Technical Report

Antivirus Scanning Best Practices Guide

Manoj Kumar D V, Brahmanna Chowdary Kodavali, NetApp
April 2011 | TR-3107

NETAPP ANTIVIRUS SCANNING

Antivirus scanning is a must-have feature in Windows® File Services deployments. NetApp provides this functionality to its customers by partnering with various premium antivirus product vendors. The administrator can control the behavior of the virus scanning mechanism from the NetApp® interface as well as the AV software interface. To obtain maximum protection for the files stored in NetApp storage systems with minimal impact on performance, there are certain best practices to be followed. This document discusses these from the NetApp virus scanning architecture to some of 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 to protect corporate data from computer viruses. The combined solutions are designed to detect and prevent the spreading of malicious virus code before data is compromised.

The antivirus architecture for NetApp storage devices is designed to protect data accessed by Windows software-based clients or other clients that access data using the Common Internet File System (CIFS) protocol.

NetApp storage devices offload the antivirus scanning activity to antivirus servers for maximum scalability and performance. Best-in-class antivirus solutions are available from Computer Associates (CA), McAfee, Sophos, Symantec, and Trend Micro. These complementary solutions augment the existing antivirus infrastructures companies are using and deploying today.

This report describes the integrated antivirus architectures for NetApp storage devices and the best practices for deploying these solutions.

1.1 NETAPP ANTIVIRUS SOLUTION OVERVIEW

There are two common approaches to scanning data and Internet content:

- Scan internal data files and Internet content for viruses at scheduled intervals
- Scan files on the fly as they are read, created, or modified

The latter of the two approaches is more effective at detecting viruses before they are able compromise data. Moreover, the scanning process occurs on an as-needed basis and thus minimizes the server and network loads observed during intensive file system scans.

Integrated antivirus solutions for NetApp storage devices help protect against malicious virus code by scanning files on access and during the download process.

The NetApp antivirus solution uses an authenticated CIFS connection and RPCs to communicate with the antivirus scanning servers. CIFS is an industry-standard protocol with features best suited for the applications. CIFS provides a secure, authenticated connection and supports byte-range reads. The ability to perform byte-range reads streamlines the scanning process, resulting in quicker file access.

2 NETAPP ANTIVIRUS SCANNING

Prior to release of the integrated antivirus functionality for NetApp storage devices in December 2000, NetApp customers long enjoyed the ability to quickly recover from virus incidents using the built-in Snapshot® technology inherent to the NetApp WAFL® file system. In the event of a virus incident, users can recover files out of their read-only "~snapshot" folders in minutes. Viruses cannot infect files in Snapshot copies because Snapshot copies and data are read-only. As Snapshot activities are commonly scheduled in weekly, daily, and hourly intervals, backups are automatic, and the drag-and-drop recovery is immediate and simple.

To detect and stop viruses before they reach the file system, NetApp integrates the antivirus functionality into the NetApp storage device's microkernel, Data ONTAP®. NetApp integrated antivirus software (from Computer Associates, McAfee, Sophos, Symantec, and Trend Micro) provides additional protection against viruses by scanning files accessed by Windows and CIFS/SMB clients. The virus scanning activity is transparent to end users and occurs before the file is committed to disk (write requests) or delivered to the requesting user or application (read requests). From Data ONTAP 7.2 onward this functionality has changed for write requests. The file is committed to disk before scanning completes: that is, there is no waiting time, and it improves the end user experience. In case a virus is found after the write operation, the file will be marked as infected and will not be accessible.

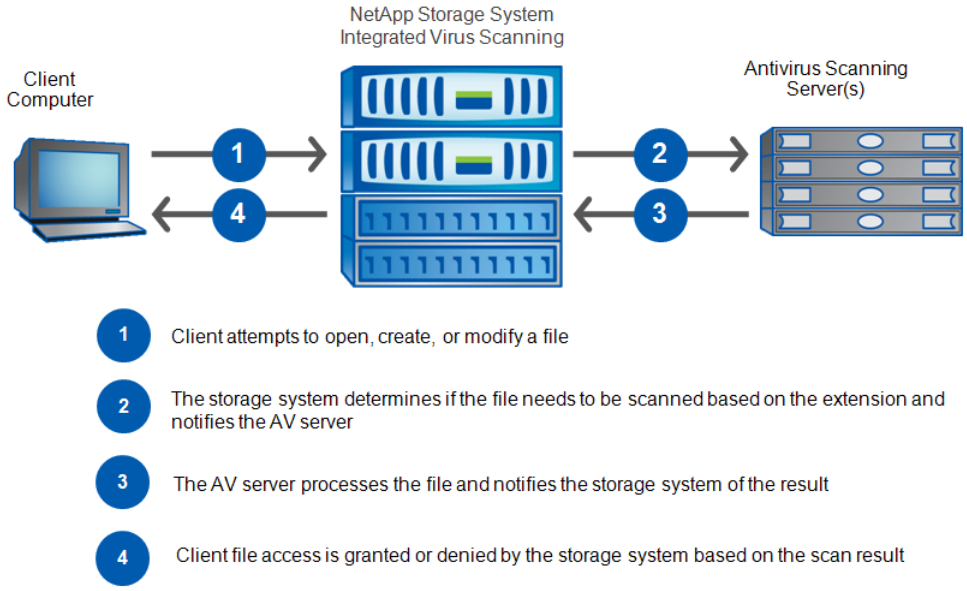
Antivirus scanning servers register with the NetApp storage device using remote procedure calls (RPCs) and a Microsoft® NTLM- or Kerberos-authenticated CIFS connection (depending on the Windows domain, Active Directory, and so on). Multiple antivirus scanning servers can be configured to register with the same NetApp storage device or with multiple NetApp storage devices for redundancy and performance. When multiple antivirus servers are deployed, the NetApp storage devices will automatically distribute scanning activity among them using a round robin load-balancing scheme.

NetApp storage devices will initiate scans (send a scan command to the scanning servers and await a reply) on files that are created, changed, and opened for read access and that meet the following criteria. For more information, see section Defining Scanning Criteria.

- The file extension is included in the list of to-be-scanned file types.
- The file has not already been marked as previously scanned, and no changes have occurred to the file.

Table 1 shows the basic steps that occur during the scanning process.

Figure 1) NetApp storage system integrated virus scanning.



When a user tries to open, create, or change a file that matches the to-be-scanned criteria, such as a .exe file, the NetApp storage device notifies a registered AV server and provides the path of the file to scan. The AV server opens a connection to the file and checks the file for a known virus signature or virus-like behavior. The scanning engine then notifies the NetApp storage device of the results. If no virus is found, the NetApp storage device permits the client to open the requested file. If a virus is found, the antivirus software will either quarantine or disinfect the file by removing the virus. (See the next section for a description of quarantine and virus removal.)

Once files are safely scanned, the NetApp storage device keeps track of recently scanned files in memory. This improves performance by minimizing redundant scanning activity. The scanning process takes a few milliseconds on most files and might take several seconds on more complex files such as .zip or .cab files that might contain many other files.

In any case, the user or application is not permitted to open or rename a file until the virus software has successfully scanned or removed the virus from the file. The antivirus software can also be configured to quarantine files and not allow access until an administrator examines the data and makes a decision.

2.1 WHEN A VIRUS IS FOUND

The action taken on an infected file is not determined by the NetApp storage device. The settings that affect how a virus is handled are determined by the administrator and stored as part of the antivirus software's configuration. If it is determined a file is infected, the virus software will typically take one of three actions: it will clean, quarantine or delete the file. The following table describes the differences.

Table 1) Actions by AV scanner when virus found.

Scanning Configuration	Action
Clean the file	The AV software removes the virus and notifies the NetApp storage device when the file is clean. The NetApp storage device then allows the client to open the requested file.
Quarantine the file	Generally this option selected if the AV scanner is not able to clean the file. The AV scanner quarantines the file or moves it to a special location, and the NetApp storage device denies the client access. The administrator must take action.
Delete the file	This is the other option that is selected if the AV scanner is not able to clean the file. The AV scanner deletes the file, and the NetApp storage device denies the client access.

Note: If the virus software is configured by the administrator to quarantine a suspected file, the user will see an access denied message and will be unable to open or create the requested file. The administrator must then take action to restore a previous version of the file or disinfect the file using antivirus software.

2.2 UPDATING VIRUS DEFINITIONS

Antivirus definitions are databases that contain information used to identify viruses. Antivirus scanning engines are designed to identify specific viruses using the aforementioned definitions and by recognizing characterized behavior. Antivirus software vendors release a new virus definition (database) for their software products when they find new viruses. These vendor-specific database definitions are used by antivirus software to identify known viruses and/or virus-like behavior. When information about a specific virus is included in a virus definition, it is said to be a known virus.

When a new virus definition becomes available, the definition update might occur automatically through the Internet or be installed by an administrator (see note below). In either case, once a new definition is applied, the virus software will notify the NetApp storage device that a new definition exists. The list of previously scanned files is then flushed, and all subsequent file accesses are scanned with the new virus definition. This makes sure that new viruses are properly identified and removed by the virus software.

Note: Behavior and configuration details will vary with each antivirus vendor. For more specific information, read the documentation included with each antivirus software product.

2.3 DEFINING SCANNING CRITERIA

The NetApp storage device may be configured to exclude certain files by their extension so that those files are not scanned. For example, it might not be necessary to scan graphics files such as .jpg or .bmp files because they do not contain executable code. The NetApp storage device will not ask its registered scanning servers to scan any files that are on the excluded list.

Antivirus software vendors suggest scanning all executable files or files that contain executable code. There are many types of executable files. For example, binary executable files have the .exe and .com extensions. There are also executable scripts such as the .vbs (Visual Basic) and .bat (batch) files. Dynamic loadable modules are files with the .dll extension that contain executable code used by the Microsoft Windows family of operating systems and applications. Finally, some applications store executable commands in the form of macros within their files or documents.

By default, the following file types are scanned for maximum protection. However, administrators can easily customize the default scanning criteria if they want to include or exclude specific types of files.

Table 2) Default extensions list as in Data ONTAP 7.3.1.

List of Extensions to Scan									
001	002	386	3GR	??_	ACE	ACM	ADE	ADP	ADT
AP?	ARC	ARJ	ASA	ASD	ASP	AX?	B64	BA?	BIN
BMP	BO?	BZ?	CAB	CC?	CDR	CDX	CEO	CGI	CHM
CL?	CMD	CNV	CO?	CPL	CPT	CPY	CRT	CSC	CSS
CSV	D?B	DAT	DEV	DIF	DL?	DO?	DOC	DOT	DQY
DRV	EE?	EFV	EML	EX?	EXE	FDF	FMT	FO?	FPH
FPW	GF?	GIM	GIX	GMS	GNA	GW?	GWI	GZ?	HDI
HHT	HLP	HT?	HWD	ICE	ICS	IM?	IN?	IQY	ISP
ITS	JAR	JP?	JS?	LGP	LIB	LNK	LWP	LZH	M3U
MB0	MB1	MB2	MBR	MD?	MHT	MOD	MPD	MPP	MPT
MRC	MS?	MSG	MSO	NAP	NEW	NWS	OB?	OC?	OFT
OL?	OLE	OTM	OV?	PCD	PCI	PD?	PDF	PF?	PHP
PI?	PLG	POT	PP?	PPZ	PRC	PWZ	QLB	QPW	QQY
QTC	RAR	REG	RMF	RQY	RTF	SCR	SCT	SH?	SIS
SKV	SLK	SMM	SPL	SRF	SWF	SYS	TAR	TAZ	TBZ
TD0	TFT	TGZ	TLB	TSP	UNP	URL	UUU	VB?	VBS
VS?	VVV	VWP	VXD	WBK	WIZ	WMV	WP?	WRI	WRL
WRZ	WS?	X32	XL?	XML	XRF	XSL	XTP	XX?	Z0M
Z??	ZI?	ZIP	ZL?	ZZZ					

Examples

The following example commands may be used to add or remove extensions from the list of files to scan on the include list.

To add extensions to the include list:

```
NetApp> vscan extensions include add txt
```

To remove extensions from the include list:

```
NetApp> vscan extensions include remove jpg, gif
```

The following example commands may be used to exclude extensions from the list of files to scan in the exclude list.

To add extensions to the exclude list:

```
NetApp> vscan extensions exclude add doc
```

To remove extensions from the exclude list:

```
NetApp> vscan extensions exclude remove jpg, gif
```

2.4 PERFORMANCE CONSIDERATIONS

Virus scanning occurs between the client's request for the file and the response from the NetApp storage device. This process results in latency of less than a millisecond to many seconds and is largely dependent on the type of file. However, the amount of I/O between the NetApp storage device and AV server is much smaller in proportion to the data served between the NetApp storage device and its clients. This is because the scanning algorithms often only need to examine a small portion of a file to determine if it is infected.

For example, large .zip or .cab files that contain many other files might require all the contents to be extracted and scanned. Moreover, it takes time to completely remove a virus from an infected file. In most cases only a fraction of a file needs to be scanned, as viruses must attach themselves to easily identified locations within different file types.

There are a number of integral design features designed to maximize performance:

- The on-access architecture eliminates the need to perform time-consuming, resource-intensive scans of entire volumes.
- NetApp storage devices maintain a list of already scanned files to reduce or eliminate redundant scans.
- The scanning algorithms vary by file type and often scan only a small portion of many files.

In any system, scanning for viruses adds processing time. Using the integrated NetApp storage device/AV solutions, the performance difference in most cases is measured in milliseconds (ms). Therefore, the entire scanning process might not be perceivable by most users. During periods of heavy use the difference might be more noticeable (in seconds), particularly if users are opening large .cab or .zip files.

Performance varies according to the file types and the speed of the antivirus server, NetApp storage device, and network. Make sure that the AV environment is compatible with section 2.8, "AV Server

2.5 NETWORK CONNECTIVITY

Network connectivity between the NetApp storage device and the AV server must consist of at least a 100MB Ethernet connection. Gigabit Ethernet (1000MB) networking is highly recommended. Connecting through an Ethernet switch or a crossover/direct connection may be used.

The NetApp storage system and AV server can be directly connected or connected using a private network to achieve a clean network. If connecting through an Ethernet switch, use a dedicated switch or configure a virtual LAN (VLAN) to separate traffic traveling through the switch.

In any case, it is imperative that the network between the NetApp storage device and the AV scanning server is clean and free from other traffic. Contention on the NetApp storage device-AV server segment might hinder scanning activity and consequently the NetApp storage device's ability to respond to clients.

Figures 2 and 3 illustrate the different methods that can be used to provide connectivity between a NetApp storage device and its AV servers.

Note: Each direct connection between a NetApp storage system and its associated AV server(s) will require a dedicated network interface card (NIC) in each computer for each connection. Moreover, the NetApp storage system and AV servers need connectivity to the corporate network for administration purposes and virus definition updates. For V-Series systems, the storage is provided by external third-party array vendors.

Figure 2) Network connectivity with direct connection.

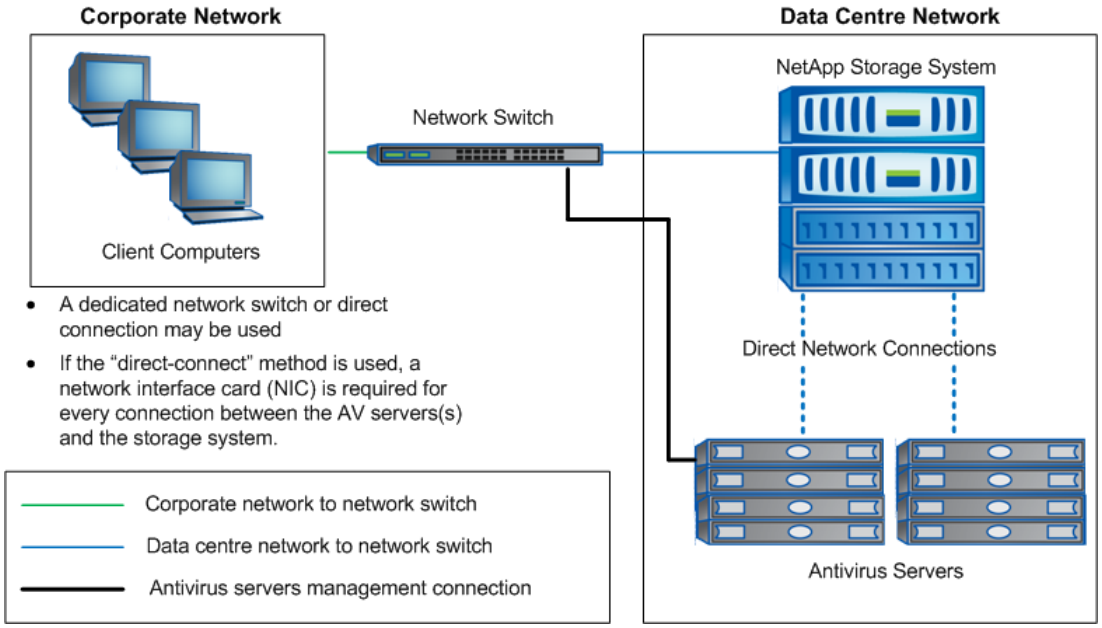
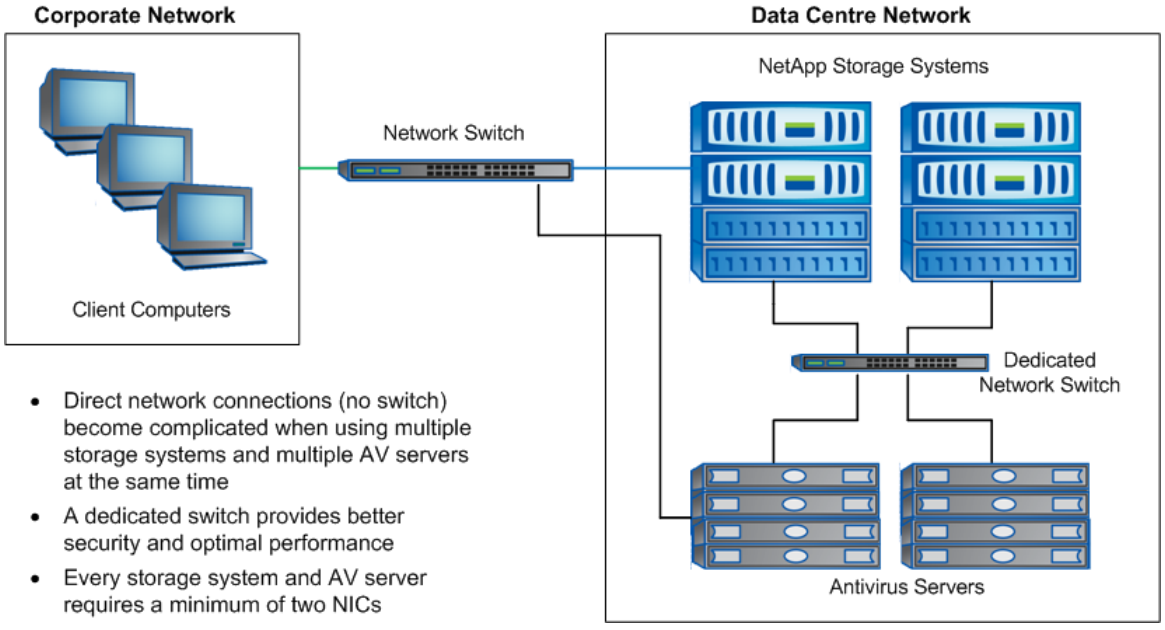


Figure 3) Network connectivity using dedicated switch.



NetApp recommends using a 100/1000Mbps dedicated network. With the latest technology change in network with 10 Gigabit Ethernet, we can have shared connection for client and AV traffic provided we have 1Gbps (approximately 10% of 10GbE) bandwidth available for AV traffic on both NetApp storage and the AV scanning server. Consider the network utilization threshold values while allowing 1Gbps bandwidth for AV traffic.

2.6 NETAPP STORAGE AND AV SERVER AUTHENTICATION

The connection between the NetApp storage device and its AV scanning servers is a trusted connection. There are several mechanisms in place to prevent unauthorized access to the scanning server:

- Scanning servers register using RPC with the NetApp storage device.
- Scanning servers are subject to authentication; the user who manages the scanning server must be a member of the backup operator group on the NetApp storage device.
- The AV server provides file system, console, and login security.

In addition, locating the antivirus servers in a secure data center adjacent to the NetApp storage devices is recommended. Administrators should secure all network equipment and servers from unauthorized physical access.

2.7 USAGE PROFILES

The NetApp storage device model and its capacity are not as important as the way data is used. The number of scans that occur is a direct result of how many different files are opened or changed in a unit of time.

Generally, odds are that a larger capacity NetApp storage device supporting more users will result in more scanning activity. But the total scans per hour do not necessarily scale with the number of users. There is no direct correlation with the NetApp storage device's capacity and the scanning load. The number of scans per hour is a result of how users access and manipulate data. In other words, only users accessing files trigger virus scans.

2.8 AV SERVER HARDWARE

NetApp recommends the following minimum system requirements for each AV server.

Table 3) Antivirus server hardware.

AV Server Hardware Configuration	
CPU speed	2.6GHz (or greater)
RAM	1GB
Hard disk	9GB
Network interface card	100/1000MB Ethernet

There are many inexpensive tower case or 1U rack-mount computers available that are qualified to run Windows NT® or Windows 2000 and the antivirus software. More information on the specific system requirements can be found on the virus software vendors' Web sites.

The limiting performance factors with AV scanners are the CPU frequency and memory bus performance. The amount of vscan requests the AV scanners will be able to process will be greatly dependent on their CPU speed and the memory bus bandwidth. NetApp recommends using AV scanners with the greatest CPU speed available. Also, NetApp recommends two dual-processor servers instead of one quad-processor server. Additionally, this server or servers should not serve many other purposes (for example, no domain controller functionality and so on).

2.9 MULTIPLE AV SERVERS AND MULTIPLE NETAPP STORAGE DEVICES

Though it is not necessary, at least two antivirus servers are recommended for redundancy and higher availability. During normal operation, the NetApp storage devices will automatically load balance between multiple AV servers.

It mostly depends on the file structure how many antivirus servers are needed per NetApp storage device. Each AV vendor is capable of scanning a maximum number of files (usually between 50 and 100 files/second per server). A single NetApp storage device is thus able to overload several AV scanners since it can deliver several hundred files/sec.

2.10 AV SERVER FAILURES

If one or more scanning servers (Windows computers that run the antivirus software) fails or is unavailable, the NetApp storage device will time out the connection to the nonresponsive scanning servers and continue using the remaining scanning servers. The default timeout period is 12 seconds. If no scanning servers are available, the administrator may configure the NetApp storage device in one of two ways:

- Resume file access without virus scanning
- Deny all file access

This behavior is configured with the vscan option mandatory_scan. In all cases the antivirus servers will automatically contact and register themselves with their associated NetApp storage devices when they are back online. Once this occurs, the NetApp storage devices will resume normal operation with virus scanning enabled.

2.11 AV ON-DEMAND SCANNING

We do not have native support for on-demand scanning. However, some AV vendors support scheduled scanning of shares. We can use this feature to achieve on-demand scanning.

On-demand scanning can be done by mounting all shares or volumes (by sharing them) on the AV scanner and creating a schedule to scan selected folders/volumes periodically.

3 APPLICATION SERVERS AND NFS

3.1 APPLICATION SERVERS

Many collaborative mail and database applications such as Microsoft Exchange Server utilize a different type of antivirus product. These antivirus products are run on the application or database server and scan the contents of e-mail attachments and so on being written to the mail database or mail files.

The NetApp on-access solution is designed to scan files accessed by Windows clients. Contact the specific database and/or antivirus vendors for e-mail and database-specific solutions.

3.2 NFS CLIENTS

Data accessed by UNIX® and NFS clients is not supported in this release and will not trigger a virus scan of a requested file. The risk of virus attacks is low for UNIX and NFS data because few viruses are targeted at platforms other than Windows.

However, when NFS and CIFS users access the same storage, the NFS access of a file resets the already set "scanned" flag, so the file will be scanned the next time it is accessed by the CIFS user.

Note: NFS virus scanning support is on the roadmap.

4 ANTIVIRUS PARTNERS

NetApp has partnered with Computer Associates, McAfee, Sophos, Symantec, and Trend Micro to deliver integrated antivirus solutions (see Table 4).

Table 4) Antivirus partner products.

Antivirus Partner	Product Name
Computer Associates	Antivirus for the Enterprise **r8.1**
McAfee	Virus Scan Enterprise for Storage **1.0**
Sophos	Antivirus for NetApp Storage Systems **1.0.1**
Symantec	Antivirus **5.2** for Network Attached Storage
Trend Micro	Server Protect for NetApp Storage Systems **5.62**

Note: The product names given here were accurate at the time when this document was prepared. Contact the respective vendors for specific product information. For the latest information about Data ONTAP support of these products, visit http://now.netapp.com/NOW/knowledge/docs/olio/guides/avmatrix.shtml.

5 BEST PRACTICES FOR ANTIVIRUS SCANNING

Note: The following recommendations are based on the setup NetApp uses in its internal QA lab for testing. It has worked well with heavy loads and with clustered pair configurations. The setup with these recommendations has demonstrated resiliency to failures. In addition, some of the larger NetApp enterprise customers have used these best practices within their environments and have achieved good results.

Best Practices
• Avoid large AV scanning farms with too many NetApp storage devices served by too many AV scanner servers. Instead, choose a pod design, as described in section 5.1. This avoids performance spikes, which might be caused if all NetApp storage devices decide to choose the same AV scanner server at the same time. In this scenario one AV scanner server could become overwhelmed by many NetApp storage devices. • Use an AV scanner server dedicated to antivirus scanning and not used for other jobs such as backup. The reason is that any application running on the machine will share the CPU cycle and memory on the server. This will increase the CPU latency (cycle) for the AV process and will reduce the number of AV requests being processed in any particular time interval. • Connect to the AV scanner server using NetApp storage device IP address and not the NetApp storage device's NetBIOS name to control which NetApp storage device interface is used. • Connect the NetApp storage system and AV scanner using a gigabit network. • For an environment with multiple NetApp storage devices and multiple scanners, make all AV scanners connected with similar high-performing network connections as primary to all the NetApp storage devices. This will improve the performance by load sharing. Refer to Figure 4. • If you have two different data centers in two different locations (local and remote), make all the local AV scanners as primary to all local NetApp storage devices and make those as secondary to all remote NetApp storage devices and vice versa. Also, depending on the amount of vscan requests, some NetApp storage devices (FAS960 or higher: NetApp storage system D) might require additional dedicated scanners that aren't to be shared with other NetApp storage devices as secondary scanners. Refer to Figure 5. • For remote sites/branch offices, it is recommended to use local AV scanners rather than remote AV scanners due to high latency. If cost is a factor, then customers can rely on laptop/PC virus protection for moderate virus protection. They can also schedule periodic complete file system scans by sharing the volumes/qtrees and scanning on them from any system in the remote site. • Setting up vscan timeout values according to the AV software product will result in smoother operation with fewer scanning errors. See the NOW™ knowledge base article KB3378 for more information on timeout values.

Figure 4) Connecting all the scanners as primary inside a data center.

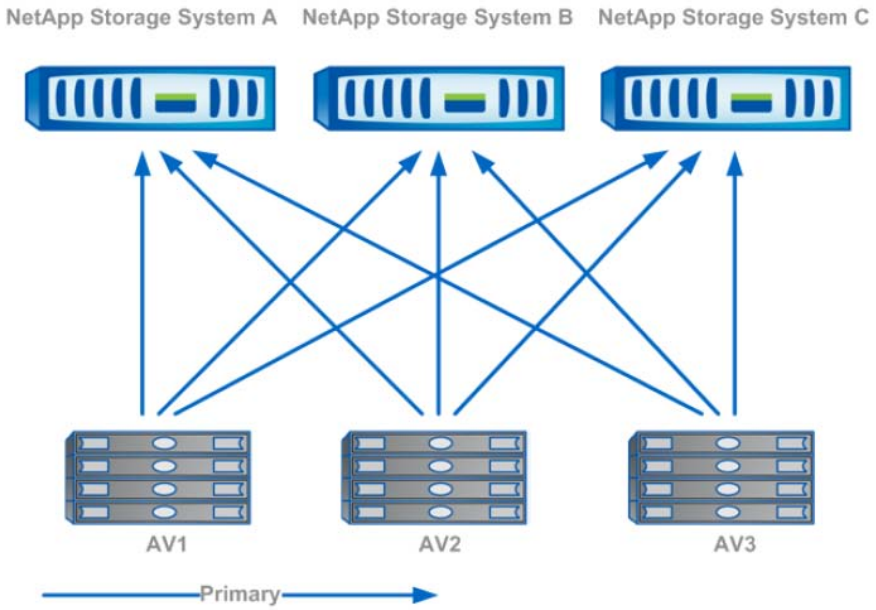
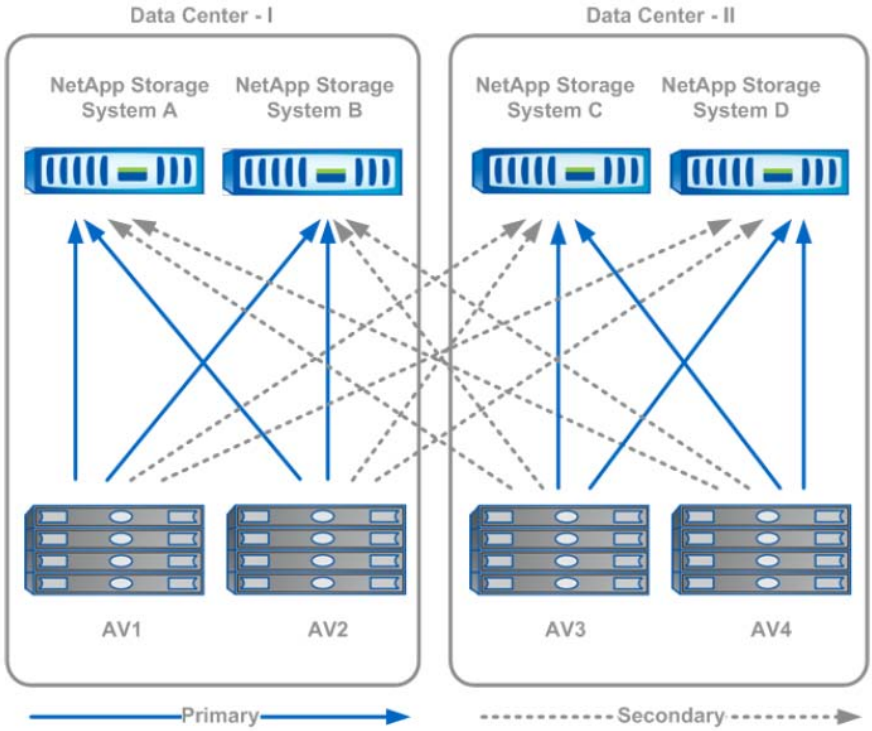


Figure 5) AV scanning pod between two data centers.



5.1 AV SCANNING POD

From Figure 5, the following relationships are established for each NetApp storage device and its primary and secondary AV scanner servers. This is what is referred to as a scanning pod.

NetApp Storage System A:

- Primary AV scanners: AV1, AV2
- Secondary AV scanners: AV3, AV4

NetApp Storage System B:

- Primary AV scanners: AV1, AV2
- Secondary AV scanners: AV3, AV4

NetApp Storage System C:

- Primary AV scanners: AV3, AV4
- Secondary AV scanner: AV1, AV2

NetApp Storage System D:

- Primary AV scanners: AV3 and AV4
- Secondary AV scanners: AV1, AV2

5.2 BENEFITS OF A SCANNING POD

- Increased redundancy of the AV scanner servers:
  - If primary AV scanner server goes down, the other remaining primary scanners can handle the AV load.
  - If both primary AV scanner servers go down, the NetApp storage device is scanned with the remaining secondary scanners.
- Make sure of an average of at least one AV scanner to one NetApp storage device ratio, which minimizes any chance of data outages due to AV scanner overload:
  - Sometimes having one AV scanner server for two NetApp storage devices is sufficient with the exception of heavy loads during peak hours, which could overload the AV scanner server. But depending on the file structure and access pattern, even as many as three servers per NetApp storage device could be necessary.
- Provides efficient use of AV scanner server hardware investment:
  - Avoids underutilization of AV scanner hardware.
  - The scanning pod model allows for the efficient utilization of hardware while providing redundancy.

5.3 SCANNING POD REQUIREMENTS AND RECOMMENDATIONS

Best Practices
• AV scanner servers should use Gigabit Ethernet: The scanning pod model allows for the efficient utilization of hardware while providing redundancy. • The NetApp storage device should have a secondary gigabit NIC dedicated to an AV network: Because AV servers require gigabit access to all the NetApp storage devices in the scanning pod, back-to-back network configurations should not be used. Instead, build an AV network for all NetApp storage devices and AV scanner servers in a switched environment. • Avoid building too large a scanning pod: This will reduce the risk from failures that cascade to other units of a scanning pod.

5.4 INCREASING BACKUP JOB PERFORMANCE

It is possible for a NetApp storage device system administrator to specifically disable virus scanning on a particular share. AV scanning by nature will affect the speed of backups on every file open created by the backup application. Note that this is not applicable for NDMP backups, but only for network-mapped backups. For example, backups might be too slow if files are being scanned during the backup over the network. To alleviate this, the administrator can create a normal data share, for which clients and apps have direct access and AV scans normally take place. A second share could then be created called databackup, pointing to the same physical location, which has virus scanning disabled on the share (this is configurable on a per share basis). After setting share permissions that only allow the backup user group to access the databackup share, normal users will be forced to use the protected data share, while backup can use the faster databackup share.

6 HOW AND WHEN A NETAPP STORAGE DEVICE DETERMINES TO SCAN A FILE

- Following are the operations that trigger virus scanning:
  - Open
  - Rename
  - Close (if the file was modified)
- The NetApp storage device initiates scanning based on the file extensions set by the NetApp storage device's administrator.
- The NetApp storage device scans a file when a file is closed after being modified. The NetApp storage device does not scan a file after each write, but only when a modified file is closed.
- Newly created files are not scanned on create, but only after data has been written to them and closed.
- The NetApp storage device does not scan a file when the file is accessed from the vscan server itself.
- If multiple applications access the same file simultaneously, they will all share the same scan results on the first application's virus scan. For example, if application-1 requests to open a file and triggers a scan for viruses, the scan is launched. If application-2 tries to open the same file, the NetApp storage device will not launch a second scan, but instead queues up application-2 to wait for the already active scan to complete. When the scan completes, both requests then continue being processed by the NetApp storage device.

7 SUMMARY

The integrated antivirus solutions for NetApp storage devices enable enterprises to protect their valuable data from computer viruses. The open, scalable, and high-performance architecture allows customers to choose the premier antivirus vendor that best suits their environment. Companies can deploy NetApp solutions enterprise-wide with best-in-class antivirus solutions that protect data without affecting the user experience.

8 REVISION HISTORY

Date	Name	Description
March 2011	Brahmanna Chowdary K, Manoj Kumar D V	Revised
April 2009	Suresh Kumar N	Creation

www.netapp.com