAP management LIFs.

## 5.2 Add SVM 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 one or more SVMs to Antivirus Connector, the prerequisites in Table 4 must be in place.

**Table 4) 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, refer to the `security login role create` and `security login create` man pages.<br>**Note:** You can also use the domain user as an account by adding an authentication tunnel SVM for an administrative SVM. For more information, refer to 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, refer to 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:

- You can create a scanner pool for an individual SVM or for a cluster.
- A scanner pool that you create 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

- Make sure that you have added all the 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 helps provide fault tolerance and allows regular maintenance.
- The number of Vscan servers to be connected per SVM depends on the size of the environment.
- It is mandatory to have a Vscan server and an SVM in the same security domain. The same user account must be used for the Antivirus Connector service, the antivirus engine, and the privileged user.

**Note:** In a secure multi-tenancy architecture, the privileged user must be different for different SVMs to enable multi-tenancy compliance.

To create a scanner pool, 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, refer to the `Vserver vscan scanner-pool create` man page.

## 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, refer to the `vserver vscan scanner-pool apply-policy` man page.

## 6.3 Create 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 created 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 having the same set of exclusions specified on the antivirus engine. For more information about supported exclusions, contact Trend Micro.

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:** For information about the parameters that you can use with this command, refer to the `vserver vscan on-access-policy create` man page.

### 6.4 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, refer to the `vserver vscan on-access-policy enable` man page.

### 6.5 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, refer to 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.<br>**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, refer to 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, refer to 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, refer to 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, refer to 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, refer to 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 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, refer to 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, refer to 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, refer to 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, refer to 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, refer to 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, refer to 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, refer to 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, refer to 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, refer to 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, refer to the `vserver vscan on-access-policy delete` man page.

# 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 may decide to run the Vscan server as a virtual machine (VM). If this is the case, make sure 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.
- 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, refer to the NetApp Interoperability Matrix Tool (IMT).
- Keep antivirus engines and definitions up to date. Consult Trend Micro for recommendations on update frequency.
- For secure multi-tenancy, a Vscan server cannot be shared between two or more SVMs, because the SVM and the Vscan server must be part of the same Active Directory domain.

## 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:

  Number of scan threads = (number of CPU cores × 2) + 2

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

  a. Run Regedit.
  b. Browse to the following key:

     `SOFTWARE\TrendMicro\ServerProtect\CurrentVersion\Engine\Filers`
  c. 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 10 lists common virus-scanning issues, their possible causes, and ways to resolve them.

**Table 10) 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.<br>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. |

Table 11 lists additional virus-scanning issues related to ServerProtect for NetApp and how to resolve them.

**Table 11) Additional virus-scanning issues related to ServerProtect for NetApp.**

| Issue | How to Resolve It |
|---|---|
| Antivirus Connector is online, but the clustered Data ONTAP system is offline. | 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. |
| 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:<br>1. Run Regedit. |

| Issue | How to Resolve It |
|---|---|
|  | 2. Browse to the following key:<br>`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ServerProtect\Current Version\Engine\Filers`<br>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 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 |
| `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, refer to 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, refer to 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 off-box 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 the 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 operations to be scanned on the Vscan server, both current and maximum; memory used; and network used.

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 |
| `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.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Go further, faster®

NetApp®

www.netapp.com