



ZFS STORAGE
APPLIANCE

An Oracle Technical White Paper
January 2014

How to Configure McAfee VirusScan Enterprise for the Oracle ZFS Storage Appliance

Table of Contents

Introduction	3
How VSCAN Works.....	4
Installing VSE and Configuring the Oracle ZFS Storage Appliance	6
Deployment of the VSE Scanner Appliance.....	7
Planning Network Topology.....	7
Installing the VSE Virus Scanner.....	8
Connecting the Oracle ZFS Storage Appliance to the Virus Scan Service.....	12
Verifying the Virus Scan Service Configuration	12
Configuration Best Practices	16
Handling Archive Type Files.....	16
Disabling the File Repair Option	17
Synchronizing System Time	18
Conclusion	18
Appendix: References	20
Figure 1. File virus scan steps.....	5
Figure 2. Internet proxy server setup.....	8
Figure 3. McAfee VSE setup window.....	9
Figure 4. McAfee VSE setup wizard	9
Figure 5. VSESTOR setup	10
Figure 6. VSE Update Now activation.....	10
Figure 7. VirusScan Console window	11
Figure 8. VSESTOR ICAP Setup.....	11
Figure 10. Oracle ZFS Storage Appliance scan engine(s) through ICAP setup	12
Figure 11. ICAP AV Scanner logging options	14
Figure 12. ICAP Scan logging example	15
Figure 13. Windows Application event logging showing AV detection.....	15
Figure 14. Oracle ZFS Storage Appliance virus scan logs.....	16
Figure 15. ICAP AV Scanner, file type selections	17
Figure 16. ICAP AV Scanner, specifying virus detect only.....	18

Introduction

Efficient protection of electronic data against threats from malware is as important to an enterprise as a comprehensive backup/restore and disaster recovery process. Computer viruses, phishing, adware, and spyware can put electronic data at risk of being manipulated or destroyed, impact the operation and availability of data services, and result in unwanted disclosure of information and exposure to unsolicited content. The ability to protect content in electronic data repositories against corruption by malicious software and the ability to isolate and dispose of files that impose potential risks are essential components of any enterprise's data protection strategy.

The Oracle ZFS Storage Appliance provides protection against computer viruses by using an integrated on-demand virus scanning service called VSCAN. The VSCAN service is based on the Internet Content Adaptation Protocol (ICAP) and works together with an external virus scanning engine which, for performance and security reasons, should be running on another host located on the same LAN segment as the Oracle ZFS Storage Appliance. The solution described in this paper uses McAfee VirusScan Enterprise antivirus software as the external virus scanning engine.

McAfee VirusScan Enterprise (VSE) antivirus scanner analyzes any files in question for suspicious patterns and passes the scan results back to the Oracle ZFS Storage Appliance VSCAN service. Based on the scan result, VSCAN makes the file accessible to users or blocks access by quarantining the file. A file quarantined by the VSCAN service is not accessible to users regardless of the access protocol used (CIFS or NFS).

This document describes the installation and configuration of McAfee VirusScan Enterprise for use as a virus scan engine with the Oracle ZFS Storage Appliance VSCAN service.

NOTE: References to Sun ZFS Storage Appliance, Sun ZFS Storage 7000, and ZFS Storage Appliance all refer to the same family of Oracle ZFS Storage Appliance products. Some cited documentation or screen code may still carry these legacy naming conventions.

How VSCAN Works

When virus scanning is enabled on a populated volume, a scan is not initiated across all files. Instead, the VSCAN service initiates a request for a virus scan to the virus scanning engine (in this case, VSE antivirus scanner) each time a "file open" or a "file close" request is issued. Thus, only files that are created, modified, or opened for read operations are scanned.

This approach ensures efficiency in that files are only scanned on demand. However, it does not support a pre-emptive scan of file system contents. A second limitation is that only shares using access protocols that issue "file open" and "file close" requests, such as CIFS and NFS v4, are candidates for virus protection using the VSCAN service. A share that is published using NFS v3 cannot be scanned using VSCAN because NFS v3 does not issue the "file open" or "file close" requests that trigger the ICAP client.

Note: As an alternative, a share can be scanned by mounting or mapping it to a host server running an antivirus client and then scanning it locally.

The VSCAN service maintains several file attributes that it uses when processing the results of a scan. These attributes describe:

- The configuration of the virus scan engine that was used for the most recent scan of the file (referred to as the scanstamp).
- Whether the file is quarantined, based on the evaluation of the file returned by the virus scan engine.
- The modified attribute, which the file system sets when the file has been changed or renamed. After a successful scan of a file, the VSCAN service clears the modified attribute.

A file is scanned when a "file open" or "file close" request is initiated and one of the following is true:

- The file does not have a scanstamp attribute, indicating it has never been scanned before.
- The scanstamp of the file does not match the virus pattern and scan options (ISTag string) specified in the current configuration of the virus scan engine.
- The modified attribute of the file is not cleared.

The VSCAN service communicates with the virus scan engine using ICAP. The Oracle ZFS Storage Appliance acts as an ICAP client and the virus scan engine acts as the ICAP server. When the Oracle ZFS Storage Appliance requests that a file be scanned, the file is transmitted without encryption to the ICAP server for analysis.

While a request to scan a file is being fulfilled by the ICAP server, access to the file is denied. The user privileges defined in the access control list (ACL) for the file are irrelevant as long as the Oracle ZFS Storage Appliance is waiting for the ICAP server to respond.

When the virus scan engine reports a file to contain a virus, the VSCAN service sets the `av_quarantined` bit in the Extended System Attributes (ESA) of the file. This prevents any further client access to the file.

Note: To avoid data becoming unavailable when a virus scan engine does not respond to ICAP requests, best practice is to configure the VSCAN service to use of at least two virus scan engines.

An ICAP server does not require registration or authentication with the Oracle ZFS Storage Appliance to serve scan requests.

Figure 1 shows the interaction between an ICAP client and an ICAP server when a NAS client requests access to data on a virus-protected share of the Oracle ZFS Storage Appliance. The workflow comprises seven steps initiated by a request from the NAS client to access a file on a shared volume using NFSv4 or CIFS protocol.

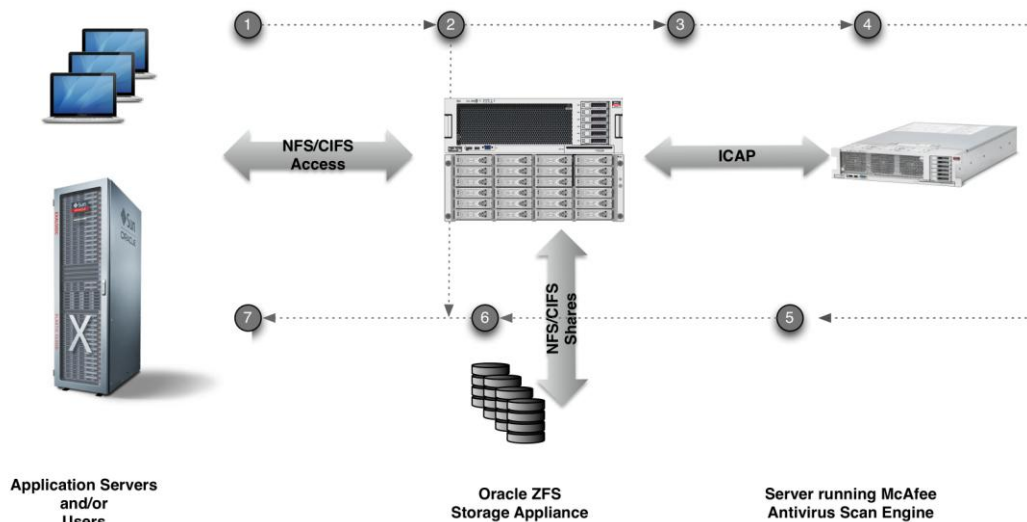


Figure 1. File virus scan steps

The following sequence of steps is followed when a file is accessed/created by a client on an NFS/CIFS file share when using a McAfee antivirus scan engine.

1. The client accesses the file.
2. The Oracle ZFS Storage Appliance determines, using scanstamp information and file open or close operation requests, if the file need to be scanned. If no scan is needed (the file was scanned before and no updates made), the client is granted access and contents are returned.

3. The file needs to be scanned; a scan request is issued to the virus scan engine.
4. The virus scan engine scans the file.
5. The virus scan engine responds back to the Oracle ZFS Storage Appliance with one of the following results:
 - a) File OK.
 - b) Virus found; file quarantined.
 - c) Virus found; file repaired.

Note: this response depends on the Actions setting in the virus scan engine. The Clean option must be set in order to trigger file repair. For use with the Oracle ZFS Storage Appliance, set this Action option to 'Continue Scanning'. These settings will be shown later in this paper in the Best Practices section.

6. The Oracle ZFS Storage Appliance takes one of the associated following actions, depending on the virus scan engine response:
 - (for result a): File stored/read.
 - (for result b): The av_quarantined toggle is set in ESA to deny further client access.
 - (for result c): The av_quarantined toggle is set in ESA to deny further client access. The Oracle ZFS Storage Appliance always sets the affected file in quarantine when a virus is detected.
7. The Oracle ZFS Storage Appliance responds, for the associated action, to the client:
 - (for result a): Client access is allowed.
 - (for result b): Client access is denied.
 - (for result c): Client access is denied.

Note: As mentioned earlier, using NFSv3 will not trigger scan requests. However, files marked as infected cannot be accessed over NFSv3.

Installing VSE and Configuring the Oracle ZFS Storage Appliance

The McAfee Individual Endpoint Product Suite contains McAfee VirusScan Enterprise (VSE), used in combination with the McAfee VirusScan Enterprise for Storage (VSESTOR) to create an antivirus scanning solution for the Oracle ZFS Storage Appliance.

The VSE and VSESTOR components are supported on various Microsoft Windows platforms. For this paper, a virtual machine running Windows 2003 Server is used.

The VSE component contains the antivirus scanning engine and a console that allows users to configure, monitor, and set maintenance functions for the antivirus scanning environment. The VSESTOR component handles the interface between the Oracle ZFS Storage Appliance and the VSE antivirus scan engine using the ICAP protocol.

The software can be installed on both virtual environments, like Oracle VM server and Oracle VirtualBox, and bare metal configurations, like Oracle x86-based servers. Oracle VM Server is more suitable for permanent deployment of virtual machines. Oracle VM VirtualBox is best used in desktop virtual clients and test environments.

Throughout this paper the Windows version of VSE has been used.

You can find the installation images using the 'Download Free Trial' option on the McAfee web site's McAfee VirusScan Enterprise pages.

Deployment of the VSE Scanner Appliance

Ensure the following prerequisites are met before deploying the VSE scanner:

- Check the section describing the Virus Scan Service of the Oracle ZFS Storage Appliance in the online help pages or PDF version found on the Oracle ZFS Storage Appliance product pages (See Appendix: References).
- Download and study the *McAfee VirusScan Enterprise* documentation and the *McAfee VirusScan Enterprise for Storage, Product Guide* available at the McAfee web site.
- Download the McAfee VSE and VSESTOR packages.
- Verify that the hardware requirements for the McAfee VSE and VSESTOR packages meet your (virtual) hardware platform specifications.
- In case a corporate proxy server is required for Internet access to McAfee's update server, verify support for virus update requests from your machine using the proxy server to McAfee's update server.
- Verify web browser access to the Oracle ZFS Storage Appliance.
- Verify that shares on the Oracle ZFS Storage Appliance you plan to protect are using either CIFS or NFSv4 protocol.
- Verify that required network connections are in place and working.
- Check if your firewall needs to be configured to let ICAP TCP traffic between the Oracle ZFS Storage Appliance and the VSE server using port 1344 passthrough.

Planning Network Topology

A LAN TCP/IP network connection is required for the Oracle ZFS Storage Appliance to access the services of the VSE. A minimal configuration requires one network connection

to the Oracle ZFS Storage Appliance and one network connection to the VSE. This is sufficient for small configurations. Note that with this configuration, all network traffic will pass through a single network port on both the Oracle ZFS Storage Appliance and the VSE.

For the Oracle ZFS Storage Appliance, best practice is to separate client data and administrative I/O traffic. The virus scan service generates extra data traffic with the ICAP interface. To prevent this I/O from impacting data I/O performance between Oracle ZFS Storage Appliance and clients, use a separate subnet for the ICAP connection.

You can also configure the VSE to separate the VSE network management traffic from the ICAP network traffic. The management interface is also used to connect to the Internet to check for virus signature and scan engine updates. If any spare network ports are available on the VSE server, the admin and Internet traffic can be split up.

Installing the VSE Virus Scanner

Make sure the server you use for the antivirus software installation is at the latest patch level for the installed OS. When a proxy server is needed to access an external web site, make sure the server is set up properly in the Windows Internet Options settings in the Control Panel using the following dialog window:

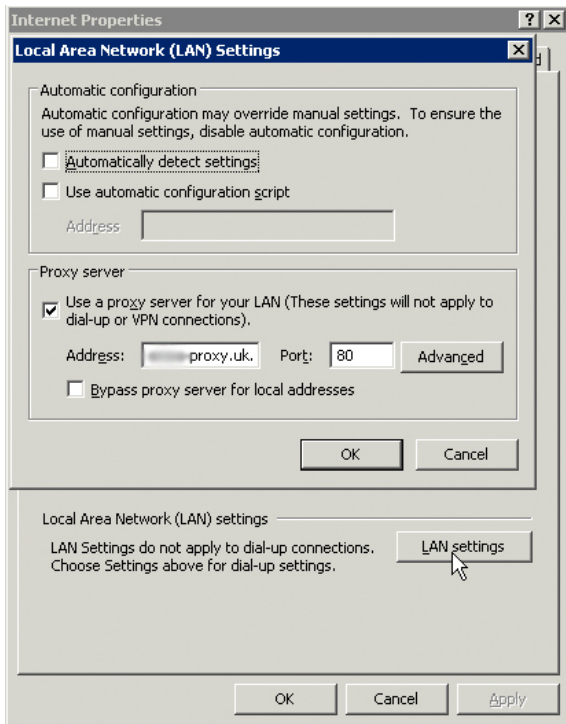


Figure 2. Internet proxy server setup

Install the required McAfee installation images on the Scan Server or Virtual Scan Server.

First, install the McAfee VSE package.

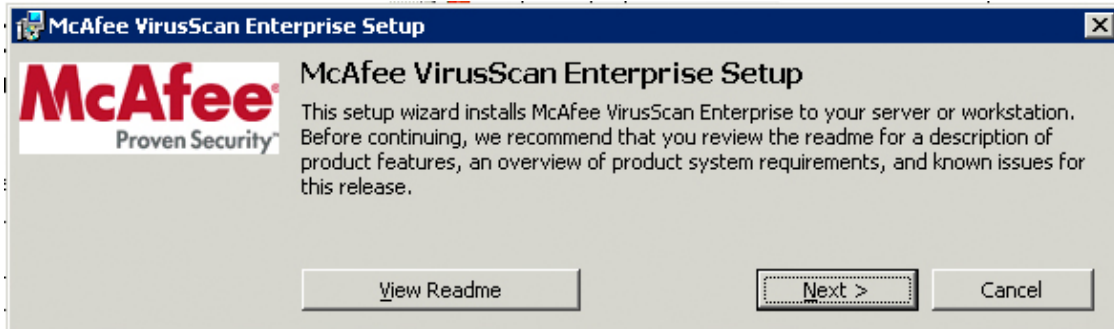


Figure 3. McAfee VSE setup window

The installation wizard will guide you through the installation of the McAfee VSE package.



Figure 4. McAfee VSE setup wizard

The next step is to install the McAfee VSESTOR component.

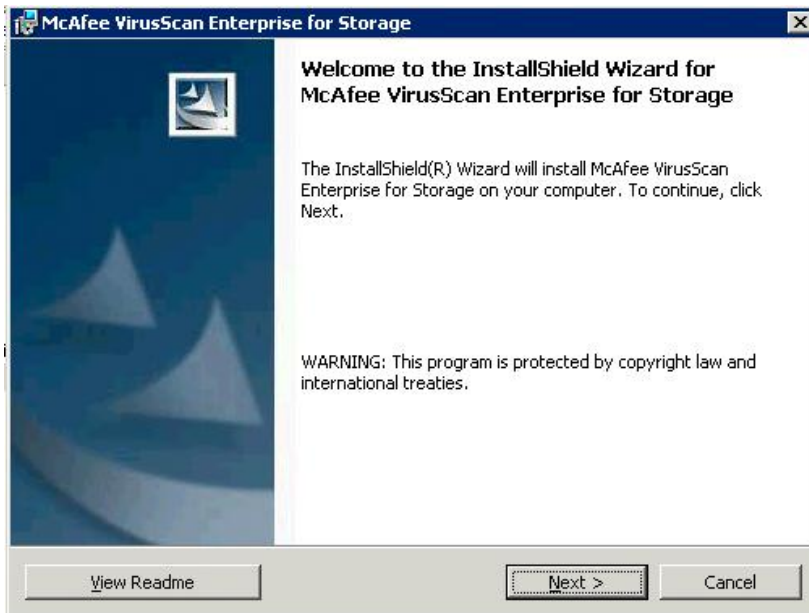


Figure 5. VSESTOR setup

Install any patches or hot fixes if required and finish the installation process by forcing an Update Now.

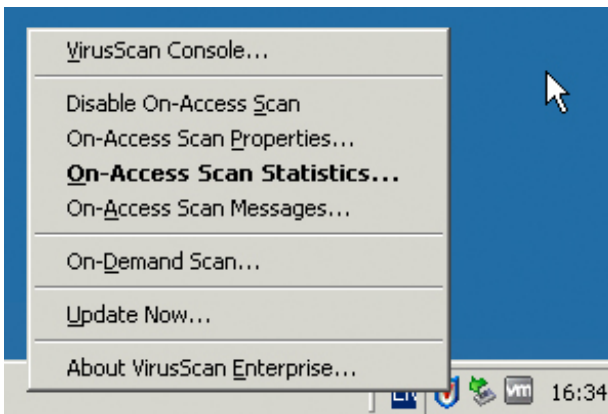


Figure 6. VSE Update Now activation

Select the VirusScan Console and verify that the update was successfully completed. For an ICAP only server, the tasks as shown in the next screenshot in the VirusScan Console utility must be enabled.

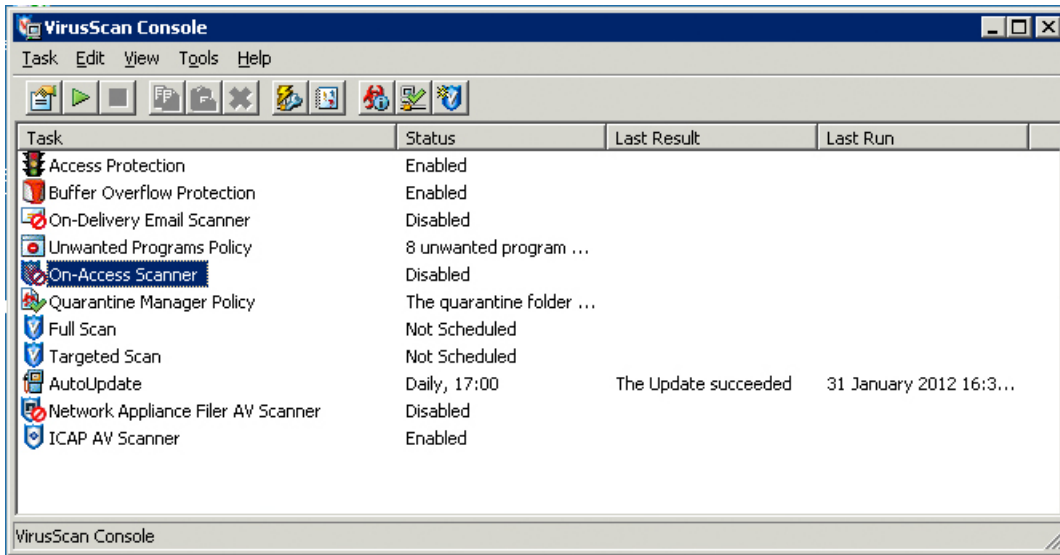


Figure 7. VirusScan Console window

Next, configure the ICAP AV Scanner for use with the Oracle ZFS Storage Appliance. You can restrict ICAP requests to the AV Scanner by specifying in the 'Connection List' window the IP address of the Oracle ZFS Storage Appliance Appliance allowed to send ICAP requests.

You must specify the AV Scanner's IP address in the ICAP Server 'Bind address' field in order for the ICAP Server to accept ICAP requests from ICAP clients. Use the port number as configured on the Oracle ZFS Storage Appliance.

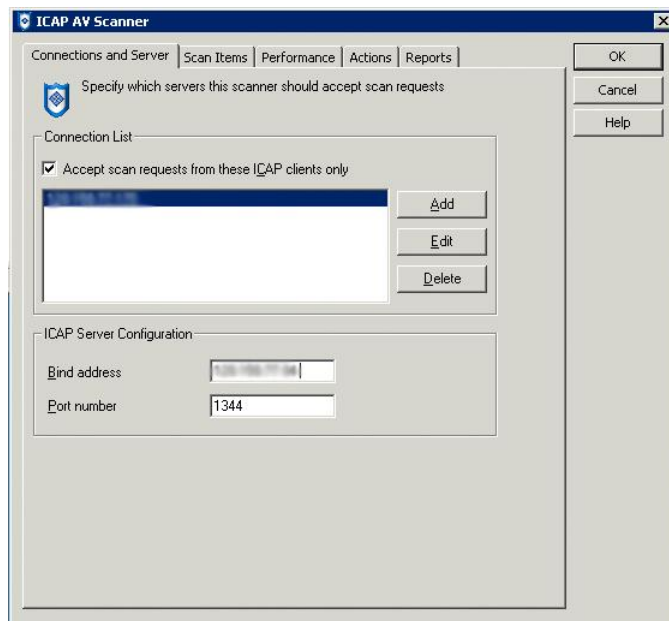


Figure 8. VSESTOR ICAP setup

Connecting the Oracle ZFS Storage Appliance to the Virus Scan Service

Now that the VSE scan engine is up and running, you can set up the Oracle ZFS Storage Appliance to connect to the scan engine through the ICAP interface. Navigate to the Virus Scan Service under Configuration>Services. Use the + button in front of Scanning Engines and specify the IP address and port number through which the VSE can be reached.

Under File Extensions, you can create a set of rules to scan or exclude a subset of files by the scan engine(s).

The screenshot displays the configuration page for the Virus Scan service. At the top, there are tabs for 'Services' and 'Virus Scan', along with 'Properties' and 'Logs' buttons. A 'Back to Services' link and a refresh icon are also present. The main content area is divided into several sections:

- Virus Scanning:** Contains instructions on how to configure virus scanning at the filesystem level. It includes a 'Maximum file size to scan' field set to '1 G' and a checked checkbox for 'Allow access to files that exceed maximum file size'.
- File Extensions:** A section for defining scan rules. It includes a table with columns for 'ACTION' and 'PATTERN'. The 'ACTION' dropdown is set to 'Scan' and the 'PATTERN' field contains an asterisk (*).
- Scanning Engines:** A table for configuring scan engines. It has columns for 'ENABLE', 'HOST', 'MAXIMUM CONNECTIONS', and 'PORT'. Two entries are shown, both with the 'ENABLE' checkbox checked, 'MAXIMUM CONNECTIONS' set to 32, and 'PORT' set to 1344.

Figure 9. Oracle ZFS Storage Appliance scan engine(s) through ICAP setup

The Oracle ZFS Storage Appliance is now ready to use the virus scan functionality. Use the virus scan checkbox in the Shares and/or Projects properties window to enable the function for the required Shares/Projects, as shown in the next section.

Verifying the Virus Scan Service Configuration

To verify the correct functioning of the virus scan service, you can use virus test files from the web site eicar.org. Copy those files onto a test machine you can use to access a share from the Oracle ZFS Storage Appliance that has been set up for testing.

Create a test CIFS/NFS share on the Oracle ZFS Storage Appliance and enable the **Virus scan** option for that share.

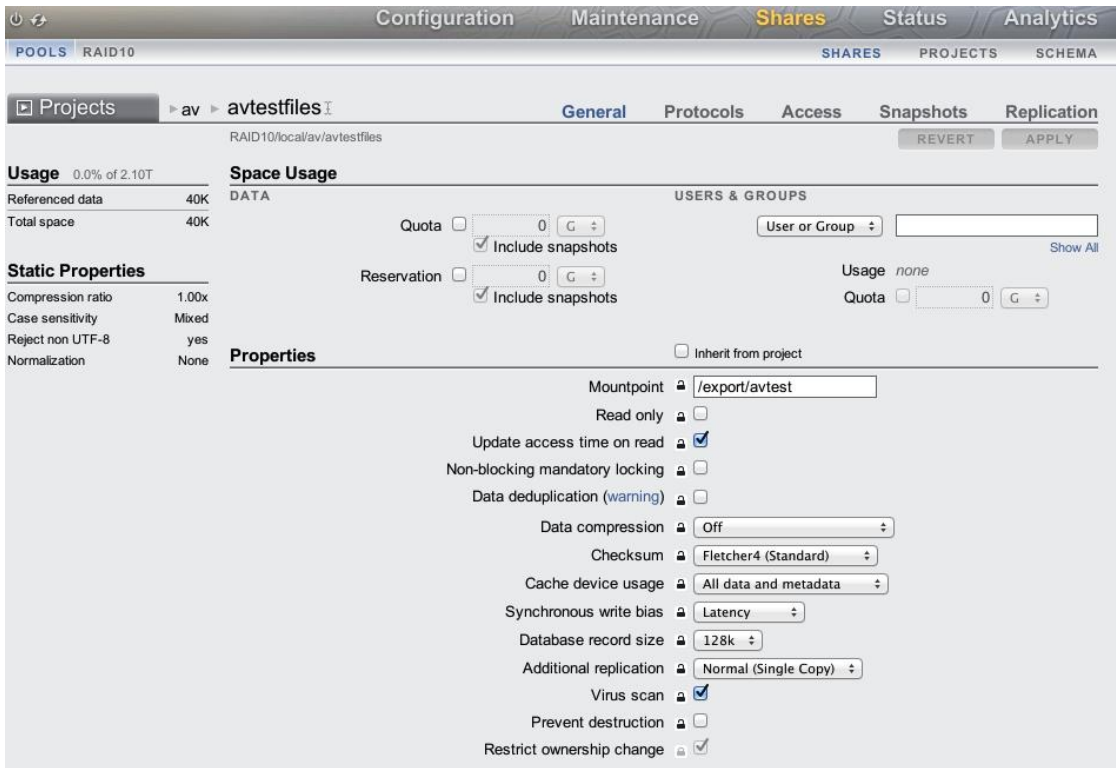


Figure 10. Oracle ZFS Storage Appliance share setup for virus protection

Set up the VSE scan software for maximum logging using the ICAP AV Scanner Reports options window.

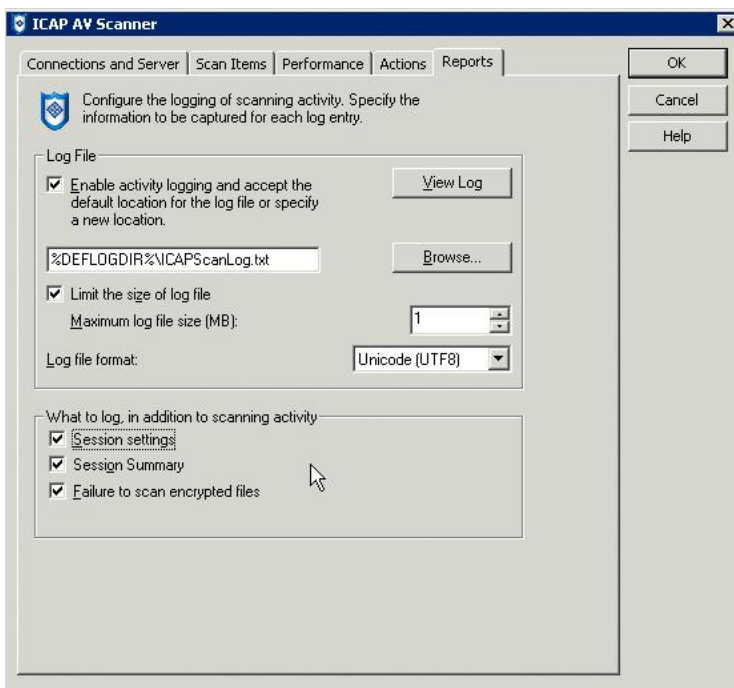


Figure 11. ICAP AV Scanner logging options

In normal operation mode it is not necessary to use the **Session settings** option.

Mount the share on a client you can use for copying the virus test files onto the share. Download the Eicar test files and copy those to a directory on the NFS share. Add one or more regular text files as well so you can see the difference in behavior in accessing infected files and non-infected files. After copying, try to access the files and observe that access to files detected as containing a virus is denied.

The following command line output shows the results of the test procedure on the NAS client.

```
root@edinburgh # ls
Eicar.org files
root@edinburgh # cp -R *files /av/avtest/testrun1
root@edinburgh # cd /av/avtest/testrun1/Eicar.org files
root@edinburgh # pwd
/av/avtest/testrun1/Eicar.org files
root@edinburgh # cat * >/dev/null
cat: cannot open eicar_com.zip
cat: cannot open eicar.com
cat: cannot open eicar.com.txt
cat: cannot open eicarcom2.zip
root@edinburgh # ls -l
total 10
-rwxr-xr-x+ 1 nobody  nobody      184 Oct 20 18:05 eicar_com.zip
-rwxr-xr-x+ 1 nobody  nobody       68 Oct 20 18:06 eicar.com
-rwxr-xr-x+ 1 nobody  nobody       68 Oct 20 18:04 eicar.com.txt
-rwxr-xr-x+ 1 nobody  nobody      308 Oct 20 17:58 eicarcom2.zip
-rwxr-xr-x+ 1 nobody  nobody       63 Oct 20 17:42 website.txt.txt
```

root@edinburgh #

Next, check the file `ICAPScanLog.txt` of the VSE to see if the files containing viruses were detected. You can easily retrieve this file using the **View Log** option in the ICAP AV Scanner, **Reports** option, as shown earlier.

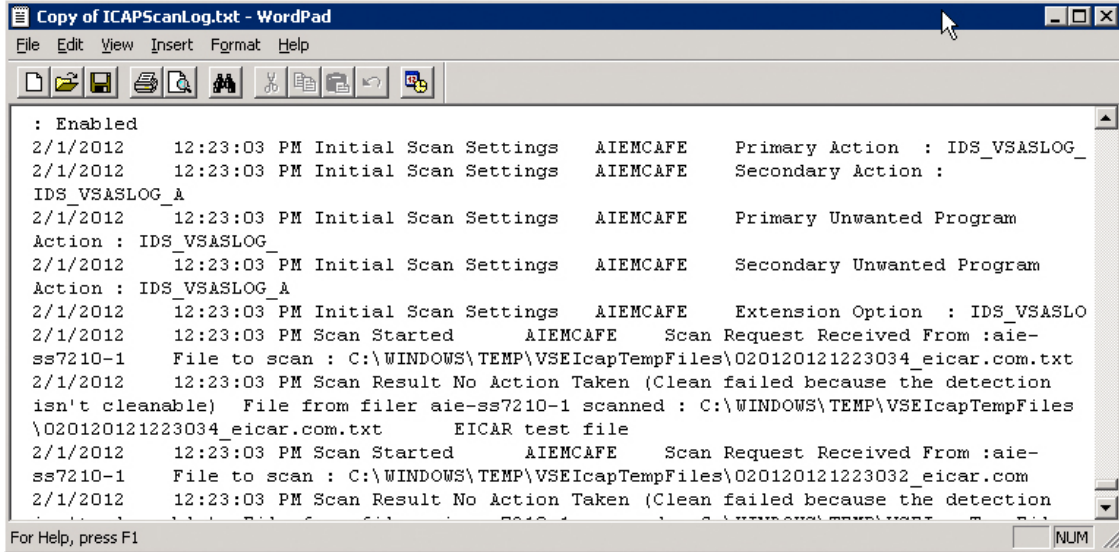


Figure 12. ICAP Scan logging example

Errors are also logged in the Windows Event Viewer under Applications.

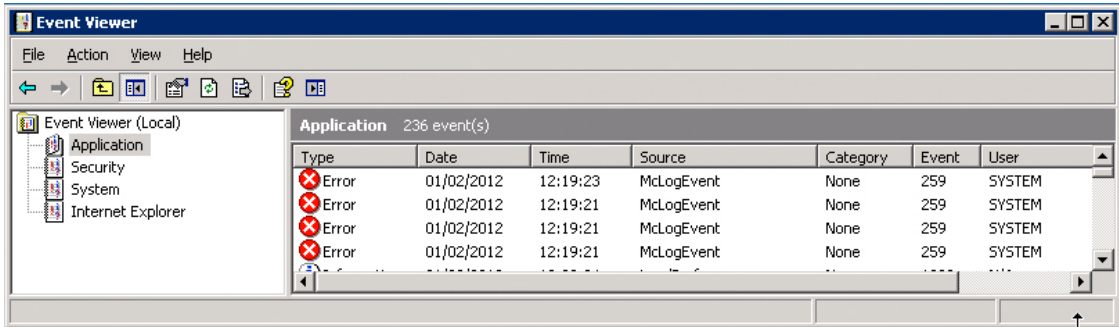
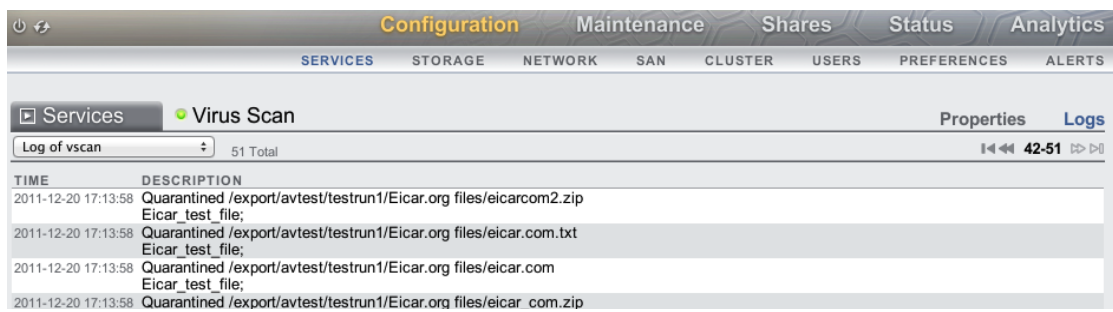


Figure 13. Windows Application event logging showing AV detection

The Oracle ZFS Storage Appliance also can be checked for reported infected files using the Logs option in the Virus Scan Services information window. Select the **Log of vscan** option to verify that the test files copied onto the NFS share have been reported here too.



TIME	DESCRIPTION
2011-12-20 17:13:58	Quarantined /export/avtest/testrun1/Eicar.org files/eicarcom2.zip Eicar_test_file;
2011-12-20 17:13:58	Quarantined /export/avtest/testrun1/Eicar.org files/eicar.com.txt Eicar_test_file;
2011-12-20 17:13:58	Quarantined /export/avtest/testrun1/Eicar.org files/eicar.com Eicar_test_file;
2011-12-20 17:13:58	Quarantined /export/avtest/testrun1/Eicar.org files/eicar_com.zip

Figure 14. Oracle ZFS Storage Appliance virus scan logs

Configuration Best Practices

Note the following file handling cases and consider the recommended settings for managing them.

Handling Archive Type Files

Methods for handling mime and zip archive type files require special consideration, as virus threats can hide in compressed files that are part of the archive file. Viruses can only be detected by unpacking the archives and scanning the individual files in the archives for the viruses' presence.

You can wait for a user to unpack an archive file and let the virus scanner pick up the threat at that time. Otherwise, you can set the virus scanner to unpack the file as soon as it is added to a file system, but this prevents the zip file from being further copied in an organization's infrastructure. This approach imposes an extra load on the virus scanner and can only handle archives that are not password protected or encrypted. Thus, you should note that enabling scanning of zip files contents is not a 100% reliable method for detecting a virus threat in files within an archive file.

McAfee VSE can manage both archive scan approaches; when an immediate archive scan is required, it can be configured. To make sure zip-type archive files and MIME Decoded files are also processed by the AV Scanner, include them in the file types to scan.

Use the ICAP AV Scanner Scan Items tab to specify the **Decode Mime encoded files** and **Scan inside archives** options.

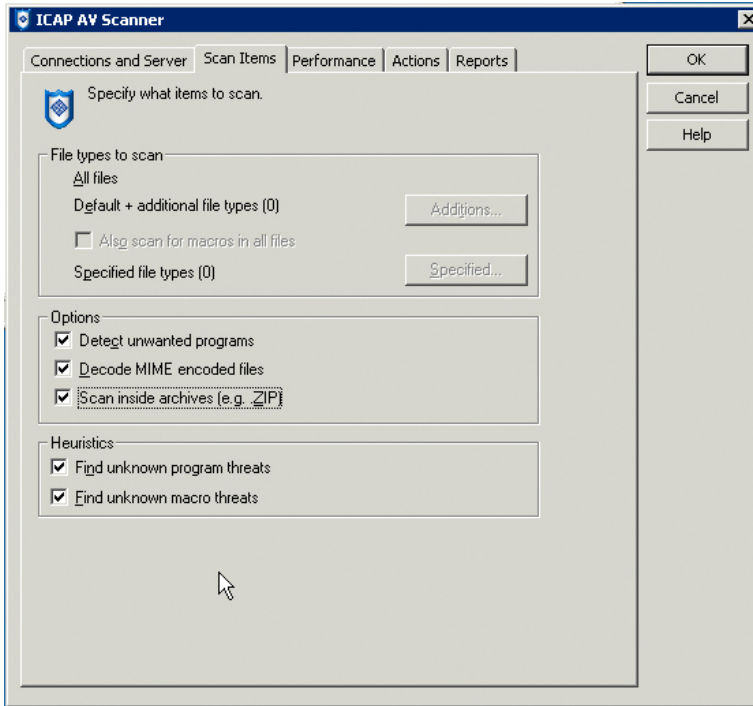


Figure 15. ICAP AV Scanner, file type selections

Disabling the File Repair Option

The Oracle ZFS Storage Appliance always quarantines a file if a virus has been detected in it. To prevent the McAfee VirusScan from executing any repair actions on the file, set up the scan engine to continue scanning instead of repairing/replacing a file.

Use the ICAP AV Scanner Actions tab to specify the **Continue scanning** option.

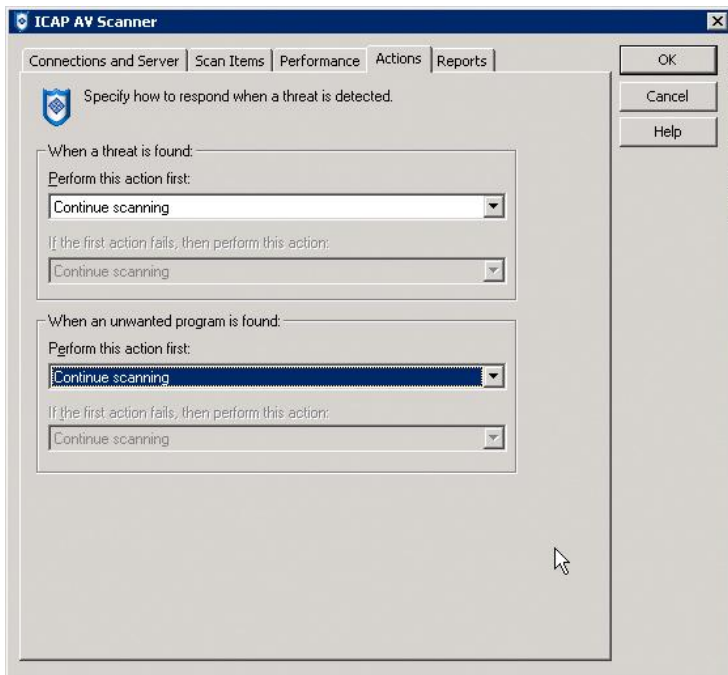


Figure 16. ICAP AV Scanner, specifying virus detect only

Synchronizing System Time

It is a best practice to keep the time between the Oracle ZFS Storage Appliance and the VSE server in sync with each other so that logging information can be easily cross-referenced when needed. A simple way to do this is to configure the use of NTP (Network Time Protocol) for both the Oracle ZFS Storage Appliance and the VSE server.

Conclusion

Using McAfee VirusScan antivirus product suite with the Oracle ZFS Storage Appliance provides a scalable and reliable virus scanning solution for protecting valuable data stored on network attached storage devices. With this solution, you can offload the burden of scanning the files from the Oracle ZFS Storage Appliance onto an external antivirus scanning platform, thereby maximizing the workload capability on the Oracle ZFS Storage Appliance, while taking advantage of the expertise embedded in the McAfee VirusScan Enterprise antivirus solution to perform scanning of files for worms, viruses, and Trojan horse threats.

Additionally, this solution takes advantage of the VSCAN virus scanning service integrated into the Oracle ZFS Storage Appliance to manage quarantining of files based on scan results from the McAfee VirusScan antivirus platform.

This antivirus solution has been qualified by Oracle to detect viruses, worms, and Trojan horses in files of all major file types, including mobile code and compressed file formats, ensuring fast virus resolution to reduce the risk of financial, data, and productivity loss.

Appendix: References

NOTE: References to Sun ZFS Storage Appliance, Sun ZFS Storage 7000, and ZFS Storage Appliance all refer to the same family of Oracle ZFS Storage Appliance products. Some cited documentation or screen code may still carry these legacy naming conventions.

- Oracle ZFS Storage Appliance documentation, including administration guide
<http://www.oracle.com/technetwork/documentation/oracle-unified-ss-193371.html>
- The *Sun ZFS Storage Appliance Administration Guide* is also available through the Oracle ZFS Storage Appliance online help context. The Help function in Oracle ZFS Storage Appliance can be accessed through the browser user interface.
- Oracle ZFS Storage Appliance white papers, solutions briefs, and implementation aids
<http://www.oracle.com/technetwork/server-storage/sun-unified-storage/documentation/index.html>
- Oracle ZFS Storage Appliance product information
<http://www.oracle.com/us/products/servers-storage/storage/nas/overview/index.html>
- McAfee VirusScan Enterprise for Storage, product guide and documentation
<http://www.mcafee.com>
- [Oracle VM VirtualBox](http://www.oracle.com/technetwork/server-storage/virtualbox/overview/index.html)
<http://www.oracle.com/technetwork/server-storage/virtualbox/overview/index.html>
- Oracle VM Server
<http://www.oracle.com/us/technologies/virtualization/oraclevm/index.html>



How to Configure McAfee VirusScan Enterprise
for the Oracle ZFS Storage Appliance
January 2014, Version 2.0
Author: Peter Brouwer
Contributing Author: Thomas Hanvey

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0611

Hardware and Software, Engineered to Work Together