Implementation Guide

McAfee® VirusScan Enterprise for Storage® software

version 1.0

Contents

Preface

Contact information

Threat Center: McAfee Avert® Labs http://www.mcafee.com/us/threat_center/default.asp

Avert Labs Threat Library
http://vil.nai.com

Avert Labs WebImmune & Submit a Sample (Logon credentials required)
https://www.webimmune.net/default.asp

Avert Labs DAT Notification Service
http://vil.nai.com/vil/signup_DAT_notification.aspx

Download Site http://www.mcafee.com/us/downloads/

Product Upgrades *(Valid grant number required)*

Security Updates (DATs, engine)

HotFix and Patch Releases
□□For Security Vulnerabilities *(Available to the public)*
□□For Products *(ServicePortal account and valid grant number required)*

Product Evaluation

McAfee Beta Program

Technical Support http://www.mcafee.com/us/support/

KnowledgeBase Search
http://knowledge.mcafee.com/

McAfee Technical Support ServicePortal *(Logon credentials required*)
https://mysupport.mcafee.com/eservice_enu/start.swe

Customer Service

Web
http://www.mcafee.com/us/support/index.html
http://www.mcafee.com/us/about/contact/index.html

Phone — US, Canada, and Latin America toll-free:
+1-888-VIRUS NOor**+1-888-847-8766** Monday – Friday, 8 a.m. – 8 p.m., Central Time

Professional Services

Enterprise http://www.mcafee.com/us/enterprise/services/index.html

Small and Medium Business http://www.mcafee.com/us/smb/services/index.html

VirusScan Enterprise for Storage advanced configuration

☐ This product is an upgrade for VirusScan for NetApp 7.1.
☐ This product expands the VirusScan Enterprise 8.7i capabilities by providing off-box scanning for NetApp and Sun appliances:

- NetApp uses RPC for connections.
- Sun storage scanner uses ICAP protocol.

This guide helps security officers and network administrators configure the advanced options of McAfee® VirusScan Enterprise for Storage software including implementing it with multiple scanners and multiple filers.

Section 1: NetApp Scanner Overview

VirusScan Enterprise for Storage allows a NetApp Filer to submit a file for anti-virus scanning before responding to a client's attempt to access that file.

When a file is scanned and found to be clean, or is cleaned by the anti-virus software, the Filer's ***operating system (see below)*** flags the file, indicating that it need not be scanned again. (**Note:** Flagging a file to exempt it from future scanning is referred to as caching. This cache is maintained by the Filer, separate to VirusScan's clean-file scan cache.)

Operating System for the NetApp Filer is called Data ONTAP. It provides a command line interface for managing the Filer. It can be accessed using Telnet or via a browser. The command for modifying anti-virus related settings is "**vscan**". **vscan** allows you to set what file extensions should be sent to the anti-virus software for scanning.

When a client attempts to access a file that is not cached, and whose filename includes an extension that is listed in the Filer's operating system, the filer transmits the file's path with scan request identification to the scanner-server. VirusScan for Storage examines the file and informs the filer whether it is safe to allow the client access to the file.

The Filer's operating system controls the list of file types to be scanned. However, VirusScan for Storage only examines files that it is configured to examine. To ensure that VirusScan for Storage scans any type of file, the installation of VirusScan for Storage automatically configures its **Network Appliance Filer AV Scanner** to **scan all files**.

To communicate with Data ONTAP and modify its list of file types, you can use a utility, such as Microsoft Telnet, that allows you to run a command-line session on the Filer. Also most Filers now allow you to access a command line session using a browser.

VirusScan for Storage is an "add-on" module to VSE 8.7, its install adds two console items (Network Appliance Filer AV Scanner and ICAP AV Scanner) and the McAfee VirusScan

Enterprise for Storage service. The McAfee VirusScan Enterprise for Storage service

manages scan requests received from the Filer and uses the McAfee Engine Service to perform the actual scan of the file.

The McAfee VirusScan Enterprise for Storage service is dependent on the McAfee Engine Service.

Section 2: Multi-to-multi configurations

Connecting multiple scan servers to a single filer

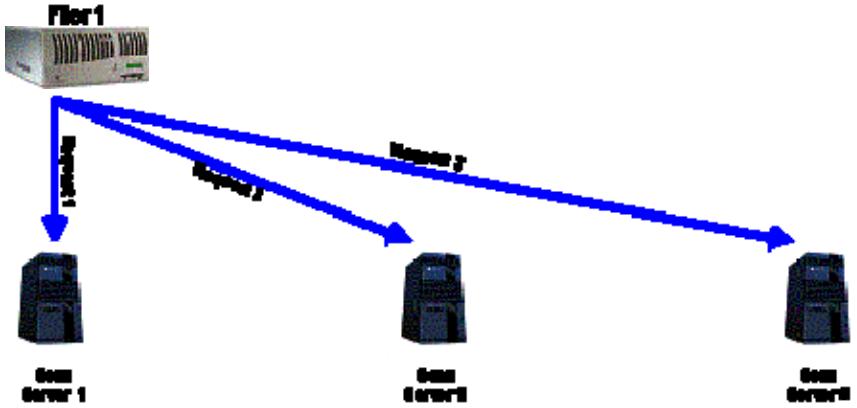
Registering multiple scan servers with a filer can improve the filer's scanning performance. When multiple scan servers are registered with a filer, scan requests are sent using a "round-robin" method. Data ONTAP™ sends outgoing scan requests incrementing through all connected scan servers. When the filer reaches the last scan server it starts over sending the next scan request to the first scan server in the array.

From the Data ONTAP™ console type "vscan" to display a list of connected scan servers.

Virus scanning is enabled.

Virus scanners(IP and Name)		Connect time (dd:hh:mm)	Reqs	Fails
192.168.16.100	\\SCANSERVER1	00:12:01	0	0
192.168.16.101	\\SCANSERVER2	00:12:01	0	0
192.168.16.102	\\SCANSERVER3	00:12:01	0	0

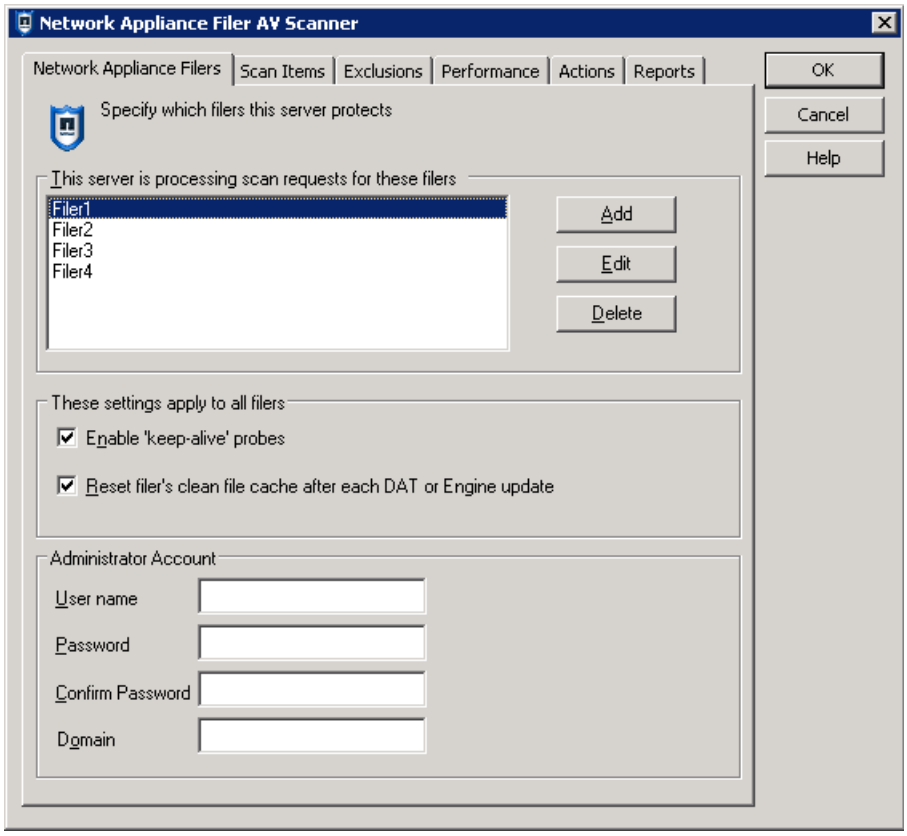
Figure 1: Connecting multiple scan servers to a single filer



Connecting multiple filers to a single scan server

A feature in VirusScan Enterprise® for Storage 1.0 allows each scan server to connect to a maximum of 20 filers. This allows an administrator to construct a multi-to-multi configuration which provides a more efficient use of equipment resources as well as improves fail over protection.

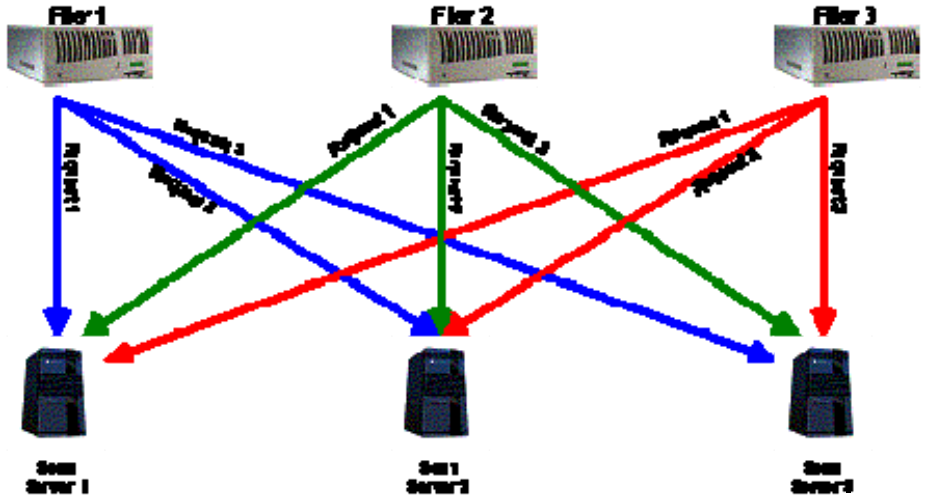
Figure 2: The scan server properties dialog allows you to specify more than one filer.



Connecting multiple scan servers to a multiple filers

Registering multiple scan servers with a filer can improve the filer's scanning performance. When multiple scan servers are registered with multiple filers, scan requests are sent using a "round-robin" method. Data ONTAP™ sends outgoing scan requests incrementing through all connected scan servers. When each connected filer reaches the last scan server it starts over sending the next scan request to the first scan server in the array.

Figure 3: Multi-2-Multi configuration



Section 3: Testing your configuration

Factors to consider

Peak usage statistics – Before you begin, it is important to understand the load conditions that the filer is working under in your current environment. For example, add NT Performance Monitor counters to a production filer during peak usage hours. Monitor and record the network traffic to and from the filer as well as the CIFS operations per second. It is essential to separate the Network traffic in and the traffic out statistics because Data ONTAP™ has the capability to cache files that have already been scanned from CIFS read operations, and you want your simulation to reflect the types of file system operations occurring in your environment.

Average file size and latency – Due to vastly diverse business needs the filer may serve many small files, fewer large files, and/or combinations of file sizes. This can become a factor when testing latency. It is important to gather data about filer usage and select a file sample set that reflects your daily business operation.

Selecting a Test Method

Following are some tools that we have used to generate load on a filer. They may be useful as a starting point for developing a test to suit your business needs

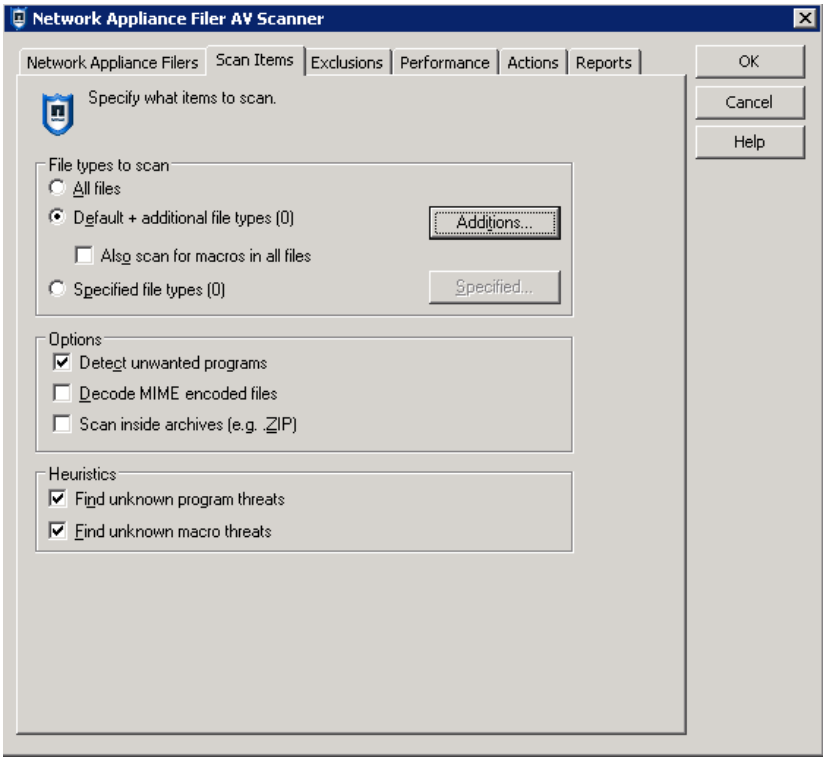
Batch Files:
Used to copy directories of files to and from the filer. This is a fairly straightforward method, but does not necessarily provide latency data for the opening of files. However, the batch files can be used to generate stress conditions under which to measure latency.

NetBench:
NetBench is designed to measure how well a file server handles file I/O requests from 32-bit Windows client. http://www.softlookup.com/download.asp?id=25367

Section 4: Tuning performance

The age-old debate: Performance vs. Reliability

There is always a trade-off for increased performance. This section describes some settings that may increase your current performance and some of the risks associated with the adjustments.



All-Files vs. Default Files Mode

Figure 4: All-Files, Default Files

Changing the **Scan Items | File types** to scan from **All files** to **Default + additional file types** can increase your scan server's performance. The **Default files** mode does not attempt to determine the type of file being scanned but rather uses the file extension to determine what type of file is being scanned.

For example, a Word document would be scanned as a Word document in **All files** mode, not because it has the extension DOC, but because VirusScan® for NetApp® has analyzed the file internally and determined it to be a Word document. In the **Default + additional file types** mode it would scan the same file as a Word document not because it analyzed the file but because the extension is DOC. The extra analysis in **All files** mode takes time to complete so setting the Filer AV Scanner to **Default + additional file types** decreases the time it takes to scan a file. The trade-off however, is that because **Default + additional file types** trust that the document is the type that the extension indicates, an infector may not be detected if it was renamed.

Section 5: What to expect

To help our customers identify the impact of using an AV solution, McAfee has some guidelines that may be useful in determining the boundaries of the particulars of their NetApp environment. There are many variables to account for in the various environments in which NetApp Filers are operated. Data ONTAP™ makes use of file caching which makes performance testing and the resulting calculations extremely complex. We have experienced vast differences in the data types managed and stored on most networks. There can be significant differences in scanning performance based on the complexity and type of the files involved. For example, scanning a text file may require the scan server to analyze only part of the file to determine if it is infected where as an MS word document may require the scan server to analyze the entire file.

The first step is to study your current filer usage. The data collected during this exercise will help to implement an effective filer AV strategy to accommodate your business needs.

To determine typical usage in your environment you will need to analyze filer data during a peek usage period. Remember that filer read operations may be cached and require fewer scan requests then write operations so it is important to separate the traffic in from the traffic out on the filer. In this
example the data was recorded using the Windows Performance Monitor utility.

NetApp Filer #1
Net-Out kb/s 339
Net-In kb/s 147

NetApp Filer #2
Net-Out kb/s 158
Net-In kb/s 22

The next step is to determine a ratio of inbound data to outbound data. In this case I plan to configure the 2 filers in a multi-2-multi configuration with the scan servers so the ratio will incorporate both filers' usage data. The network traffic will need to be classified using

the following categories. You may want to weight this data differently depending on how often the cache is reset on your filer or if a significant portion of traffic is generated from database activity that you have may have excluded from scanning.

Cached Read Operations	Read Operations	Write Operations
249	249	169

We have constructed a few multiplier categories based on the performance impact we have observed using different types of files. You should use the use the multiplier category that best suits your filer needs.

Category 1: Graphics and Web Design
Inbound Traffic Multiplier: 0.56
Outbound Traffic Multiplier: 0.77

Category 2: Microsoft Office and B2B
Inbound Traffic Multiplier: 0.60
Outbound Traffic Multiplier: 0.98

Category 3: CAD, Database, Large Files
Inbound Traffic Multiplier: 0.57
Outbound Traffic Multiplier: 0.63

To help estimate your performance impact when scanning all files multiply the KB/s by the appropriate multiplier to retrieve your estimate.

[Net-In kb/s] X [Inbound Traffic Multiplier] = Estimated KB/S with Scan Server
[Net-Out kb/s] X [Outbound Traffic Multiplier] = Estimated KB/S with Scan Server

Note that these estimates assume that Data ONTAP™ has "???" added to the extension list so that all files will be sent to the scan server. Calculations for other extension list settings require weighted information about the file types in use on your filer.

Observations

Adding Scan Servers:
The number of Scan Servers to a filer utilizes can have a significant effect on the data throughput between the client systems and the filer. In this example we measured the client throughput and Average response time using Netbench with one to three scan servers connected.

Adding Scan Servers to Improve Performance

Data Throughput

# of Scan Servers

Average Response Time

# of Scan Servers

		1	2	3
# of Clients	**10**	43.27	49.63	50.85
	15	54.01	69.83	73.60
	20	56.90	85.33	92.64
	25	57.14	93.42	108.31
	30	56.98	95.12	115.57

		1	2	3
# of Clients	**10**	1.35	0.87	0.79
	15	2.09	1.08	0.90
	20	3.27	1.40	1.10
	25	4.66	1.93	1.34
	30	6.10	2.70	1.80

Section 6: Determining if your configuration is adequate

The easy way to determine if the scan server is able to keep up with the scan requests coming from the Filer is to look at the "Scan Request Denied" statistic. This statistic can be viewed from the client UI's "Network Appliance Filer Scanner Statistics" dialog. To see this dialog open VSE, and right mouse click on the "Network Appliance Filer AV Scanner" item and select "Statistics". This dialog shows total statistics for the scan server, to see specific statistic for a Filer double click on the Filer name, this will display the "Filer Statistics" dialog. This dialog shows statistics since the VSE for Storage service was started. To see historical statistics use the "Stats_NetApp.log" log or use ePO 4.0 reporting.

To understand the load the Filer is placing on the Scan Server check the "Highest Scan Thread Count" statistic shown on the "Network Appliance Filer Scanner Statistics" dialog. The higher the number the greater the load.

In conjunction to checking the above information, also take a look at task manager for cpu and memory usage for VirusScanAdvancedServer.exe and EngineServer.exe.

Based on what the results gathered from the above items (if server is not being maxed out - concurrent threads, CPU and memory usage) , the recommended changes would be to increase the scan timeout on the scan server from 60 to 90. Increase the scan timeout on the filer to 120 to see if it helps reduce the errors.

If you are still seeing a lot of timeouts, you can revisit increasing the scan timeouts but you would need to go over the items above to make sure you are not overloading the scan server. If the scan server is maxed out, one consideration would be to add an additional scanning server to handle the requests coming from the filer.

Section 7: Additional antivirus considerations for Netapp

Network Connectivity

- Directly connected or private connections between the NetApp storage system and each scan scanner will provide a clean network
- If connecting through an Ethernet switch it's best to use a dedicated switch

- If dedicated switch is not available configure VLAN for just filer and AV scan server.

Best Practices for Antivirus Scanning

- Avoid large AV scanning farms with too many storage systems served by too many AV scan servers.
- Use a Pod Design to avoid performance spikes. (See figure 1)
- Configure VSE for Storage to use the IP address of filers instead of the NetBios name
- For a multi to multi configuration make all AV scan servers which are connected to the same switch Primaries. (See figure 1)
- In a multi to multi configuration, if you have 2 different sites (local and remote), make all local AV scan servers as primary and make all remote scan servers secondary's. (See figure 2)

Figure 1- 'Scanning Pod" for NetApp storage systems and AV scan servers having consistent connectivity

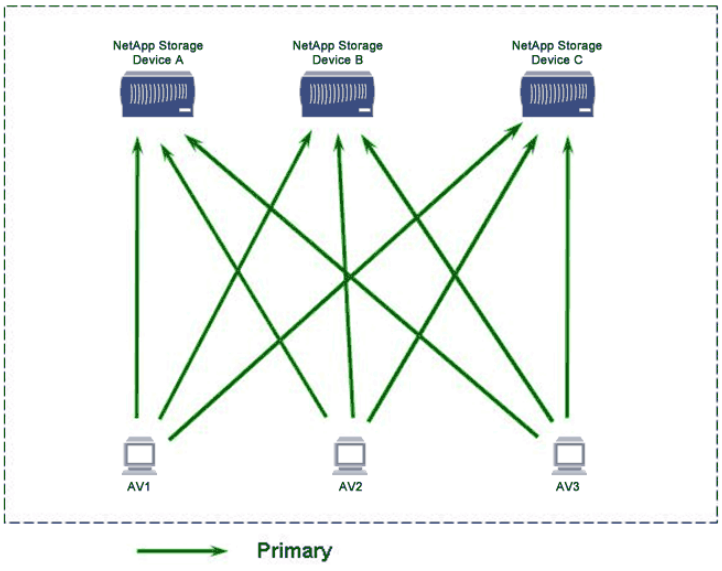
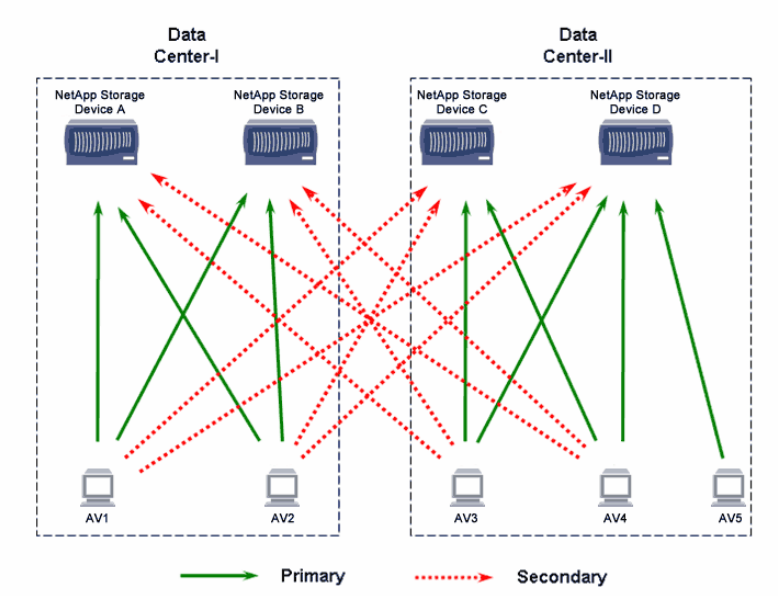


Figure 2. Scanning Pod for two datacenters in different locations



Benefits of a Scanning Pod

- If primary AV scan server goes down, the other primary scanners can handle the AV load.
- If both primary scanners go down, the filer can be scanned by the secondary scanners.
- Provided efficient use of AV scanner server hardware

Scanning Pod Requirements and Recommendations

- It's best for AV scan servers to use Gigabit Ethernet
- The filer should have a secondary Gigabit NIC dedicated to AV network.
- Avoid building too large a scanning pod.