Antivirus Scanning Best Practices Guide

Network Appliance, Inc.

April 2006, TR-3107

Table of Contents

1. Introduction

NetApp storage systems and NetCache® appliances include integrated antivirus functionality to protect corporate data from computer viruses. NetApp storage systems include both the FAS product line and V-Series product line. 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 systems 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. NetCache appliances protect against viruses by initiating scans on content downloaded from the Internet.

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

This paper will describe the integrated antivirus architectures for both NetApp storage systems and NetCache appliances and describe some 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
- 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 systems and NetCache caching appliances help protect against malicious virus code by scanning files "on access" and during the download process.

The NetApp NAS and NetCache caching solution architectures are modular and share many similarities. The differences lie mostly in the protocol used to communicate with the antivirus servers and the antivirus products themselves.

The NetApp antivirus solution uses an authenticated CIFS connection and RPCs to communicate with the antivirus scanning servers. NetCache employs the HTTP-based Internet Content Adaptation Protocol (ICAP) when interacting with ICAP antivirus servers. CIFS and ICAP are industry-standard protocols with features best suited for their respective 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 accesses.
- ICAP provides RPC-like functionality for HTTP-based services and supports a wide variety of applications that offload specialized tasks such as virus scanning.

2. NetApp Antivirus Scanning

Prior to release of the integrated antivirus functionality for NetApp storage systems 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. Since Snapshot activities are commonly scheduled in weekly, daily, and hourly intervals, backups are automatic, and the "drag-and-drop" recovery is immediate and simple.

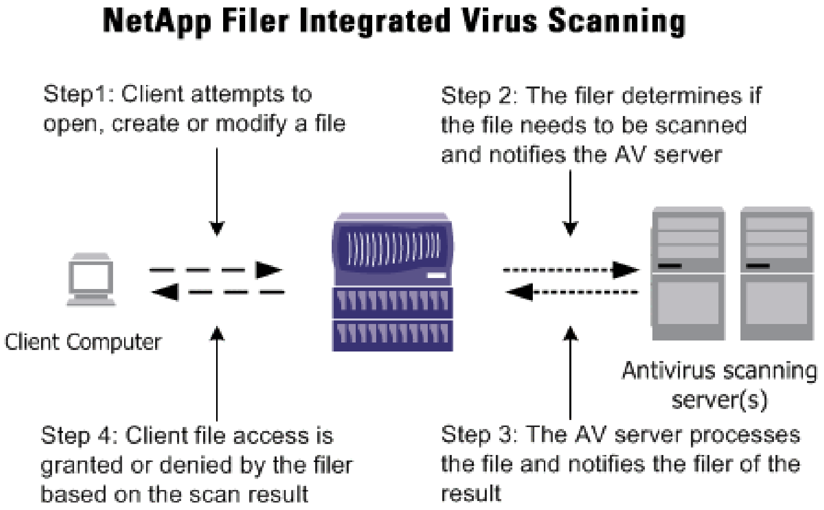
In order to detect and stop viruses before they reach the file system, Network Appliance integrated antivirus functionality into the NetApp storage system's microkernel, Data ONTAP™. NetApp integrated antivirus software (from McAfee, Symantec, Trend Micro, Sophos and Computer Associates) provides additional protection against viruses by 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).

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

NetApp storage systems 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 (see "How and When a NetApp storage system Determines to Scan a File" for more specifics):

- 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

The following diagram describes the basic steps that occur during the scanning process. Note for V-Series systems, the storage is provided by external 3rd party array vendor.


NetApp Filer Integrated Virus Scanning
Step1: Client attempts to open, create or modify a file
Step 2: The filer determines if the file needs to be scanned and notifies the AV server
Client Computer
Antivirus scanning server(s)
Step 4: Client file access is granted or denied by the filer based on the scan result
Step 3: The AV server processes the file and notifies the filer of the result

When a user tries to open, create, or change a file that matches the "to be scanned" criteria, such as an ".exe" file, the NetApp storage system 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 system of the results. If no virus is found, the NetApp storage system 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 system 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 may take several seconds on more complex files such as .zip or .cab files that may 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 system. 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 two actions. It will either "quarantine" the file or "disinfect" the file by removing the virus code and writing a new file. The following table describes the differences.

SCANNING CONFIGURATION	ACTION
Quarantine the file	The AV scanner quarantines the file or moves it to a special location, and the NetApp storage system denies the client access. The administrator must take action.
Disinfect the file	The AV software removes the virus and notifies the NetApp storage system when the file is clean. The NetApp storage system then allows the client to open the requested file.

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 may occur automatically via 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 system 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 ensures 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, please read the documentation included with each antivirus software product.

2.3 Defining Scanning Criteria

The NetApp storage system may be configured to "exclude" certain files by their extension so that those files are not scanned. For example, it may not be necessary to scan graphics files such as .jpg or .bmp files because they do not contain executable code. The NetApp storage system 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 wish to include or exclude specific types of files.

??_	**DOT**	**JS?**	**OV?**	**VBS**	**ASP**	**EXE**	**MD?**
ARJ	**BIN**	**CAB**	**CL**	**DL?**	**DRV**	**EML**	**IM?**
LZH	**MD?**	**MPP**	**OFT**	**PIF**	**POT**	**WPD**	**RAR**
POT	**VS?**	**BAT**	**GMS**	**MPP**	**PPL?**	**WXD**	**CDR**
GZ?	**MPT**	**RTF**	**WBK**	**COM**	**HLP**	**MSG**	**SCR**
WPD	**CSC**	**HT?**	**MSO**	**SHS**	**XL?**	**DL?**	**IM?I**
OCX	**SMM**	**XML**	**DOC**	**INI**	**OLE**	**SYS**	**XL?**
SWF	**VS?**	**VXD**					

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 on 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 on the "exclude" list.

To add extensions to the "exclude" list:

```
netapp> vscan extensions exclude add doc
```

To remove extensions on 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 system. 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 system and AV server is much smaller in proportion to the data served between the NetApp storage system 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 may 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 systems 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 system/AV solutions, the performance difference in most cases is measured in milliseconds (ms). Therefore, the entire scanning process may not be perceivable by most users. During periods of heavy use the difference may 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 system, and network. NetApp has observed a difference in throughput of up to 10% and a 15% increase in response time on unscanned files when virus scanning is enabled on a busy NetApp storage system. (For example, 10ms response times increase to almost 12ms.)

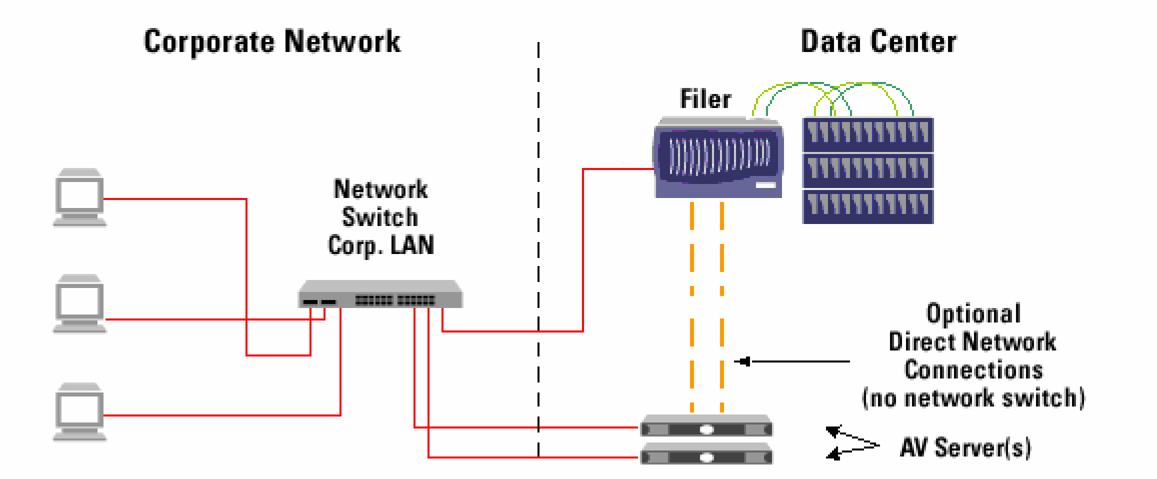
2.5 Network Connectivity

Network connectivity between the NetApp storage system 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.

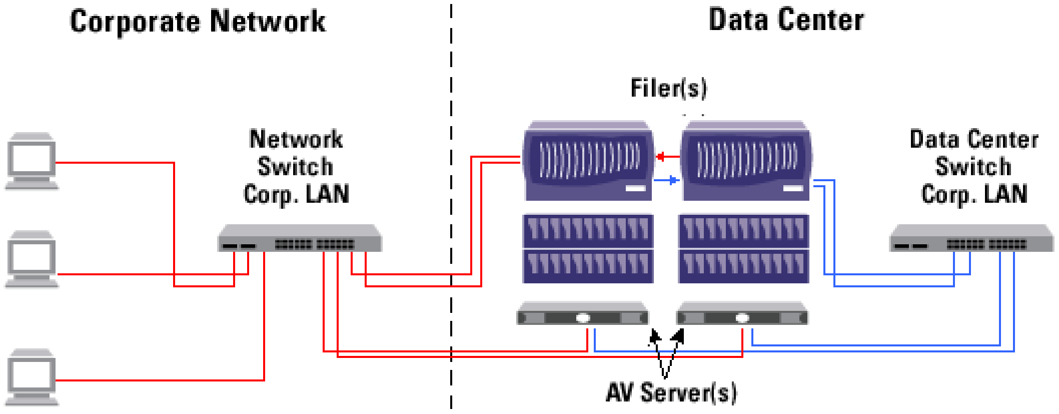
Directly connected or private connections between the NetApp storage system and each AV server will provide a clean network. If connecting through an Ethernet switch, use a dedicated switch or configure a virtual LAN (VLAN) to separate traffic traveling through the switch.

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

The following diagrams illustrate the different methods that can be used to provide connectivity between a NetApp storage system and its AV servers.



- A dedicated network switch or direct network connections may be used
- If the "direct-connect" method is used, a network interface card (NIC) is required for every connection between the AV server(s) and the filer



- Direct Network Connections (no switch) become complicated when using multiple filers and multiple AV servers together
- A dedicated switch guarantees better security and optimal performance
- Every filer and AV server required a minimum of two NICs

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 3rd party array vendor.

2.6 NetApp storage and AV Server Authentication

The connection between the NetApp storage system 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 are subject to authentication and must be a member of the "backup operators" group on the NetApp storage system
- Scanning servers register via RPC with the NetApp storage system
- 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 systems is recommended. Administrators should secure all network equipment and servers from unauthorized physical access.

2.7 Usage Profiles

The NetApp storage system 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 system supporting more users will result in more scanning activity. But the total scans per hour does not necessarily scale with the number of users. There is no direct correlation with the NetApp storage system'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

Network Appliance recommends the following minimum system requirements for each AV server.

AV SERVER	
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 factor with AV scanners is the CPU freq 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. Network Appliance recommends using AV scanners with the greatest CPU speed available. Also Network Appliance recommends rather two Dual processor servers vs one Quad processor server. Additional this server should not serve many other purposes (e.g. no Domain controller functionality etc.)

2.9 Multiple AV Servers and Multiple NetApp storage systems

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

It mostly depends on the file structure how many antivirus servers are needed per NetApp storage system. 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 system 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 system will time out the connection to the nonresponsive scanning servers and continue using the remaining scanning servers. The default time-out period is 12 seconds. If no scanning servers are available, the administrator may configure the NetApp storage system in one of two ways:

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

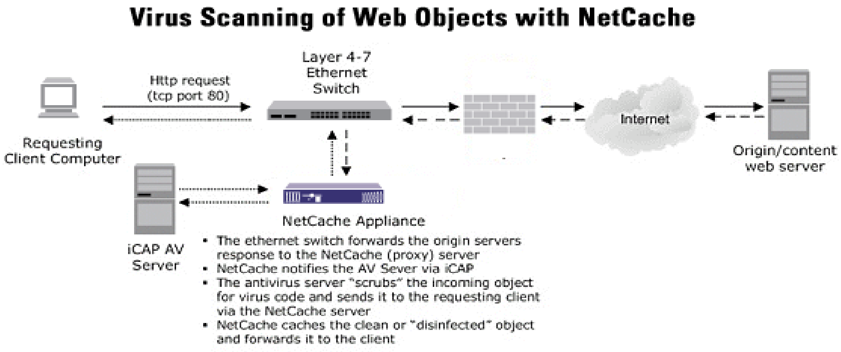
This behaviour is configured with the vscan option mandatory_scan. In all cases the antivirus servers will automatically contact and register themselves with their associated NetApp storage systems when they are back online. Once this occurs, the NetApp storage systems will resume normal operation with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

3. NetCache Antivirus Scanning

NetCache appliances deliver accelerated content management, content manipulation, streaming, proxy, and traffic monitoring functionality in a single appliance. NetCache provides industry-leading support for best-of-breed applications that extend functionality and increase scalability by offloading specialized processes to other computers.

NetCache uses the industry standard ICAP to communicate with ICAP-enabled antivirus servers. The antivirus servers scan and disinfect incoming content prior to caching (storing) the content and delivering it to users.

Client browser applications may be configured to use NetCache as a proxy, or NetCache can be deployed transparently, as shown in the following diagram.



- The ethernet switch forwards the origin servers response to the NetCache (proxy) server
- NetCache notifies the AV Sever via iCAP
- The antivirus server "scrubs" the incoming object for virus code and sends it to the requesting client via the NetCache server
- NetCache caches the clean or "disinfected" object and forwards it to the client

In the preceding example, NetCache performs a precache response modification on an object retrieved from an origin server. The content is directed to NetCache, which uses an ICAP response modification to forward the object to an ICAP antivirus server. The file is scanned for viruses, cached, and sent to the requesting client.

For more information on NetCache visit www.netapp.com.

4. Application Servers and NFS

4.1 Application Servers

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

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

4.2 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.

5. Antivirus Partners

Network Appliance has partnered with, Symantec, Trend Micro, McAfee, Sophos and Computer Associates to deliver integrated antivirus solutions. Contact Symantec, Trend Micro, McAfee, Sophos and Computer Associates for specific product information.

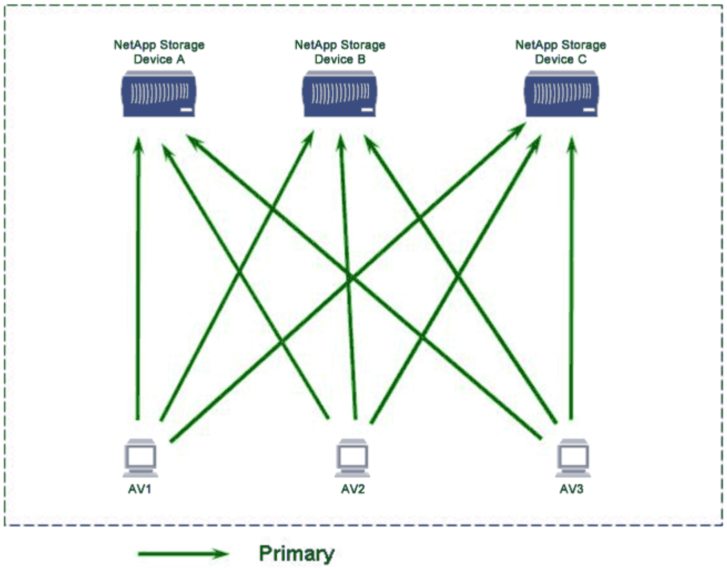
ANTIVIRUS PARTNER	PRODUCTS	NETCACHE ANTIVIRUS PRODUCTS
Symantec	X	X
Trend Micro	X	X
McAfee	X	
Sophos	X	
Computer Associates	X	

6. 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.

1. Avoid large AV scanning farms with too many NetApp storage systems served by too many AV scanner servers. Instead, choose a "Pod design," as described in section 6.1. This avoids performance spikes, which may be caused if all NetApp storage systems 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 systems.
2. Best practices dictate that you use an AV scanner server dedicated to antivirus scanning and not used for other jobs such as backup.
3. Connect to the AV scanner server via NetApp storage system IP address and not the NetApp storage system's NetBIOS name to control which NetApp storage system interface is used.
4. For multi NetApp storage system-multi scanner environment, make all AV scanners, which are connected with similar high performing network connection, as primary to all the NetApp storage systems. This will improve the performance by load sharing. Refer to Figure 6.1.
5. If you have two different data centers in two different locations (Local and Remote), then make all the local AV scanners as primary to all local NetApp storage systems and make those as secondary to all remote NetApp storage systems and vice versa. Also, Depending on the amount of

vscan requests some NetApp storage systems (FAS960/GF960 or higher – NetApp Storage Device D) may require additional dedicated scanners that aren't to be shared with other NetApp storage systems as secondary scanners. Refer to Figure 6.2.



All AV servers are configured as primary scanners to all NetApp storage systems

Figure 6.1. 'Sanning Pod" for NetApp storage systems and AV servers having consistent connectivity

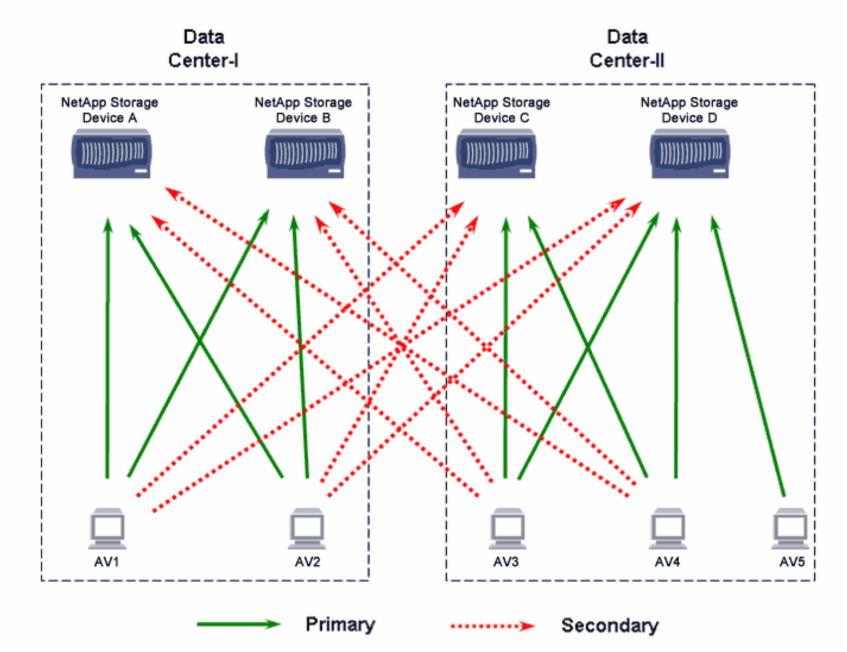


Figure 6.2. Scanning Pod for two datacenters in different locations

6.1 AV Scanning Pod

From Figure 6.2, the following relationships are established for each NetApp storage system and its primary and secondary AV scanner servers. This is what is referred to as a "Scanning Pod."

NETAPP STORAGE SYSTEM - A

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

NETAPP STORAGE SYSTEM - B

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

NETAPP STORAGE SYSTEM - C

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

NETAPP STORAGE SYSTEM - D *(due to its load, it has one dedicated primary scanner)*

Primary AV scanner: AV3, AV4, and AV5 Secondary AV scanners: AV1, AV2

6.2 Benefits of a Scanning Pod

1. 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 system is scanned with the remaining secondary scanners.
2. Ensures am average of at least "one AV scanner to one NetApp storage system" ratio, which minimizes any chance of data outages due to AV scanner overload:
   - Sometimes having one AV scanner server for two NetApp storage systems 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 system are necessary.
3. 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.

6.3 Scanning Pod Requirements and Recommendations

1. *AV scanner servers should use Gigabit Ethernet:*

The "Scanning Pod" model allows for the efficient utilization of hardware while providing redundancy.

2. *The NetApp storage system should have a secondary Gigabit NIC dedicated to an AV network:*

Because AV servers require Gigabit access to all the NetApp storage systems in the "Scanning Pod," "back to back" network configurations should not be used. Instead build an "AV network" for all NetApp storage systems and AV scanner servers in a switched environment.

3. *Avoid building too large a "Scanning Pod":*

This will reduce the risk from failures that cascade to other units of a "Scanning Pod."

6.4 Increasing Backup Job Performance

It is possible for a NetApp storage system system administrator to specifically disable virus scanning on a particular share. AV scanning by nature will impact the speed of backups on every file open created by the backup application. Note that this does not apply for NDMP backups—only 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 share, data, 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.

7. How and When a NetApp storage system determines to scan a File

1. Technically, the NetApp storage system will scan on:

   Open
   Rename
   Close (if the file was modified)

2. The NetApp storage system will scan a file based on the file extensions set by the NetApp storage system's administrator.
3. The NetApp storage system scans a file when the file is opened.
4. The NetApp storage system scans when a file is renamed to a file name that has one of the designated file extensions.
5. The NetApp storage system scans a file when a file is closed after being modified. The NetApp storage system does not scan a file after each write, but only when a modified file is closed.
6. Newly created files are not scanned on create, but only after data has been written to them and closed.
7. The NetApp storage system does not scan a file when the file is accessed from the vscan server itself.
8. 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 system 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 system.

8. Antivirus Integration with Decru DataFort

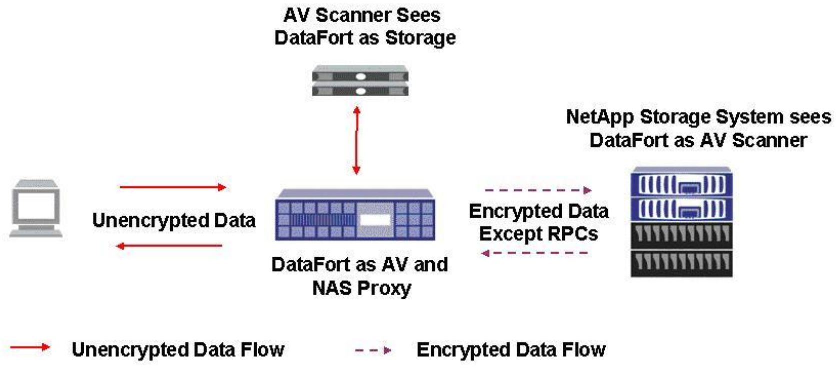
NetApp storage systems have integrated antivirus functionality with Decru DataFort appliances to detect viruses in files that are encrypted in storage.

When a DataFort appliance is used to encrypt the data stored on a NetApp storage system that will be scanned for viruses, the Antivirus scanners (AV scanners) must have access to the data in unencrypted form in order to correctly scan the file contents and detect viruses. The following steps must be performed for such integration:

- Add the AV scanners to DataFort as hosts
- Setup client/server Virtual IPs (VIPs) – NetApp storage system as the server and AV scanners as the clients

- Setup routes for RPC communication between NetApp storage system and DataFort
- Register DataFort as the RPC target instead of NetApp storage system during the installation of Antivirus software
- Export Cryptainers.This includes even the cleartext Cryptainers as virus scanning will be done through DataFort exclusively

When completed, DataFort acts as a proxy between NetApp storage system and AV scanner as depicted in the following figure. Maximum level or data security is ensured by integrating DataFort with NetApp storage system's antivirus solution.



9. Summary

The integrated antivirus solutions for NetApp NetApp storage systems and NetCache appliances 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-of-breed antivirus solutions that protect data without affecting the user experience.

10. Revision History

DATE	NAME	DESCRIPTION
04/24/2006	Network Appliance, Inc.	Revision
02/01/2006	Network Appliance, Inc.	Revision
09/01/2005	Network Appliance, Inc.	Revision
01/31/2005	Network Appliance, Inc.	Revision
09/12/2003	Network Appliance, Inc.	Revision
05/22/2002	Network Appliance, Inc.	Revision
05/01/2001	Network Appliance, Inc.	Creation