Technical Report

Antivirus Solution Guide for Clustered Data ONTAP: Symantec

Saurabh Singh and Brahmanna Chowdary Kodavali, NetApp
July 2016 | TR-4304

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 5

1.1 Audience 5

1.2 Purpose and Scope 5

2 Antivirus Solution Architecture 6

2.1 Components of Vscan Server 6

2.2 Components of System Running Clustered Data ONTAP 6

2.3 Workflow for Configuring and Managing Virus Scanning 7

3 Vscan Server Requirements 8

3.1 Antivirus Software Requirements 8

3.2 Antivirus Connector Requirements 9

4 Installing and Configuring Antivirus Engine 10

4.1 How Symantec Protection Engine Works with the System Running Clustered Data ONTAP 10

4.2 Prepare to Install Symantec Protection Engine 11

4.3 Install Symantec Protection Engine on Windows 12

4.4 Access Symantec Protection Engine Console 15

4.5 Configure Symantec Protection Engine to Work with Clustered Data ONTAP 16

4.6 Schedule LiveUpdate to Update Virus Definitions Automatically 21

4.7 Configure Rapid Release Updates to Occur Automatically 22

5 Installing and Configuring Antivirus Connector 22

5.1 Install Antivirus Connector 23

5.2 Add SVMs to Antivirus Connector 24

6 Configuring Vscan Options in Clustered Data ONTAP 25

6.1 Create Scanner Pool 25

6.2 Apply Scanner Policy to Scanner Pool 26

6.3 Create Vscan Policy 27

6.4 Enable Virus Scanning on SVM 29

7 Managing Vscan Options in Clustered Data ONTAP 30

7.1 Modify Vscan File-Operations Profile for CIFS Share 30

7.2 Manage Scanner Pools 31

7.3 Manage On-Access Policies 33

7.4 Manage On-Demand Task 35

8 General Best Practices 36

8.1 Best Practices for Clustered Data ONTAP 36
8.2 Best Practices for Symantec Protection Engine 38
9 Troubleshooting and Monitoring 40
9.1 Troubleshooting Virus Scanning 40
9.2 Monitoring Status and Performance Activities 41
9.3 Troubleshooting and Monitoring Symantec Protection Engine 44
Appendix 45
Allocate Resources for Symantec Protection Engine 45
Specify File Size Threshold for in-Place Scanning 45
Enhance Performance by Limiting Scanning 46
Specify File Size Threshold for Scanning Exclusion 46
Set Container File Limits 47

LIST OF TABLES

Table 1) Minimum system requirements for Symantec Protection Engine. 8
Table 2) Limiting virus scanning by file type. 11
Table 3) Installer check results. 12
Table 4) RPC protocol options. 17
Table 5) Granular scan status for clustered Data ONTAP. 19
Table 6) Client information logging in log files. 20
Table 7) Notification when queued scan requests reach threshold. 20
Table 8) Scanning files through an encoded path. 20
Table 9) Prerequisites for installing Antivirus Connector. 23
Table 10) Prerequisites for adding an SVM to Antivirus Connector. 24
Table 11) Prerequisite for configuring a scanner pool for SVMs. 25
Table 12) On-demand task parameters. 29
Table 13) Prerequisites for enabling virus scanning on the SVM. 30
Table 14) Prerequisite for modifying the Vscan file-operations profile. 30
Table 15) Types of file-operations profiles. 30
Table 16) Prerequisite for adding privileged users to a scanner pool. 32
Table 17) Prerequisite for adding Vscan servers to a scanner pool. 33
Table 18) On-demand task parameters. 35
Table 19) Configuration best practices. 38
Table 20) File configuration options. 39
Table 21) Common virus-scanning issues. 40
Table 22) Commands for viewing information about the connection status of Vscan servers. 41
Table 23) `offbox_vscan` counters: Vscan server requests and latencies across Vscan servers. 42

Table 24) `offbox_vscan_server` counters: individual Vscan server requests and latencies. 42
Table 25) `offbox_vscan_server` counters: Vscan server utilization statistics. 43
Table 26) Symantec Protection Engine detailed information. 44
Table 27) Resource settings. 45
Table 28) `FilerPerformanceThreshold` parameter settings. 46
Table 29) Performance enhancement options. 46
Table 30) Maximum value to exclude files from scanning. 47

LIST OF FIGURES

Figure 1) Antivirus solution architecture. 6
Figure 2) Workflow for configuring and managing virus scanning. 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 Vscan server.
- **On-demand scanning**. Introduced in ONTAP 9, this feature enables AV scanning whenever required on files/folders in a specific path through a scheduled job. It leverages the existing AV servers configured for on-access AV scanning to run the scanning job. The on-demand job updates the "scan status" of the files and reduces an additional scan on the same files when accessed next unless the files are modified. It can be used to scan volumes that cannot be configured for on-access scanning, such as NFS exports.

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

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

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

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

1.1 Audience

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

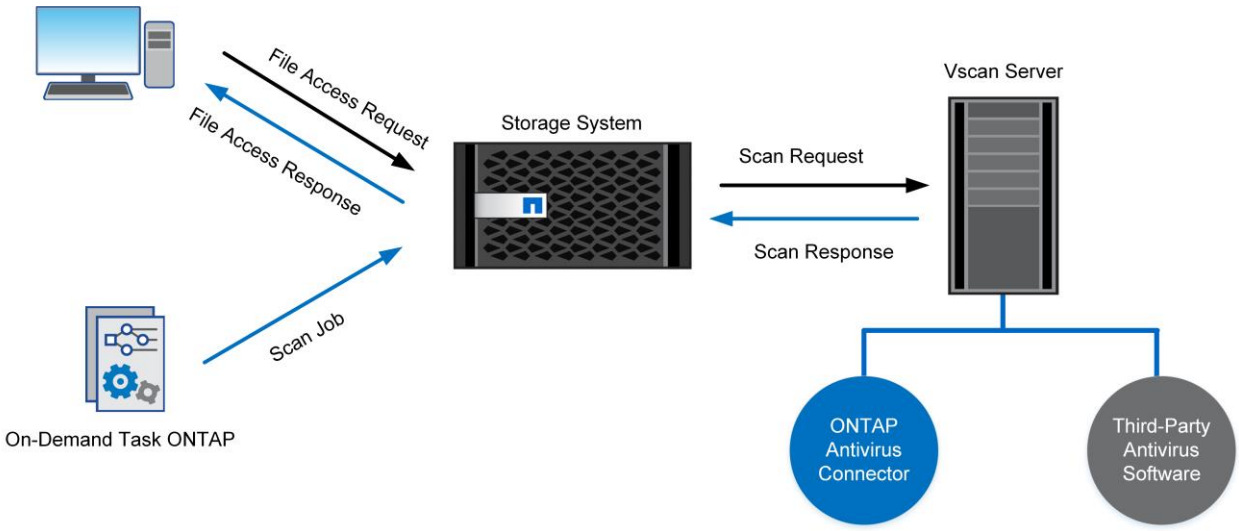
1.2 Purpose and Scope

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

2 Antivirus Solution Architecture

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

Figure 1) Antivirus solution architecture.



2.1 Components of Vscan Server

Antivirus Software

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

Antivirus Connector

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

2.2 Components of System Running Clustered Data ONTAP

Scanner Pool

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

Scanner Policy

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

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

A scanner policy can have one of the following values:

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

On-Access Policy

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

On-Demand Task

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

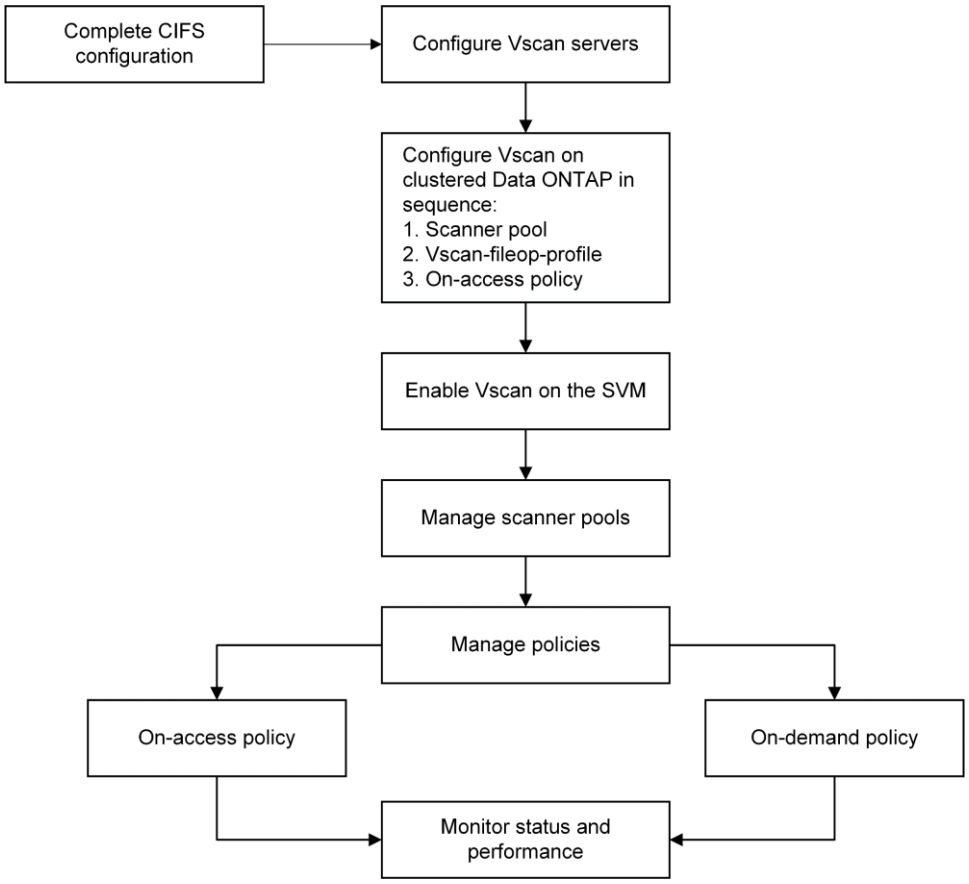
Vscan File-Operations Profile

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

2.3 Workflow for Configuring and Managing Virus Scanning

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

Figure 2) Workflow for configuring and managing virus scanning.



3 Vscan Server Requirements

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

3.1 Antivirus Software Requirements

The antivirus engine featured in this document is Symantec Protection Engine. The minimum system requirements to install Symantec Protection Engine on Windows are presented in Table 1.

Table 1) Minimum system requirements for Symantec Protection Engine.

Component	Requirements
Operating system	• Windows Server 2008 SP2 (64-bit) • Windows Server 2008 R2 (64-bit) • Windows Server 2012 (64-bit) **Note:** For detailed information about the supported platforms, see the Symantec Protection Engine Platform Support Matrix.
Processor	Intel or AMD server grade single processor quad core systems or higher
Memory	4GB RAM or higher

Component	Requirements
Disk space	5GB of hard disk space 10GB of hard disk space if the URL filtering feature is used
Hardware	• Network interface card (NIC) running TCP/IP with a static IP address • Internet connection to update definitions • 100Mbps Ethernet link (1Gbps recommended)
Software	• Java 2SE Runtime Environment (JRE) 7.0 (update 45 or later) • Microsoft Visual C++ 2010 (SP1 or later) redistributable package (x86) One of the following web browsers is required to access the Symantec Protection Engine console: • Microsoft Internet Explorer 10 or later. Use Internet Explorer to access the Symantec Protection Engine console from a Windows client computer. • Mozilla Firefox 24 or later. Use Firefox to access the Symantec Protection Engine console from a Solaris or Linux client computer. **Note:** The web browser is required only for web-based administration. You must install the web browser on the computer from which you want to access the Symantec Protection Engine console. This computer must have access to the server on which Symantec Protection Engine is running.
Hypervisor support	• VMware vSphere hypervisor version 5.1 or later • Windows Server 2008 R2 Hyper-V • Windows Server 2012 Hyper-V • Citrix XenServer 3.4.3 (installed on RHEL 5.4 64-bit)

Note: Install JRE only if you plan to operate Symantec Protection Engine in the core server with the user interface mode. Symantec Protection Engine supports only 32-bit JRE versions; it cannot be installed with 64-bit JRE versions.

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

4.1 How Symantec Protection Engine Works with the System Running Clustered Data ONTAP

Symantec Protection Engine provides virus scanning and repair capabilities for clustered Data ONTAP. It must be installed on a computer that is running Windows Server 2008 or Windows Server 2012. Symantec Protection Engine has been certified with clustered Data ONTAP for the following platforms:

- Windows Server 2008 SP2 64-bit
- Windows Server 2008 R2 SP1 64-bit
- Windows Server 2012 (64-bit)

Symantec Protection Engine must be located in the same domain as the storage system for which it provides scanning and repair services. It uses the proprietary NetApp adaptation of the Remote Procedure Call (RPC) protocol to communicate with the storage system.

A single Symantec Protection Engine installation can support multiple NetApp storage systems. You can use multiple protection engines to support one or more storage systems for sites with larger scan volumes. Load balancing is handled through the storage system interface.

Virus scanning on the storage system is available only for those files that are requested through CIFS. Files requested through NFS clients are not scanned for viruses.

What Happens When a File Is Scanned

The NetApp storage system can submit files to Symantec Protection Engine for scanning on open, read, rename, and close operations. Scanning can also be configured for the CIFS share.

When a user tries to access a file, the storage system passes the file to Symantec Protection Engine for scanning. After the file is scanned, Symantec Protection Engine indicates the scan results to the storage system:

- If the file is infected and can be repaired, the protection engine returns the repaired file to the user after taking the action configured in the virus scanning policy. The stored version of the infected file is then replaced with the repaired file.
- If the file is infected and cannot be repaired, the user is denied access to the file and the infected file is deleted from the storage system. Symantec Protection Engine can be configured to quarantine unrepairable files.

The storage system caches scan results for files (along with the antivirus definition version) to avoid redundantly scanning files that have already been scanned. When a file is accessed by the user, the storage system checks the antivirus version for the last scan of that file against the version of the available protection engines and performs one of the following actions:

- If the file version matches the version of any available scanner, the file is not scanned.
- If the versions do not match, a scan is triggered.
- If the cache is full and a file that is not in the cache is accessed, the oldest information in the cache is purged so that the scan results for the newly scanned file can be stored.

Connecting to Symantec Protection Engine

A connection is maintained between each NetApp storage system and Symantec Protection Engine. Symantec Protection Engine monitors the connection with each storage system by checking the connection at a configured time interval. The protection engine tries to reconnect if it determines that the connection is not active. The number of times that the protection engine tries to reestablish the connection can also be configured.

Limiting Scanning by File Type

Viruses are found only in file types that contain executable code. Therefore, only the file types that can contain executable code need be scanned. Limiting scanning by file type saves bandwidth and time. Table 2 describes how you can limit virus scanning by file type.

Table 2) Limiting virus scanning by file type.

Level of Control	Description
You can control the files that are initially submitted to the protection engine by the storage system for scanning.	The storage system lets you specify the file extensions to be excluded from scanning and the files to be passed to Symantec Protection Engine for scanning. You can configure the file types that you want to submit for scanning through the storage system interface.
You can control which of the files embedded in archival file formats (for example, .zip or .lzh files) will be scanned by Symantec Protection Engine.	Symantec Protection Engine lets you specify the file types and the file extensions that you do not want to scan: • You can create exclusion lists to limit scanning of certain file types and file extensions. • You can scan all file types regardless of extension. • You can configure which embedded files are scanned through the Symantec Protection Engine administrative interface.

Note: For more information, see Enhance Performance by Limiting Scanning and Excluding Files from Scanning.

Handling Infected Files

You can configure Symantec Protection Engine to take any of the following sets of actions when an infected file is found:

- **Scan only.** Scan for viruses; deny access to the infected file but do nothing to the infected file.
- **Scan and repair files.** Scan for viruses; try to repair the infected file and deny access to any unrepairable file.
- **Scan and repair or delete.** Scan for viruses; try to repair the infected file and delete any unrepairable file.

You can also configure the protection engine to quarantine unrepairable files. For more information about how to configure Symantec Protection Engine to handle infected files, see the section “Configure Antivirus Scan Policy.”

4.2 Prepare to Install Symantec Protection Engine

Before you install Symantec Protection Engine, complete the following tasks:

1. If you want to use an authentication method based on Windows Active Directory to access the Symantec Protection Engine console, verify the following:
   - A security group in Active Directory is authorized to access the Symantec Protection Engine console. You can either create the security group or identify an existing group to access the Symantec Protection Engine console.
   - The server on which you plan to install Symantec Protection Engine belongs to the same domain or has a trust relationship with the Active Directory instance that contains the security group authorized to access the Symantec Protection Engine console.
2. Install JRE 7.0 (update 45 or later).

Note: You must install JRE only if you plan to operate Symantec Protection Engine in the core server with the user interface mode.

3. Disable any third-party antivirus products that are running on the server on which you plan to install Symantec Protection Engine. You can turn on the antivirus protection after the Symantec Protection Engine installation is complete.

   Note: Symantec Protection Engine scans the files that client applications pass to Symantec Protection Engine but does not protect the computer on which it runs. Because Symantec Protection Engine processes files that might contain threats, the server on which it runs is vulnerable if it has no real-time protection. Use an antivirus program such as Symantec Endpoint Protection to protect the server on which Symantec Protection Engine runs. To prevent scanning conflicts, configure the antivirus program to not scan the temporary directory that Symantec Protection Engine uses for scanning.

4. Review the deployment considerations and recommendations. These recommendations can enhance your overall performance.

4.3 Install Symantec Protection Engine on Windows

The Symantec Protection Engine installer checks for the previous version of the product before installing or upgrading to a newer version. The results of the check determine what happens next, as described in Table 3.

Table 3) Installer check results.

Version Detected	Action Taken by Installer
No previous version is detected.	A full installation is performed.
Version 7.0 is detected.	Symantec Protection Engine supports an upgrade from version 7.0. You can select to upgrade the product and preserve your existing settings or to perform a clean upgrade. If you choose to do a clean upgrade, the installer removes the previous version and then installs the newer version as a full installation, without preserving the previous settings.
Version 5.1 or 5.2 is detected.	Symantec Protection Engine does not support direct upgrades from version 5.1 or 5.2. You must first upgrade to version 7.0 and then further upgrade to version 7.5.
Version 5.0 is detected.	Symantec Protection Engine does not support direct upgrades from version 5.0. To install version 7.5, you must first either uninstall version 5.0 or upgrade to version 7.0 and then further upgrade to version 7.5.
Version 4.3.x is detected.	Symantec Protection Engine does not support direct upgrades from version 4.3.x. To install version 7.5, you must first either uninstall 4.3.x or upgrade to 5.2.x, then upgrade to 7.0, and then further upgrade to version 7.5.

After you install Symantec Protection Engine, activate all applicable licenses. If you upgrade from a previous version that had valid licenses, Symantec Protection Engine automatically recognizes these licenses after the installation is complete.

Symantec Protection Engine is shipped with the minimum set of URL definitions. If you want to use the URL filtering feature, run LiveUpdate and get the latest URL definitions before you start URL filtering. If Symantec Protection Engine fails to start before it can initiate standard logging, information about the failure is written to the abort log file (`SymantecProtectionEngineAbortLog.txt`). This file is located in the installation directory.

Note: If you need to install or upgrade multiple Symantec Protection Engine instances on your network, you can use the silent installation or upgrade feature to facilitate the process. For more

information, see the Symantec Protection Engine for Network Attached Storage Implementation Guide.

During the Symantec Protection Engine installation, you can choose the authentication mode for accessing the Symantec Protection Engine console:

- **If you choose authentication based on Symantec Protection Engine**, Symantec Protection Engine installs an administrator account. Symantec recommends that you remember the password for this account because it is the only account used to manage Symantec Protection Engine. If you want to change the password in the console, you must have the old password.
- **If you choose authentication based on Active Directory**, Symantec Protection Engine allows users from the authorized Active Directory security group to access the console.

Note: Before you begin the installation process, ensure that your computer meets the minimum system requirements.

When the installation is complete, Symantec Protection Engine is installed as a Windows Server 2008 or Windows Server 2012 service. It is listed as Symantec Protection Engine in the services console. The Symantec Protection Engine service starts automatically when the installation is complete. Any significant installation activities are recorded in the Windows Application Event Log.

Install Antivirus Engine with Authentication based on Symantec Protection Engine

To install Symantec Protection Engine on Windows with Symantec Protection Engine-based authentication, complete the following steps:

1. Log in to the computer on which you plan to install Symantec Protection Engine as an administrator or as a user with administrator rights.
2. From the Symantec Protection Engine .zip file, run `SymantecProtectionEngine.exe` to start the installation wizard.
3. On the Welcome page of the wizard, click Next.
4. On the License Agreement page, read and accept the terms of the Symantec Software License Agreement. Click Next.

   Note: The default setting is that you do not agree with the terms of the Symantec Software License Agreement. If you do not indicate that you agree, the installation is canceled.
5. On the Destination Folder page, select the location to install Symantec Protection Engine and then click Next:
   - For 32-bit Windows platforms, the default location is `C:\Program Files\Symantec\Scan Engine`.
   - For 64-bit Windows platforms, the default location is `C:\Program Files (x86)\Symantec\Scan Engine`.
6. On the Initialization Methods page, select one of the following options and then click Next:
   - If you want to use the user-interface console of Symantec Protection Engine, select Core Server with User Interface (Requires JRE). This method requires JRE to be installed. Go to step 7.
   - If you do not want to use the user-interface console of Symantec Protection Engine, select Core Server Only (Does Not Require JRE). This method does not require JRE to be installed. Go to step 10.
7. On the UI Authentication Method page, select Symantec Protection Engine-Based Authentication. Click Next.
8. On the Administrative UI Setup page, type a password for the administrator account that you intend to use to manage Symantec Protection Engine and then confirm the password. Click Next.
9. On the Administrative UI Setup page, configure the port options and then click Next:

a. For Administrator Port, type the port number on which the web-based console listens. The default port number is 8004.

   If you change the port number, use a number that is greater than 1024 and that is not in use by any other program or service. You can disable the console by typing `0`. If you disable the console, you can configure Symantec Protection Engine by editing the configuration file.

b. For SSL Port, type the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security. The default SSL port number is 8005.

   If this port is already in use, select an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.

10. On the URL Filtering page, select the provided option to enable the URL filtering feature and the downloading of URL definitions. Click Next.

    Note: You can change this setting after the installation is complete. Go to Policies > Filtering URL to set this option.

11. On the Reputation-Based Protection (Insight) page, configure the Insight feature and then click Next:

    a. Select the Enable Insight checkbox to enable the Insight feature.

    Note: The Select Insight Aggression Level drop-down list is enabled only if you select the Enable Insight checkbox.

    b. Set the Insight aggression level.

    Note: If you set the level higher, Insight detects more files as malicious. Higher settings, however, return more false positives.

12. On the Ready to Install the Program page, click Install.
13. Click Finish.

Install Antivirus Engine with Authentication Based on Active Directory

To install Symantec Protection Engine on Windows with authentication based on Active Directory, complete the following steps:

1. Log in to the computer on which you plan to install Symantec Protection Engine as an administrator or as a user with administrator rights.
2. On the Symantec Protection Engine installation CD, run `SymantecProtectionEngine.exe` to start the installation wizard.
3. On the Welcome page of the wizard, click Next.
4. On the License Agreement page, read and accept the terms of the Symantec Software License Agreement. Click Next.

   Note: The default setting is that you do not agree with the terms of the Symantec Software License Agreement. If you do not indicate that you agree, the installation is canceled.

5. On the Destination Folder page, select the location to install Symantec Protection Engine and then click Next:
   - For 32-bit Windows platforms, the default location is `C:\Program Files\Symantec\Scan Engine`.
   - For 64-bit Windows platforms, the default location is `C:\Program Files (x86)\Symantec\Scan Engine`.
6. On the Initialization Methods page, select one of the following options and then click Next:
   - If you want to use the user-interface console of Symantec Protection Engine, select Core Server with User Interface (Requires JRE). This method requires JRE to be installed. Go to step 7.

- If you do not want to use the user-interface console of Symantec Protection Engine, select Core Server Only (Does Not Require JRE). This method does not require JRE to be installed. Go to step 10.

7. On the UI Authentication Method page, select Windows Active Directory-Based Authentication. Click Next.
8. On the Windows Active Directory-Based Authentication Settings page, in the Group Name box, type a valid security group name in the `domain\groupname` format. Click Next.

   Note: If the group name is incorrect, a Group Name Validation message appears. Click Back to type the security group name again.

   Alternatively, click Next to continue the installation without a valid group name. The Symantec Protection Engine service will start after the installation, but you will not be able to access the Symantec Protection Engine console. After the installation is complete, you must go to the `configuration.xml` file and enter the user name to be able to access the console.
9. On the Administrative UI Setup page, configure the port options and then click Next:
   a. For Administrator Port, type the port number on which the web-based console listens. The default port number is 8004.

      If you change the port number, use a number that is greater than 1024 and that is not in use by any other program or service. You can disable the console by typing `0`. If you disable the console, you can configure Symantec Protection Engine by editing the configuration file.

   b. For SSL Port, type the Secure Socket Layer (SSL) port number on which encrypted files are transmitted for increased security. The default SSL port number is 8005.

      If this port is already in use, select an SSL port that is not in use by any other program or service. Use a port number that is greater than 1024.
10. On the URL Filtering page, select the provided option to enable the URL filtering feature and the downloading of URL definitions. Click Next.

    Note: You can change this setting after the installation is complete. Go to Policies > Filtering URL to set this option.
11. On the Reputation-based Protection (Insight) page, configure the Insight feature and then click Next:
    a. Select the Enable Insight checkbox to enable the Insight feature.

    Note: The Select Insight Aggression Level drop-down list is enabled only if you select the Enable Insight checkbox.

    b. Set the Insight aggression level.

    Note: If you set the level higher, Insight detects more files as malicious. Higher settings, however, return more false positives.
12. On the Ready to Install the Program page, click Install.
13. Click Finish.

4.4 Access Symantec Protection Engine Console

The Symantec Protection Engine console is a web-based interface that you can use to manage Symantec Protection Engine. The interface is provided through a built-in HTTPS server. You can access the interface by using the virtual administrative account that you set up during installation. You access the Symantec Protection Engine console through a web browser; you can use any computer on your network that can access the server that is running Symantec Protection Engine.

Note: Symantec Protection Engine no longer supports accessing the console through an HTTP server.

The first time that you access the Symantec Protection Engine console after login, one of the following occurs:

- The **license page** appears. If the license page appears, no valid license is installed. The license page is the only page that is active until you install a valid license.
- The **homepage** appears. If the homepage appears, at least one valid license is installed. You can navigate through the entire console.

When a valid license is installed, each time that you start a new browser session, log in, and open the console, the homepage appears. If the browser session continues to run, you return to the page that you were on when you logged off or when the session timed out.

Note: Only one user should use the console at a time to avoid possible race conditions and configuration change conflicts.

To access the Symantec Protection Engine console, complete the following steps:

1. Open a web browser on any computer on your network that can access the server that is running Symantec Protection Engine.
2. In the web browser, type the address `https://<servername>:<port>/`, where:
   - `<servername>` is the host name or IP address of the server that is running Symantec Protection Engine.
   - `<port>` is the port number that you selected for the built-in web server during installation. The default port number is 8004.
3. If a Security Alert dialog box appears, click Yes to confirm that you trust the integrity of the applet and then click Yes to display the webpage.
4. In the Enter Password box, type the password for the administrative account.
5. Press Enter.

4.5 Configure Symantec Protection Engine to Work with Clustered Data ONTAP

For Symantec Protection Engine to work with clustered Data ONTAP, you must complete the following tasks:

- Configure Symantec Protection Engine to use RPC as the communication protocol. The Internet Content Adaptation Protocol (ICAP) is the default protocol at installation, but you can change the protocol to RPC through the administrative interface and then configure the RPC-specific options.
- Configure Symantec Protection Engine parameters specific to clustered Data ONTAP.
- Edit the Windows service startup properties to identify an account that has the appropriate permissions.

Configure Symantec Protection Engine to Use RPC as Communication Protocol

After you install Symantec Protection Engine, you must configure settings that are specific to the RPC protocol:

- Change the protocol to RPC and provide an IP address for each storage system for which Symantec Protection Engine will provide virus-scanning services. You can edit this list to add or delete storage systems at any time.
- Configure the additional RPC-specific options.
- Configure the antivirus scan policy.

You must manually stop and restart the Symantec Protection Engine service when you change to the RPC protocol to ensure that there is a proper connection to the NetApp storage system. Table 4 summarizes the RPC protocol options that you must configure.

Table 4) RPC protocol options.

Option	Description
Protocol	You must change the protocol to RPC.
RPC client list	A single Symantec Protection Engine instance can support one or more NetApp storage systems. The storage systems must be located in the same domain as the protection engine. You must provide the IP address of each storage system. Enter 127.0.0.1 in the RPC client list for Symantec Protection Engine to be able to operate with clustered Data ONTAP. **Note:** Multiple protection engines can support a single storage system. Configure the scan engines through the storage system interface.
Check RPC connection every __ seconds	Symantec Protection Engine maintains a connection with the storage system. You can configure Symantec Protection Engine to check the connection with the storage system at a prescribed interval to verify that the connection is active. The default value is 20 seconds.
Maximum number of reconnect attempts	You can configure the protection engine to make a specified number of tries to reestablish a lost connection with a storage system. By default, Symantec Protection Engine is configured to try to reconnect with the storage system indefinitely. **Note:** Do not set a maximum number of reconnect attempts if the protection engine provides virus scanning for multiple storage systems. Use the default setting.
Automatically send antivirus update notifications	You can configure Symantec Protection Engine to automatically notify the storage system when new virus definitions are used. This notification causes the storage system to clear its cache of scanned files.
Antivirus scan policy	You can configure Symantec Protection Engine to do one of the following operations when an infected file is found: • Scan only • Scan and repair • Scan and repair or delete

Change Protocol to RPC and Edit List of NetApp Storage Systems

To change the protocol that Symantec Protection Engine uses for communication to RPC and to edit the list of storage systems, complete the following steps:

1. On the Symantec Protection Engine administrative interface, in the left pane, click Configuration.
2. Under Views, click Protocol.
3. In the right pane, under Select Communication Protocol, click RPC. The configuration settings are displayed for the selected protocol.
4. In the Manual Restart Required dialog box, click OK. Whenever you switch protocols, you must restart the server. You can continue to make and apply changes in the administrative interface. However, the changes do not take effect until you restart the Symantec Protection Engine service.
5. Add NetApp storage systems to the list of RPC clients:

a. Type the IP addresses of the storage systems for which Symantec Protection Engine will provide scanning services. Type one entry per line.

b. Enter 127.0.0.1 in the RPC client list for Symantec Protection Engine to be able to operate with clustered Data ONTAP.

6. To delete a storage system from the list of RPC clients, select and delete the IP address of the storage system.
7. On the toolbar, click one of the following options:
   - Click Save to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click Apply to apply your changes. Your changes are not implemented until you apply them. You must perform a manual restart for the changes to take place and for a proper connection to the storage system.

Configure Additional RPC-Specific Options

To configure additional RPC-specific options, complete the following steps:

1. On the Symantec Protection Engine administrative interface, in the left pane, click Configuration.
2. Under Views, click Protocol.
3. Under RPC Configuration, in the Check RPC Connection Every box, type how frequently Symantec Protection Engine should check the RPC connection with the storage system to verify that the connection is active. The default interval is 20 seconds.
4. In the Maximum Number of Reconnect Attempts box, type the maximum number of tries that Symantec Protection Engine will undertake to reestablish a lost connection with the storage system.

   Note: The default setting is 0. Symantec Protection Engine tries indefinitely to reestablish a connection. Use the default setting if the protection engine provides scanning for multiple NetApp storage systems.

5. On the toolbar, click one of the following options:
   - Click Save to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click Apply to apply your changes. Your changes are not implemented until you apply them. You must perform a manual restart for the changes to take place and for a proper connection to the storage system.

Configure Antivirus Scan Policy

To configure the antivirus scan policy, complete the following steps:

1. On the Symantec Protection Engine administrative interface, in the left pane, click Policies.
2. Under Views, click Scanning.
3. Select an antivirus scan policy to configure Symantec Protection Engine to take one of the following sets of actions when an infected file is found:
   - Scan only. Scan the file for viruses; deny access to the infected file but do nothing to the infected file.
   - Scan and repair files. Scan the file for viruses; try to repair the infected file and deny access to any unrepairable file.
   - Scan and repair or delete. Scan the file for viruses; try to repair the infected file and delete any unrepairable file from archived files.

   Note: You must select the scan and repair or delete option if you plan to quarantine infected files that cannot be repaired. For more information, see the Symantec Protection Engine for Network Attached Storage Implementation Guide.

4. On the toolbar, click one of the following options:
   - Click Save to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click Apply to apply your changes. Your changes are not implemented until you apply them. You must perform a manual restart for the changes to take place and for a proper connection to the storage system.

Configure Symantec Protection Engine Parameters Specific to Clustered Data ONTAP

You can configure some parameters specific to clustered Data ONTAP in the Symantec Protection Engine `configuration.xml` file. To modify an XML file, you must know its XPath and the field values. You can use the XML modifier command-line tool of Symantec Protection Engine to configure the following options:

- Enable granular scan status for clustered Data ONTAP
- Specify client information logging in log files
- Specify a notification threshold in case of overload
- Specify scanning through an encoded path

Note: The XML modifier command-line tool is available by default in the installation directory of Symantec Protection Engine.

Enable Granular Scan Status for Clustered Data ONTAP

If you enable granular scan status for clustered Data ONTAP, Symantec Protection Engine registers with scanning functionality and reports the granular status of the scan. Examples of reported statuses are no violation found, infection found, file is repaired, container violation found, and error encountered during scan. If you disable granular scan status, Symantec Protection Engine reports only whether a policy violation has occurred or not.

Table 5 presents the settings for the option to enable granular scan status.

Table 5) Granular scan status for clustered Data ONTAP.

XPath	Field Values	XML File

`/configuration/protocol/RPC/EnableGranularScanStatus`	• True (default). Enables Symantec Protection Engine to send the granular scan status for clustered Data ONTAP.
	• False. Disables Symantec Protection Engine from sending the granular scan status for clustered Data ONTAP.
		`configuration.xml`
		
		Example:
		`./xmlmodifier -s //protocol/RPC/EnableGranularScanStatus/@value true configuration.xml`

Specify Client Information Logging in Log Files

By default, Symantec Protection Engine logs client information only when a policy violation is detected. You can choose to log the client information for all scanned files; however, doing so can affect performance. Symantec Protection Engine logs client information such as the DNS host name, IP address of the host that requested the scan, and name of the server that initiated the scan request.

Table 6 presents the settings for the option to log client information.

Table 6) Client information logging in log files.

XPath	Field Values	XML File

`/configuration/protocol/RPC/LogClientInformationForCleanFiles`	• True. Logs client information for all files.
	• False (default). Logs client information only when a policy violation is detected.
		`configuration.xml`
		
		Example:
		`./xmlmodifier -s //protocol/RPC/LogClientInformationForCleanFiles/@value true configuration.xml`

Specify Notification Threshold in Case of Overload

Note: This option is applicable only to the RPC protocol.

You can use this option to send a notification to the specified logging destinations when Symantec Protection Engine reaches its threshold for queued scan requests. Symantec Protection Engine then rejects further requests and sends a notification that the threshold has been reached. This feature lets the client determine load balancing and prevents the server from being overloaded with scan requests.

Note: To use this option, you must first enable the granular scan status parameter. That is, `EnableGranularScanStatus = true`.

Table 7 presents the settings for the option to send a notification when queued scan requests reach the specified threshold.

Table 7) Notification when queued scan requests reach threshold.

XPath	Field Values	XML File

`/configuration/protocol/RPC/EnableServerTooBusyResponse`	• True (default). Enables Symantec Protection Engine to send a notification when queued requests reach the threshold.
	• False. Disables Symantec Protection Engine from sending a notification when queued requests reach the threshold.
		`configuration.xml`
		
		Example:
		`./xmlmodifier -s //protocol/RPC/EnableServerTooBusyResponse/@value true configuration.xml`

Specify Scanning Through Encoded Path

By default, Symantec Protection Engine enables scanning of files through their encoded paths:

- If you enable the scanning of files through encoded paths, Symantec Protection Engine communicates to the storage system that it can accept encoded paths. The storage system sends the information to be scanned to Symantec Protection Engine with encoded characters.
- If you disable this capability, the storage system sends information to be scanned to Symantec Protection Engine as a regular UNC path without any encoding.

Table 8 presents the settings for the option to scan files through an encoded path.

Table 8) Scanning files through an encoded path.

XPath	Field Values	XML File
`/configuration/proto`	• True (default). Enables the scanning of files through the	`configuration.xml`

XPath	Field Values	XML File
`col/RPC/EncodedPaths`	encoded path. • False. Disables the scanning of files through the encoded path.	**Example:** `./xmlmodifier –s //protocol/RPC/EncodedPaths/@value true configuration.xml`

Edit Service Startup Properties

If you change the protocol setting to RPC, you must change the service startup properties to identify a user account that has the following permissions:

- Local administrator permissions on the computer on which the protection engine is installed
- Backup operator privileges or higher on the NetApp storage system

Note: You must change the service startup properties if the list of NetApp storage systems is edited. See the section "Configure Symantec Protection Engine to Use RPC as Communication Protocol."

To edit the service startup properties, complete the following steps:

1. On the Windows Server 2008 SP2 (64-bit) or Windows Server 2012 (64-bit) Control Panel, click Administrative Tools.
2. Click Services.
3. In the list of services, right-click Symantec Protection Engine and then select Properties.
4. In the Properties dialog box, on the Log On tab, click This Account.
5. Type the account name and password for the user account that has local administrator rights on the computer on which Symantec Protection Engine is installed. This account should also have domain backup operator privileges or higher.

   Note: Use the format `domain\username` for the account name.
6. Click OK.
7. Stop and restart the Symantec Protection Engine service.

   Note: For more information about stopping and restarting the Symantec Protection Engine service, see the Symantec Protection Engine for Network Attached Storage Implementation Guide.

4.6 Schedule LiveUpdate to Update Virus Definitions Automatically

You must schedule LiveUpdate to occur automatically at a specified time interval so that Symantec Protection Engine has the most current virus definitions. If you use multiple protection engines to support virus scanning, schedule LiveUpdate to occur at the same time for each protection engine. This scheduling enables all protection engines to have the same version of virus definitions. Having the same version of virus definitions is necessary for the proper functioning of virus scanning on the NetApp storage system.

You must schedule LiveUpdate on each Symantec Protection Engine. When LiveUpdate is scheduled, it runs at the specified time interval relative to the LiveUpdate base time. The default LiveUpdate base time is the time that the protection engine was installed, but you can change the LiveUpdate base time. If you change the scheduled LiveUpdate interval, the interval adjusts based on the LiveUpdate base time.

Note: For more information about changing the base time, see the Symantec Protection Engine for Network Attached Storage Implementation Guide.

To schedule LiveUpdate to update virus definitions automatically, complete the following steps:

1. On the Symantec Protection Engine administrative interface, in the left pane, click System.
2. Under Views, click LiveUpdate Content.
3. In the right pane, under LiveUpdate Content, select the Enable Scheduled LiveUpdate checkbox. This option is enabled by default.
4. In the LiveUpdate Interval drop-down list, choose an interval. You can select from 2, 4, 8, 10, 12, or 24-hour intervals. The default LiveUpdate interval is 2 hours.
5. On the toolbar, click one of the following options:
   - Click Save to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click Apply to apply your changes. Your changes are not implemented until you apply them.

4.7 Configure Rapid Release Updates to Occur Automatically

You can configure Symantec Protection Engine to obtain uncertified definition updates with Rapid Release and to retrieve Rapid Release definitions every 5 to 120 minutes.

Rapid Release definitions are created when a new threat is discovered. The definitions undergo basic quality assurance tests by Symantec Security Response. However, they do not undergo the intense testing that is required for a LiveUpdate release. Symantec updates Rapid Release definitions as needed to respond to high-level outbreaks.

Note: Rapid Release definitions do not undergo the same rigorous quality assurance tests as LiveUpdate and Intelligent Updater definitions. Symantec encourages users to rely on the full quality-assurance-tested definitions whenever possible. Always deploy Rapid Release definitions in a test environment before you install them on your network.

If you are using a proxy or firewall that blocks FTP communications, the Rapid Release feature will not function. Your environment must allow FTP traffic for the FTP session to succeed.

You can schedule Rapid Release updates to occur automatically at a specified time interval so that Symantec Protection Engine has the most current definitions. Scheduled Rapid Release updates are disabled by default.

To configure Rapid Release updates to occur automatically, complete the following steps:

1. On the Symantec Protection Engine administrative interface, in the left pane, click System.
2. Under Views, click Rapid Release Content.
3. In the content area under Rapid Release Content, select the Enable Scheduled Rapid Release checkbox to enable automatic downloads of Rapid Release definitions. This option is disabled by default.
4. In the Rapid Release interval box, specify the interval between which you want Symantec Protection Engine to download Rapid Release definitions. You can select any number between 5 and 120 minutes. The default value is 30 minutes. To specify the interval, you can either type it or click the up arrow or the down arrow to select the target interval.
5. On the toolbar, click one of the following options:
   - Click Save to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click Apply to apply your changes. Your changes are not implemented until you apply them.

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 9 must be in place.

Table 9) Prerequisites for installing Antivirus Connector.

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

To install Antivirus Connector, complete the following steps:

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

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

Best Practices

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

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

Best Practices

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

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

Important

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

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

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

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

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

5.2 Add SVMs to Antivirus Connector

To send files for virus scanning, you must configure Antivirus Connector to connect to one or more SVMs by entering the Data ONTAP management LIF, the poll information, and the account credentials. The management LIF is polled to retrieve the list of data LIFs. Before you can add SVMs to Antivirus Connector, the prerequisites in Table 10 must be in place.

Table 10) Prerequisites for adding an SVM to Antivirus Connector.

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

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

1. Right-click the Configure ONTAP Management LIFs for Polling icon, which was saved on your desktop when you completed the Antivirus Connector installation. Select Run as Administrator.
2. in the Configure Data ONTAP Management LIFs for Polling dialog box, configure the following settings:
   a. Specify the management LIF of the SVM:
   – If you have an existing management LIF or IP address, enter the management LIF or IP address of the SVM that you want to add.
   – If you want to create a management LIF, create one with the role set to `data`, the data protocol set to `none`, and the firewall policy set to `mgmt`. For more information about creating a LIF, see the Clustered Data ONTAP 8.2 Network Management Guide.

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

   b. Enter the poll duration, in seconds.

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

c. Enter the account name and password.

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

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

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

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

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

6 Configuring Vscan Options in Clustered Data ONTAP

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

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

6.1 Create Scanner Pool

You must create a scanner pool for an SVM or a cluster to define the list of Vscan servers and privileged users that are allowed to access and connect to that SVM or cluster. Before you can configure a scanner pool, the prerequisite in Table 11 must be in place.

Table 11) Prerequisite for configuring a scanner pool for SVMs.

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

Scanner pools have the following characteristics and limits:

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

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

Configure Scanner Pool for SVM

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

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

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

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

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

Configure One Scanner Pool for Use with Multiple SVMs

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

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

Cluster-Scoped Configuration

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

1. Create a scanner pool with the cluster scope.

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

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

SVM-Scoped Configuration

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

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

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

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

   Note: Due to the trust relationship between domains, the authentication request 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 vscan scanner-pool apply-policy` command.

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

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

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

6.3 Create Vscan Policy

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

- On-access policy
- On-demand policy

On-Access Policy

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

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

Best Practices

- Consider excluding large files (file size can be specified) from virus scanning because they might result in a slow response or a scan request timeout for CIFS users. The default file size for exclusion is 2GB.
- Consider excluding file extensions such as .vhd and .tmp because files with these extensions might not be appropriate for scanning.
- Consider excluding file paths such as the quarantine directory or paths in which only virtual hard drives or databases are stored.
- Verify that all exclusions are specified in the same policy, because only one policy can be enabled at a time. NetApp highly recommends that you specify the same set of exclusions on the antivirus engine. For more information about supported exclusions, contact Symantec.

Create On-Access Policy

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

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

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

```
vserver vscan on-access-policy create -vserver vs1 -policy-namePolicy1 -protocol CIFS -filters
scan-ro-volume -max-file-size 3GB -file-ext-to-exclude "mp3","txt" -paths-to-exclude "\vol\a
b\","\vol\a,b\"
```

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

Enable On-Access Policy

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

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

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

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

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

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

On-Demand Policy

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

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

Create On-Demand Task

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

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

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

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

Table 12 describes the parameters used in the command.

Table 12) On-demand task parameters.

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

Run an On-Demand Task

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

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

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

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

6.4 Enable Virus Scanning on SVM

After you configure the scanner pool, the on-access policy, and the Vscan file-operations profile parameter, you must enable virus scanning on the SVM to protect the data. When virus scanning is enabled on the SVM, the SVM connects to the Vscan servers that are listed in the active scanner pool for that SVM. Before you can enable virus scanning on the SVM, the prerequisites in Table 13 must be in place.

Table 13) Prerequisites for enabling virus scanning on the SVM.

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

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

1. Run the `vserver vscan enable` command.

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

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

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

7 Managing Vscan Options in Clustered Data ONTAP

7.1 Modify Vscan File-Operations Profile for CIFS Share

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

Before you can modify the Vscan file-operations profile for a CIFS share, the prerequisite in Table 14 must be in place.

Table 14) Prerequisite for modifying the Vscan file-operations profile.

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

Table 15 lists the file-operations profile types and the file operations that they monitor.

Table 15) Types of file-operations profiles.

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

Best Practices

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

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

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

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

7.2 Manage Scanner Pools

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

View Scanner Pools of SVMs

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

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

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

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

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

View Active Scanner Pools of SVMs

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

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

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

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

Modify Scanner Pool

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

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

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

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

Delete Scanner Pool

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

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

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

Add Privileged Users to Scanner Pool

You can add one or more privileged users to a scanner pool to define the privileged users who can connect to an SVM. Before you can add privileged users to the scanner pool, the prerequisite in Table 16 must be in place.

Table 16) Prerequisite for adding privileged users to a scanner pool.

Description
You have created a scanner pool for the SVM.

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

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

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

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

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

Remove Privileged Users from Scanner Pool

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

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

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

View Privileged Users of All Scanner Pools

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

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

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

Add Vscan Servers to Scanner Pool

You can add one or more Vscan servers to a scanner pool to define the Vscan servers that can connect to an SVM. Before you can add Vscan servers to the scanner pool, the prerequisite in Table 17 must be in place.

Table 17) Prerequisite for adding Vscan servers to a scanner pool.

Description
You have created a scanner pool for the SVM.

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

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

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

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

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

Remove Vscan Servers from Scanner Pool

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

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

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

View Vscan Servers of All Scanner Pools

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

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

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

7.3 Manage On-Access Policies

You can manage on-access policies to define the scope of scanning when files are accessed by a client. You can modify the maximum file size that is allowed for virus scanning and the file extensions and file paths to be excluded from scanning. You can also delete and disable an on-access policy if it is no longer required.

View On-Access Policies of SVMs

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

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

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

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

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

Modify On-Access Policy

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

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

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

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

Disable On-Access Policy

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

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

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

Delete On-Access Policy

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

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

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

7.4 Manage On-Demand Task

View On-Demand Task Information

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

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

Manage On-Demand Task Schedule

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

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

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

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

On-Demand Task Report

Each on-demand task creates a report that contains results of the scan job. Table 18 lists the parameters contained in the reports. You can generate reports based on these parameters.

Table 18) On-demand task parameters.

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

To generate the reports, complete the following step:

1. Run the following command:

```
vscan_on_demand_report
```

Delete On-Demand Task

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

1. Run the following command:

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

Manage On-demand Task Job

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

1. Run the following command:

```
job show –name *on-demand*
```

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

```
job stop –id <job-id>
```

8 General Best Practices

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 Symantec 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 Symantec 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 Symantec 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 be lesser than the `scanner-pool request-timeout`. If it is set to a higher value, access to files might be delayed and may eventually time out.

  To avoid this, configure the `scan-engine timeout` to 5 seconds lesser than the `scanner-pool request-timeout` value. See the scan engine vendor's documentation for instructions on how to change the `scan-engine timeout` settings. The `scanner-pool timeout` can be changed by using the following command in advanced mode and by providing the appropriate value for the `request-timeout` parameter:

```
vserver vscan scanner-pool modify
```

- For an environment that is sized for on-access scanning workload and requiring the use of on-demand scanning, it is recommended to schedule the on-demand scan job in off-peak hours to avoid additional load on the existing AV infrastructure.

8.2 Best Practices for Symantec Protection Engine

Hardware and Software

Observe the following hardware and software best practices before installing Symantec Protection Engine:

- Verify that you comply with the hardware and software system requirements for Symantec Protection Engine.
- Before you install Symantec Protection Engine, install and configure the operating system software and applicable updates for your server. Also, ensure that your operating system software and server work correctly. For more information, see the documentation for your server.
- Verify that all software prerequisites are installed before you install Symantec Protection Engine.
- Ensure that you have installed and configured Antivirus Connector.
- Install the latest version (latest major version, CRT release, or hotfix release) of Symantec Protection Engine on a server that is dedicated to virus scanning and not used for other tasks.
- Use an antivirus program to protect the server on which Symantec Protection Engine runs, such as Symantec Endpoint Protection. To prevent scanning conflicts, configure the antivirus program not to scan the temporary directory (`C:\Program Files (x86)\Symantec\Scan Engine\Temp`) that Symantec Protection Engine uses for scanning.

Configuration Best Practices

Table 19 explains the best practices to implement when you configure Symantec Protection Engine.

Table 19) Configuration best practices.

Configuration Item	Best Practice
Maximum RAM to use for in-memory file system	Configure 2048MB as the maximum amount of RAM to use for the in-memory file system. For systems with larger amounts of memory, scanning is improved when a larger section of RAM is set aside for in-memory file scanning. **Note:** For more information, see the section “Allocate Resources for Symantec Protection Engine.”
Clustered Data ONTAP configuration for RPC protocol	Enable the following Symantec Protection Engine parameters: • **Encoded paths**. For more information, see the section “Specify Scanning Through Encoded Path.” • **Granular scan status reporting.** Symantec Protection Engine reports the granular status for each scan request. For more information, see the section “Enable Granular Scan Status for Clustered Data ONTAP.” • **Scan request load balancing and notification threshold in case of overload.** With this feature, clustered Data ONTAP can load balance scan requests sent to Symantec Protection Engine and prevent Symantec Protection Engine from being overloaded with scan requests. For more information, see the section “Specify Notification Threshold in Case of Overload.”
Definition update mechanism	Use LiveUpdate as the preferred update mechanism and keep the update frequency as two hours.
Event log level, resources used, and statistics	Configure the following settings: • **Logging level.** Keep logging at the warning level in the

Configuration Item	Best Practice
	configured logging destination. • **Logging resources used by Symantec Protection Engine.** Ensure that Symantec Protection Engine logs the resources that it has used in a log file for analysis. • **Statistics.** Enable statistics logging and report cumulative scan data. • **Client information in log.** Symantec Protection Engine can log client information every time a file is scanned. For better performance, configure the parameter `LogClientInformationForCleanFiles` in the `configuration.xml` file to `false` so that the client information is logged only when a policy violation is detected. • **LiveUpdate Administration utility.** In scenarios in which multiple Symantec Protection Engine instances share the scanning load, you can save on the bandwidth required to download definitions by configuring one or more intranet FTP, HTTP, or LAN servers to act as internal LiveUpdate servers. Once an internal LiveUpdate server is configured, you can point all Symantec Protection Engine instances to it for definition updates. **Note:** For more information, see the LiveUpdate Administrator's Guide in the Symantec Protection Engine .zip file.

You can configure several parameters in Symantec Protection Engine by taking into account the type and the size of files that are sent for virus scanning. Table 20 describes these parameters.

Table 20) File configuration options.

Option	Configuration Description
Define the maximum file size that can be stored within the in-memory file system (in megabytes).	This parameter defines the maximum size of a particular file that can be loaded in memory for scanning. Files that exceed the specified size are written to the disk. **Note:** For more information, see the section “Allocate Resources for Symantec Protection Engine.”
Specify the file size threshold for in-place scanning.	The `FilerPerformanceThreshold` parameter allows you to specify the file size threshold value below which a file is copied from the RPC client share to the Symantec Protection Engine temporary folder. Therefore, for most of the files to be scanned in place, you must enter a threshold value that is lower than the average file size in your environment. **Note:** For more information, see the section “Specify File Size Threshold for in-Place Scanning.”
Enhance performance by limiting scanning.	You can exclude specific file extensions from scanning. When you enable this option, Symantec Protection Engine scans only the file extensions that are not in the exclusion lists. The default file exclusion lists contain the most common file extensions and the file types that are unlikely to contain threats. **Note:** For more information, see the section “Enhance Performance by Limiting Scanning.”

Option	Configuration Description
Specify file size threshold for scanning exclusion.	This parameter specifies the file sizes that will be excluded from scanning. Any file whose size is greater than or equal to the specified value is not scanned. Symantec Protection Engine reports the file as clean, logs that the file was bypassed from scanning, and increments the number of requests by 1. The `FileSizeScanThreshold` parameter accepts values in bytes. **Note:** For more information, see the section "Specify File Size Threshold for Scanning Exclusion."
Impose limits on container files	You can impose limits on how Symantec Protection Engine decomposes and scans container files. Imposing limits can conserve scanning resources. You can also specify whether to allow or deny access to files for which an established limit is met or exceeded. Access is denied by default. You can specify the following limits for handling container files: • The maximum amount of time, in seconds, that is spent decomposing a container file and its contents • The maximum file size, in megabytes, for the individual files that are in a container file • The maximum number of nested levels to be decomposed for scanning **Note:** For more information, see the section "Set Container File Limits."

9 Troubleshooting and Monitoring

9.1 Troubleshooting Virus Scanning

Table 21 lists common virus-scanning issues, their possible causes, and ways to resolve them.

Table 21) Common virus-scanning issues.

Issue	How to Resolve It
The Vscan servers are not able to connect to the clustered Data ONTAP storage system.	Check whether the scanner pool configuration specifies the Vscan server IP address. Check also if the allowed privileged users in the scanner pool list are active. To check the scanner pool, run the `vserver vscan scanner-pool show` command on the storage system command prompt. If the Vscan servers still cannot connect, there might be an issue with the network.
Clients observe high latency.	It is probably time to add more Vscan servers to the scanner pool.
Too many scans are triggered.	Modify the value of the `vscan-fileop-profile` parameter to restrict the number of file operations monitored for virus scanning.

Issue	How to Resolve It
Some files are not being scanned.	Check the on-access policy. It is possible that the path for these files has been added to the path-exclusion list or that their size exceeds the configured value for exclusions. To check the on-access policy, run the `vserver vscan on-access-policy show` command on the storage system command prompt.
File access is denied.	Check whether the `scan-mandatory` setting is specified in the policy configuration. This setting denies data access if no Vscan servers are connected. Modify the setting as appropriate.

9.2 Monitoring Status and Performance Activities

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

View Vscan Server Connection Information

You can view the connection status of Vscan servers to manage the connections that are already in use and the connections that are available for use. Table 22 lists the commands that display information about the connection status of Vscan servers.

Table 22) 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, 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 23.

Table 23) `offbox_vscan` counters: Vscan server requests and latencies across Vscan servers.

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

Example:

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

View Statistics for Individual Vscan Server Requests and Latencies

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

1. Run the `statistics show –object offbox_vscan –instance SVM:servername:nodename` command with the counters listed in Table 24.

Table 24) `offbox_vscan_server` counters: individual Vscan server requests and latencies.

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

Example:

```
Object: offbox_vscan_server
```

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

View Statistics for Vscan Server Utilization

You can also use Data ONTAP `offbox_vscan_server` counters to collect Vscan server–side utilization statistics. These statistics are tracked on a per-SVM, per–off-box Vscan server, and per-node basis. They include CPU utilization on the Vscan server; queue depth for scanning operations on the Vscan server, both current and maximum; used memory; and used network.

These statistics are forwarded by Antivirus Connector to the statistics counters within Data ONTAP. They are based on data that is polled every 20 seconds and must be collected multiple times for accuracy; otherwise, the values seen in the statistics reflect only the last polling. CPU utilization and queues are particularly important to monitor and analyze. A high value for an average queue can indicate that the Vscan server has a bottleneck.

To collect utilization statistics for the Vscan server on a per-SVM, per–off-box Vscan server, and per-node basis, complete the following step:

1. Run the `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` command with the counters listed in Table 25.

Table 25) `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
-------------------------------------------------------------------
```

9.3 Troubleshooting and Monitoring Symantec Protection Engine

To troubleshoot and monitor Symantec Protection Engine, perform the following tasks:

- Verify that the user account that you assign to the Symantec Protection Engine service has all of the following rights and permissions that are required for the RPC protocol:
  - Access rights to the RPC clients
  - Domain administrator privileges
  - Local administrator permissions on the computer on which Symantec Protection Engine is running
  - Rights to run as a service
- Verify that the Antivirus Connector services are running with the same user account that you assigned to the Symantec Protection Engine service.
- Verify that the RPC client IP address is correctly configured and successfully registered. The address 127.0.0.1 should be configured in the RPC client list for Symantec Protection Engine to be able to operate with clustered Data ONTAP. To view the RPC client list, complete the following steps:
  a. Launch the Symantec Protection Engine user interface.
  b. Go to Resources in the Reports tab.
  c. Review the list of RPC clients that are successfully registered.
- Verify information logs, error logs, or warning level logs after the RPC client is configured. At startup, Symantec Protection Engine logs a message that contains the Antivirus Connector version and status information. The log records the following details:
  - Antivirus Connector version
  - Antivirus Connector state
  - Management IP addresses
  - SVM IP addresses

  Note: If Symantec Protection Engine is not able to connect to the configured RPC client, it logs the message `Symantec Protection Engine has failed to connect to RPC client`.
- Review information about Symantec Protection Engine as explained in Table 26.

Table 26) Symantec Protection Engine detailed information.

Information to View	Symantec Protection Engine UI Navigation Flow
Symantec Protection Engine summary of overall statistics, definitions date, license status, and charts	Homepage
Symantec Protection Engine detailed statistics	Reports > Statistics
Detailed reports	Reports > Detailed
Registered RPC clients with Symantec Protection Engine and resources used by Symantec Protection Engine	Reports > Resources
Detailed license status	System > License
Detailed status of definitions	System > LiveUpdate Content

- Monitor scan requests. Symantec Protection Engine offers a feature that lets you define the expected scanning load for specific time periods. When the Symantec Protection Engine scanning load

decreases significantly, it might indicate a performance issue. You can use this feature to detect possible problems before they become critical. If Symantec Protection Engine detects fewer scan requests than the expected load, it logs the event to the designated logging destinations and alert destinations. The event is logged at the warning level.

To configure the monitoring feature, navigate to Monitors > Requests.

Appendix

Allocate Resources for Symantec Protection Engine

You can allocate resources for Symantec Protection Engine and limit the system resources that are devoted to scanning. You can also limit the server resources that Symantec Protection Engine uses for processing files in memory. Table 27 describes the resource settings.

Table 27) Resource settings.

Option	Description
Threshold number of queued requests	Symantec Protection Engine is at maximum load when the number of queued requests exceeds the specified threshold. You can configure Symantec Protection Engine to log the event to the specified logging destinations when the queue exceeds the maximum load. When the RPC threshold notification feature is enabled (default value), Symantec Protection Engine takes the following actions: • Logs the event to the logging destinations • Rejects the scan request • Notifies the client that the server is too busy to process the request When the RPC threshold notification feature is disabled, Symantec Protection Engine continues to queue all incoming requests after the threshold is exceeded until a thread becomes available. You can configure the threshold for queued requests for Symantec Protection Engine. The client can then adjust the load balancing, which prevents the server from being overloaded with scan requests. **Note:** For logging to occur at maximum load, the logging level for the logging destination must be set to warning or higher.
In-memory file processing	Symantec Protection Engine can decompose and scan the contents of container files in memory, which eliminates the latency imposed by on-disk scanning. This feature can improve performance in environments in which large volumes of container and archive file formats are routinely submitted for scanning. You can limit the resources that are consumed for processing files in memory by specifying the following values: • The maximum RAM to use for the in-memory file system (in megabytes) • The maximum file size that can be stored within the in-memory file system (in megabytes)

Specify File Size Threshold for in-Place Scanning

Note: This parameter is applicable only to the RPC protocol.

Scanning files over the network can cause network congestion. You can choose to scan files in place on the RPC client share to improve overall performance.

The `FilerPerformanceThreshold` parameter in the `filtering.xml` file allows you to specify the file size threshold value below which a file is copied from the RPC client share to the protection engine temporary folder. Therefore, for most of the files to be scanned in place, you must enter a threshold value that is lower than the average file size in your environment. The `FilerPerformanceThreshold` parameter accepts value in bytes. If you specify the default value (0), all files are copied to the protection engine temporary folder and then scanned.

Table 28 presents the settings for the `FilerPerformanceThreshold` parameter.

Table 28) `FilerPerformanceThreshold` parameter settings.

XPath	Field Values	XML File

`filtering/Container/ FilerPerformance Threshold/ @value`	Integer 0 or greater
	
	Default: 0
		`filtering.xml`
		
		Example:
		`./xmlmodifier –s //Container/FilerPerformanceThreshold/@value <value in bytes> filtering.xml`

Enhance Performance by Limiting Scanning

You can limit the files that Symantec Protection Engine scans to enhance scanning performance. Table 29 explains how you can limit the files that are scanned.

Note: For more information, see Enhance Performance by Limiting Scanning and Excluding Files from Scanning.

Table 29) Performance enhancement options.

Option	Description
Exclude specific file extensions and file types from scanning.	When you enable this option, Symantec Protection Engine scans only the file extensions or the file types that are not in the exclusion lists. The default file exclusion lists contain the most common file extensions and types that are unlikely to contain threats.
Impose limits on container files.	You can impose limits on how Symantec Protection Engine decomposes and scans container files. Imposing limits can conserve scanning resources. You can specify the following limits for handling container files: • The maximum amount of time, in seconds, that is spent decomposing a container file and its contents **Note:** This setting does not apply to .hqx or .amg files. • The maximum file size, in megabytes, for the individual files that are in a container file • The maximum number of nested levels to be decomposed for scanning • The maximum number of bytes that are read when determining whether a file is MIME encoded

Specify File Size Threshold for Scanning Exclusion

You can use the `FileSizeScanThreshold` parameter to specify the file sizes that will be excluded from scanning. Any file whose size is greater than or equal to the specified value is not scanned. This parameter also logs that the file was bypassed from scanning and increments the number of requests by 1. The `FileSizeScanThreshold` parameter accepts values in bytes.

Table 30 presents the settings for the `FileSizeScanThreshold` parameter.

Table 30) Maximum value to exclude files from scanning.

XPath	Field Values	XML File
`filtering/FileAttribute/ FileSizeScanThreshold/@value`	Integer 0 or greater Default: 0	`filtering.xml`

Set Container File Limits

Symantec Protection Engine protects your network from file attachments that can overload the system, consume scanning performance, and degrade performance. This protection includes container files that have any of the following characteristics:

- Files that are overly large
- Files that contain large numbers of embedded, compressed files
- Files that are designed to maliciously use resources and degrade performance

To enhance scanning performance and reduce your exposure to denial-of-service attacks, you can impose limits to control how Symantec Protection Engine handles container files. You can specify the following limits:

- The maximum amount of time, in seconds, that is spent decomposing a container file and its contents

  Note: This setting does not apply to .hqx or .amg files.
- The maximum file size, in megabytes, for the individual files that are in a container file
- The maximum number of nested levels to be decomposed for scanning
- The maximum number of bytes that are read when determining whether a file is MIME encoded

Symantec Protection Engine scans a file and its contents until it reaches the maximum depth that you specify. Symantec Protection Engine stops scanning any file that meets the maximum file size limit or that exceeds the maximum amount of time to decompose. It then generates a log entry and resumes scanning any remaining files. This process continues until Symantec Protection Engine scans all of the files that do not meet any of the processing limits to the maximum depth.

You can specify whether to allow or deny access to files for which an established limit is met or exceeded. Access is denied by default.

Note: If you allow access to a file that has not been fully scanned, you can expose your network to risks. If you allow access and Symantec Protection Engine detects a risk, it does not repair the file, even if under normal circumstances the file can be repaired. In this case, the file is handled as though it is unrepairable.

To set container file limits, complete the following steps:

1. In the console, on the primary navigation bar, click Policies.
2. In the sidebar under Views, click Filtering.
3. Locate the content area in the Container Handling tab, under Container File Processing Limits.
4. In the Time to Extract File Meets or Exceeds box, type the maximum time that Symantec Protection Engine can spend extracting a single container file:
   - The default setting is 180 seconds (3 minutes).
   - To disable this setting (so that no limit is imposed), type `0`.
5. In the Maximum Extract Size of File Meets or Exceeds box, type the maximum file size, in megabytes, for individual files in a container file:

- The maximum value that you can specify for individual files in .tar, .rar, and .zip containers is 30719MB (~30GB).
- The maximum value that you can specify for other containers is 1907MB (~2GB).
- The default setting is 100MB.
- To disable this setting so that no limit is imposed, type `0`.

6. In the Maximum Extract Depth of File Meets or Exceeds box, type the maximum number of nested levels of files that are decomposed within a container file:
   - The default setting is 10 levels.
   - The maximum value for this setting is 50.
7. Under When Processor Limit Is Met (or Exceeded), select whether to allow or deny access to container files for which one or more limits are exceeded. Access is denied by default.
8. Under NonMIME Threshold, in the No Determination After Reading box, type the maximum number of bytes that Symantec Protection Engine should scan to determine whether a file is MIME encoded. The default setting is 200,000 bytes.

   Note: If Symantec Protection Engine reads the maximum number of bytes and cannot determine whether the file is MIME encoded, the file is considered to be non-MIME encoded.
9. On the toolbar, click one of the following options:
   - Click Save to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
10. Click Apply to apply your changes. Your changes are not implemented until you apply them.

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.