Technical Report

Sophos Anti-Virus Protection for Data ONTAP Operating in Cluster-Mode

Manoj Kumar D V, Dhaval Bhadeshiya, NetApp

April 2012 | TR-3985

Executive Summary

Antivirus scanning is an integral feature for file services deployments. NetApp provides this functionality to its customers by partnering with premium antivirus product vendors. With on-board antivirus protection, storage administrators can configure the virus scanning mechanism and storage from one unified NetApp® interface. This document discusses the scanning configurations for Sophos® Anti-Virus for NetApp systems with NetApp Data ONTAP® operating in Cluster-Mode. It also discusses the best practices for deploying this solution.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

NetApp storage devices include integrated antivirus (AV) functionality in partnership with Sophos to protect corporate data from computer viruses. The combined solutions are designed to detect and prevent the spread of malicious virus code before data is compromised.

NetApp offers two solutions for protecting data:

- **Off-box antivirus.** NetApp storage devices offload the antivirus scanning activity to antivirus servers for maximum scalability. This solution is available for Data ONTAP 7.x and Data ONTAP 8.x operating in 7-Mode. For more information about off-box AV, refer to TR-3107: Antivirus Scanning Best Practices Guide.
- **On-board antivirus.** This solution enables an integrated approach to secure data. The Sophos Anti-Virus engine is bundled with Data ONTAP and can run on the storage controller. This solution is available starting with Data ONTAP 8.1.x operating in Cluster-Mode.

This report describes the Sophos Anti-Virus for NetApp Data ONTAP 8.1 operating in Cluster-Mode and the best practices for deploying this solution.

1.1 Overview of Sophos Anti-Virus for NetApp

Sophos Anti-Virus provides integrated virus protection for Data ONTAP operating in Cluster-Mode. The AV scanning engine from Sophos runs on NetApp storage systems. This solution offers two options to protect data:

- **On-access.** The scanning process occurs every time clients access the files. The files are scanned for any threat before they are served to clients.
- **On-demand.** This option scans the file system at the scheduled time. AV scanning can be configured to meet the customer’s scanning needs by scheduling antivirus scans during off-peak hours.

Unlike most off-box antivirus solutions that are for CIFS only, Sophos Anti-Virus scans both CIFS and NFS file access for threats. The Sophos Anti-Virus scan engine runs in the user space that is available in Cluster-Mode.

AV scanning is a cluster-wide feature and it is not associated with any Vserver. Using AV policies, scanning polices can be applied per volume.

1.2 On-Board Antivirus Solution Benefits

On-board AV protects customers’ data stored on NetApp storage systems from viruses. This feature improves the robustness, performance, and scalability of the antivirus solution while simplifying manageability. It removes the network between the NetApp storage controllers and the antivirus servers, bringing the antivirus servers closer to the data. Here are some of the benefits of using on-board AV:

- **Better management.** No external server is required to perform virus scanning. By removing the external antivirus server, the management of the antivirus feature is concentrated in one place—on the storage management interface.
- **Better scalability.** In Cluster-Mode, scalability is a key design consideration. The AV solution takes advantage of the Cluster-Mode architecture that provides the ability to scale.
- **Scheduled scanning.** Virus scanning can be performed during off-peak hours by using the on-demand scanning feature.
- **Improved performance.**
  - The on-board antivirus design allows the antivirus engines to directly access the data by using a fast native storage controller protocol. This reduces the overhead seen in traditional off-box antivirus solutions that use CIFS protocol for data access. It can also help in improving performance by reducing the network traffic and eliminating data copies.

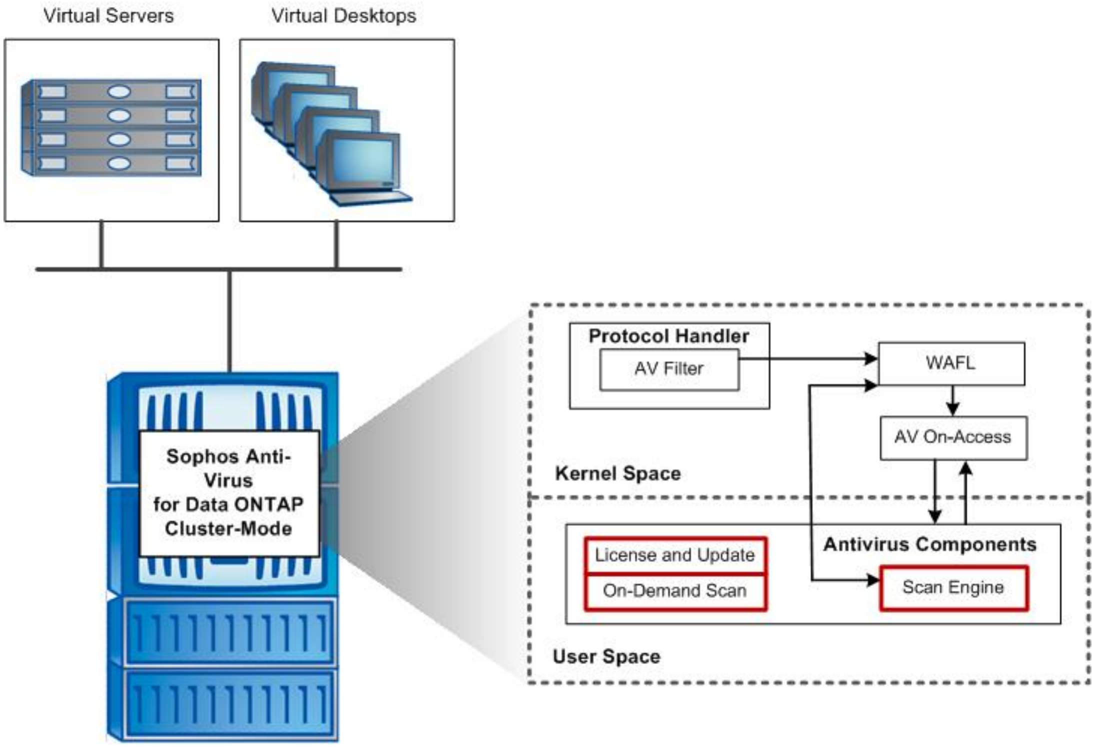
  - The scanned file information is persistent. This eliminates load during on-access scanning because only modified files are scanned.
- **Security.** Supports both CIFS and NFS file access scanning.
- **Scanning options**.
  - Centralized configuration of AV from console and UI.
  - Different on-access policies can be set for different volumes.
  - Using the privileged mode, it is possible to change various engine options like the archive recursion depth, scan timeout, and so on.

2 Sophos Anti-Virus for NetApp Architecture

The Sophos Anti-Virus solution is integrated into the Data ONTAP operating system. Data ONTAP operating in Cluster-Mode is designed to provide space for applications such as antivirus servers. Sophos Anti-Virus uses this user space to run its scan engine.

Figure 1 is a high-level overview of the Sophos Anti-Virus for NetApp architecture.

Figure 1) Sophos Anti-Virus for NetApp architecture overview.



Note: Figure 1 shows the Sophos main on-board antivirus components in a single-node Cluster-Mode setup. Multiple-node interactions are beyond the scope of this document.

The Sophos Anti-Virus solution consists of hooks in the data path to delay file operations and generate scan requests, and a user-mode application that mediates scan and management requests with a third-party scanning engine. The main components of this architecture are:

- **AV filter.** When a file is accessed by using the network protocols, the AV filter first decides whether or not the file needs to be scanned. This predecision is based on information like file extension, the share through which the request is coming, the protocol used, and so on. This information is passed to the AV on-access client.

- **AV on-access client.** A module used by NetApp WAFL® (Write Anywhere File Layout) to manage virus scanning. Based on the predecision passed by the AV filter and the AV attributes of the inode, the AV on-access client decides whether or not to scan the file. To scan a file, the AV client sends a request to the AV server.
- **AV server.** Located in the user space, the AV server contains the third-party scan engine. Upon request of the AV on-access and on-demand clients, the AV server scans the file. A maximum of one AV server can be present per node.
- **AV on demand.** Parses directories upon an administrator's request and scans the files by sending a request to the AV server.
- **AV manager.** Used to configure and monitor the antivirus feature and to manage the AV subsystems.

On-access scanning is based on the AV policy defined for the volume. The AV policy can be assigned either to a Vserver or to a volume. A volume inherits the AV policy from the Vserver if there is no explicit policy assigned to it.

The AV policy can be used to determine scanning options based on common questions such as:

- Is scanning mandatory even when the AV server is down?
- What protocols should be scanned?
- For CIFS:
  - What shares should be scanned?
  - What files should be scanned?
  - Scan only files that are opened with execute access?
- For NFS:
  - Scan only files that are opened with execute permission?
- What file operations should be scanned (FileOp profile)?

The actual scan depends on the protocol and file operations. Sophos Anti-Virus now supports both CIFS and NFS protocols, but the file operations differ for each protocol. To simplify administration and optimize performance, inbuilt file operations profiles are created that define which files operations to scan and the priority for each protocol.

Table 1 presents the four possible file access profiles, as well as the scan action that should be taken for each incoming file operation.

Table 1) File access profiles.

FileOP profile / Protocol	CIFS, NFSv4 only	NFSv2, v3 only	Multiprotocol Strict	Multiprotocol Standard
CIFS, NFSv4				
Open	Scan, block	N/A	Scan	Scan, block
Read	No scan	N/A	Scan	Scan
Write	No scan	N/A	Scan	No scan
Close	Scan	N/A	Scan	Scan
Rename	Scan	N/A	Scan	Scan
NFSv2, v3				
Read	N/A	Scan, block	Scan, block	Scan, block
Write	N/A	Scan	Scan	No scan
Rename	N/A	No scan	Scan	Scan

The scan action in Table 1 contains the following parameters that determine the scanning behavior:

- **Scan/no scan.** Specifies whether or not to scan a file.
- **Block.** True if the AV on-access client needs to wait for scan completion before completing the file operation.

Once the files are scanned, scanned information like scan result and the AV version used for scanning the file is stored. The file scan state can be:

- Unknown
- Clean
- Infected

File scan state is reset to "unknown" when the file is modified or when the AV version is updated. The files are scanned only when the state is "unknown" or the scanned AV version is different from the current AV version.

On-demand scanning can be used to scan a file, directory, Vserver, or cluster. Scanning can be triggered manually or by a predefined schedule. On-demand offers many options to suit each customer's needs. For more information about this feature, see section 5, "On-Demand Scanning."

3 Installing and Updating Sophos Anti-Virus

The section describes how to install and administer Sophos Anti-Virus for NetApp.

3.1 Installing the Engine

Prerequisites for Installing the Engine

- Disable the engine before the initial configuration.
- Configure DNS for the cluster to access the Internet to download the required files from partner sites.
- Verify that you have the Sophos for Network Storage license. Most Endpoint Protection licenses include this license. Contact your Sophos account manager or partner if you are unsure.

Sophos Installation

To install the Sophos Anti-Virus scan engine, perform the following steps:

1. Configure the Sophos Anti-Virus engine:

```
antivirus engine modify -vendor sophos -num-license 1 -sophos-http-url SOPHOS -sophos-http-user
<username>
Please enter password: <password>
Please enter password again: <password>
```

   Note: If the engine is currently disabled, the activation code will be activated and license information will be updated when the engine is enabled.

   Note: Set the number of licenses to the number of nodes in the cluster.

2. Check the configuration:

```
antivirus engine show

Antivirus Vendor        : sophos
State                   : off
Runtime State           : Disabled.
Product Information     : Sophos Anti-Virus for Data ONTAP
Number of Licenses      : 1
URL                     : SOPHOS
User                    : <username>
```

3. Enable the AV engine:

```
antivirus engine enable
```

4. Modify the engine configuration.

   Options such as update URL, license URL, number of licenses, and so on can be modified by using the CLI.

5. Install the AV engine by using the proxy configuration.

   If nodes are not connected to the Internet, the installation and virus definition update can be done by using the proxy configuration. To configure proxy for the antivirus engine, use the privilege mode by entering:

```
Set diagnostic
```

   This will take you to the privilege mode. Enter:

```
antivirus engine option modify -proxy-host <hostname> -proxy-port <port number> -proxy-login
<username>
Please enter password: <password>
```

3.2 Enabling Automatic Updates

Updates are run as a job based on the schedule defined by the administrator. The update operation downloads the antivirus software updates, such as virus definition files, scan engine libraries, virus pattern files, and so on, from Sophos update sites to the cluster. Updates are stored in a common repository shared among all nodes in a cluster. After downloading the updates, the cluster sends an update request to all the antivirus server instances to request that antivirus software definitions be updated.

Only one antivirus update job can run at any time in the cluster. The automatic update options and the commands to enable them are described below.

Enable Automatic Update

```
antivirus update modify -auto-update on
```

By default, updates are scheduled at 2 a.m. every day.

Set Timed Update

To schedule the update, you must update the `modify` command with the appropriate options. The following sample of the command shows how to set the virus definition update at 2 a.m. on Saturday and Sunday.

```
antivirus update modify -auto-update on -schedule-hour 2 -schedule-minute 0 -schedule-dayofweek
saturday,sunday
```

Perform Manual Update

To perform a one-time manual update, use the following command:

```
antivirus update sync
[Job 236] Job succeeded: There are no updates.
```

Update Rollback

AV update provides an option to roll back changes made by the last update. Use this option to revert changes if there are problems after the update.

```
antivirus update rollback
```

Disable Automatic Update

```
antivirus update modify -auto-update off
```

4 On-Access Scanning

The on-access policy defines the scanning rules when data is accessed over either CIFS or NFS. Each volume is associated with an on-access scanning policy. If no specific scanning policy is assigned to a volume, it inherits the policy of the Vserver.

This section describes the creating, assigning, and modifying of on-access policies.

4.1 Scan Policy

Default Scan Policy

```
antivirus on-access policy show default

                        Scan      Mandatory  Scan          Fileop
Name         Scan       RO vol    scan       protocols     profile
------------ ---------- --------- ---------- ------------- ---------
default      off        off       on         cifs, nfs4    multi_proto_standard
  CIFS
    Shares include list    : ^.*$
    Files include list     : ^.*$
    Only scan files opened with execute access     : off
  NFS
    Only scan files with execute permission        : off
```

Create a New Scan Policy

```
antivirus on-access policy create -name cifs_nfs4 -scan on  -scan-mandatory on -protocols
cifs,nfs4 -cifs-share include -cifs-share-list "^.*$" -cifs-scan-execute-access on -cifs-file
include -cifs-file-list "^.*$" -nfs-scan-execute-permission on -fileop-profile multi_proto_strict
```

Modify an On-Access Policy

```
antivirus on-access policy modify -name cifs_nfs4 -nfs-scan-execute-permission off
```

Delete an On-Access Policy

```
antivirus on-access policy delete -name cifs_nfs4
Assigning vscan policies to vservers/volumes
Assigning on-access policy for vserver
antivirus on-access modify -vserver vwfs1 -volume * -vserver-policy cifs_nfs4
```

Assign an On-Access Policy for Volumes

```
antivirus on-access modify -vserver vwfs1 -volume vol1 -volume-policy default
antivirus on-access show -vserver vwfs1

Vserver               Volume                On-Access Policy
--------------------  --------------------  --------------------
vwfs1                 -                     cifs_nfs4
                      root_vol              test1
                      test1                 cifs_nfs4
                      vol1                  default
3 entries were displayed.
```

5 On-Demand Scanning

Antivirus on-demand scanning can be used to perform virus scans on a schedule based on your requirements. The on-demand scan commands are created by the user and can scan one file or the entire cluster file system as required. They can be run manually or on a schedule. On-demand scanning generates a report upon completion.

5.1 AV On-Demand Scan Configuration

The following commands can be used to scan a file, directory, or Vserver:

- `scan -file <Vserver> <filename> [-force]`
- `scan -dir < Vserver > <pathname>  [-force] [-dont-cross-junctions][-dont-recurse] [-files {include|exclude} <list>]`
- `scan -vserver < Vserver > [-force] [-dont-cross-junctions] [-dont-recurse][-files {include|exclude} <list>] [-directories  {include|exclude} <list>]`
- `scan -cluster [-force] [-dont-cross-junctions] [-dont-recurse] [-files {include|exclude} <list>][-directories {include|exclude} <list>][-vservers {include|exclude} <list>]`

Where:

`vserver` : The Vserver where the file resides.

`filename` : Full path and name of the file to be scanned.

`-force`: : Forces the file to be scanned even if it was scanned previously.

`pathname`: : Full path of the directory to scan.

`-dont-cross-junctions` : Disables the crossing of volume junctions.

`-dont-recurse` : Disables recursion through subdirectories.

`-files` : List of files to be scanned. The default is to include all files. This option is case insensitive.
For example: `^.*\.(doc|xls|ppt|exe)$`

`-directories` : List of directories to be scanned; the default is to include all directories.

`-vservers` : List of Vservers to be scanned; the default is to include all Vservers.

Examples:

- To scan a file:

```
antivirus on-demand command create -name scanfile -command-line “scan -file vwfs1
/vol1/testSymLink”
```

- To scan a directory:

```
antivirus on-demand command create -name scandir -command-line "scan -dir vwfs1 /vol/vol1/xp"
```

- To scan a Vserver:

```
antivirus on-demand command create -name scanvserver -command-line "scan -vserver vwfs1 -force"
```

- Display on-demand commands:

```
antivirus on-demand command show

Name                  Command Line
--------------------  --------------------------------------
scandir               scan -dir vwfs1 /vol/vol1/xp
scanfile              scan -file vwfs1 /vol1/testSymLink
scanvserver           scan -vserver vwfs1 -force
3 entries were displayed.
```

- Execute an on-demand command:

```
antivirus on-demand run –command scanvserver
```

- View AV on-demand reports:

```
antivirus on-demand report show
antivirun on-demand report print –id <id of report>
```

Example:

```
antivirus on-demand report print -id 4

scan -dir vwfs1 /vol/vol1/xp
BEGIN: Wed Apr 27 17:10:20 2011

Files that have been found infected, or that couldn't be scanned:
-----------------------------------------------------------------

Statistics:
-----------
 Number of scans attempted  : 4
 Number of scans succeeded  : 4
 Number of scans failed     : 0
 Number of remedies failed  : 0
 Number of scans retried    : 0
 Number of files infected   : 0
 Number of files repaired   : 0
 Number of files deleted    : 0
 Number of files quarantined: 0
 Scan Duration              : 00:04:59

 END: Wed Apr 27 17:15:19 2011scan -cluster
```

- On-demand scan schedule

```
Schedule options
```

```
5min           @:00,:05,:10,:15,:20,:25,:30,:35,:40,:45,:50,:55
8hour                       @2:15,10:15,18:15
avUpdateSchedule            Sun,Sat@2:00
daily                       @0:10
hourly                      @:05
weekly                      Sun@0:15
```

Example:

```
antivirus on-demand> schedule -command scanvserver -schedule avUpdateSchedule
```

5.2 AV On-Demand Scan Limitations

Currently AV on demand has the following limitations and known issues:

- Symlinks and widelinks cannot be scanned due to an internal file system limitation.
- If the same command is run at intervals of less than 5 minutes, the following error occurs:

```
antivirus on-demand run ScanSymLink

ERROR: command failed: Failed to queue anti-virus on-demand scan job (command'ScanSymLink',
schedule ); reason: 'failed to queue job - status 6 (Exists).'
```

To retry the scan, wait for 5 minutes before repeating the scan; or create a new command with the same requirements but a different name.

6 Remedy

Remedy determines the actions to be taken when a file is found to be infected with a virus during scanning. The remedy action can be one of the following:

- **Repair.** The scan engine tries to clean or repair the infected file.
- **None.** Takes no action.
- **Delete.** Deletes the infected file.
- **Quarantine.** Moves the infected file to a quarantine directory; or a file extension is added to the name of the infected file. The quarantine action is specified in the configuration.

6.1 Configure Remedy Options

To configure remedy options, enter:

```
antivirus remedy modify

Usage:
[-action] {none|repair|delete|quarantine}           Action
[[-failed-repair-action] {none|delete|quarantine}]  Failed Repair Action
[ -quarantine-action {move|add_extension} ]         Quarantine Action
[ -quarantine-ext <text> ]                          File Extension
[ -quarantine-dir <text> ]                          Quarantine Directory
```

6.2 Remedy Action

When a virus is found, the following remedy actions can be taken:

- **None.** Takes no action.
- **Repair.** The scan engine tries to clean or repair the infected file.
- **Failed repair action.** If the repair action fails, you can define the following action to protect the infected file:
  - **None.** Takes no action.

- **Delete.** Deletes the infected file.
- **Quarantine.** Takes the action specified in the `-quarantine-action` field.

The `-quarantine-action` field is used only when the action is set to Repair.

- **Delete.** Deletes the infected file.
- **Quarantine.** Takes the action specified in the `-quarantine-action` field.
- **Quarantine action.** The following two quarantine options are supported:
  - **Move.** Moves the infected file to the directory specified by `–quarantine-dir`.

```
antivirus remedy modify -action quarantine -quarantine-action move -quarantine-dir
/infected_files
antivirus remedy show

Action               : quarantine
Quarantine Action    : move
Quarantine Directory : /infected_files
```

  - **add_extension.** An extension (as specified in `–quarantine-ext`) is added to the infected file.

```
antivirus remedy modify -action quarantine -quarantine-action add_extension -quarantine-ext vir
antivirus remedy show

Action               : quarantine
Quarantine Action    : add_extension
Quarantine Extension : vir
```

For example, if the file `abc.txt` is infected, it is renamed to `abc.txt.vir`.

7 Debugging and Troubleshooting

7.1 Antivirus Statistics

On-Access Scan Statistics

On-access scan-related information is available through AV on-access statistics. This information is useful to understand the number of files scanned, the average number of bytes scanned per file, and so on. To check the statistics of AV on-access scanning, run the following command:

```
statistics show -object avoa

Node: OBAV-01
    Object.Instance.Counter                         Value         Delta
    --------------------------------------- ------------- -------------
    avoa.avoa.instance_name                          avoa
             -
    avoa.avoa.node_name                                 -             -
    avoa.avoa.ScanReqReceived                           0             -
    avoa.avoa.ScanReqSent                               0             -
    avoa.avoa.ObjScanned                                0             -
    avoa.avoa.BytesScanned                             0B             -

Node: OBAV-02
    Object.Instance.Counter                         Value         Delta
    -------------------------------------------- ------------- --------
    avoa.avoa.instance_name                          avoa
             -
    avoa.avoa.node_name                                 -             -
    avoa.avoa.ScanReqReceived                           0             -
    avoa.avoa.ScanReqSent                               0             -
    avoa.avoa.ObjScanned                                0             -
    avoa.avoa.BytesScanned                             0B             -
12 entries were displayed.
```

To get details of the on-access statistics, run the same command in diagnostics privilege mode.

AV Server Statistics

To generate antivirus server statistics, run the following command:

```
antivirus statistics -module avs
```

The statistics are generated and added to the `/mroot/etc/messages.log` file.

7.2 Debugging

Antivirus notifications and debug information are logged in the event log and other log files, such as `/mroot/etc/mlog/messages.log`.

To check messages in the event log, use the following command:

```
event log show -messagename  av*
```

Installation and Update Logs

For details on update and license manager errors, check `mum_log` and `mlm_log`.

Trace Level

The default antivirus server, on demand, and update log level are set to “notice.” To get more debug information for these modules, set the log level to “debug” by using the following command in diagnostics privilege mode:

```
antivirus options modify -avod-log-level debug -update-log-level debug
```

8 Common Problems

This section covers some common errors that might occur when using Sophos Anti-Virus and their possible resolution.

8.1 Download Errors

Invalid URL

Error

```
ERROR: command failed: [Job 63] Job failed: Sophos job failed, error: '144, server or proxy -
invalid URL
```

Resolution

Check that DNS is enabled on the system and that it is connected to the Internet. Check that the URLs entered for “URL for Intel 32” and “URL for AMD 64” are both valid.

Invalid Username/Password

Error

```
ERROR: command failed: [Job 64] Job failed: Sophos job failed, error: '146, invalid server
credentials'
```

Resolution

Verify the username and password and retry the command.

Corrupted Download

Error

```
ERROR: command failed: [Job 64] Job failed: Sophos job failed, error: '148, SDDM integrity check
failed'
```

Resolution

The download is corrupted. Try again. If it fails again, contact Sophos.

8.2 Generic Errors

File is Not Scanned

Resolution: Make sure that the file is not a symlink. Symlinks cannot be scanned due to file system limitations.

Scan Takes too Long

Resolution: If the scan is taking too long, use job manager to confirm that the job is running properly:

```
job watch-progress <avod job id>
```

The output should indicate that the files are being scanned. If the same file is shown for several minutes and that file is not very large, then the scan may be having problems. Check the avod and avs event logs to see if there are any problems. If there are timeouts in the AVOD event log, abort the job, disable and then reenable the AV engine, and retry the job.

Scan Times Out on Large Files

Resolution: The scan timeout is set for 30 minutes by default. If the scan times out, for example due to large zip files, increase the AV on-demand timeout:

```
antivirus options modify -avod-scan-timeout <number of seconds>
```

Error: “Failed to queue job - status 6 (Exists)” When Trying to Run a Job

Resolution: Two AV on-demand jobs cannot run simultaneously. Wait for the previous job to finish before retrying the job. If the command is not running but you still get this error message, wait for 5 minutes before repeating the command. This is a job manager limitation.

Error: “No AV servers are running on this cluster”

Resolution: This error message indicates that all AV servers on the cluster are down. Refer to the vendor’s troubleshooting guide for information about how to restart the AV servers. Before restarting the servers, collect the logs for debugging purposes.

9 Best Practices for Antivirus Scanning

- Set up on-demand scanning to scan files on a regular basis during off-peak hours.
- To maximize protection, set up automatic antivirus updates.
- To maximize performance, select “Scan only executable files.”
- Don’t assign AV policies to NetApp FlexCache® volumes; that would increase latency. Instead, define AV policies at the source.
- Exclude files that change frequently and cannot be scanned (for example, database files). Although the Sophos Anti-Virus engine rapidly confirms that these files don’t need scanning, it adds an overhead to every read and/or write operation

10 Summary

Integrated antivirus solutions for NetApp storage devices enable enterprises to protect their valuable data from viruses. Customers can deploy NetApp solutions enterprise-wide with best-in-class Sophos Anti-Virus solutions to protect data. The open, scalable, and high-performance architecture enhances the customer’s experience.

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

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

Go further, faster®

NetApp®

www.netapp.com