An Oracle Technical White Paper
January 2014

How to Configure Symantec Protection Engine for Network Attached Storage for the Oracle ZFS Storage Appliance

ORACLE

Table of Contents

Table of Figures

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 Symantec Protection Engine for Network-Attached Storage software as the external virus scanning engine.

Symantec Protection Engine for Network-Attached Storage (SPE for NAS) scan engine analyzes any files in question for suspicious patterns and passes the scan results back to the VSCAN service of the Oracle ZFS Storage Appliance. 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 [Common Internet File System] or NFS [Network File System]).

This document describes the installation and configuration of Symantec Protection Engine for Network-Attached Storage for use as a virus scan engine with the Oracle ZFS Storage Appliance VSCAN service.

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, SPE for NAS, or simply SPE, 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 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 NSF v4 or CIFS protocol.

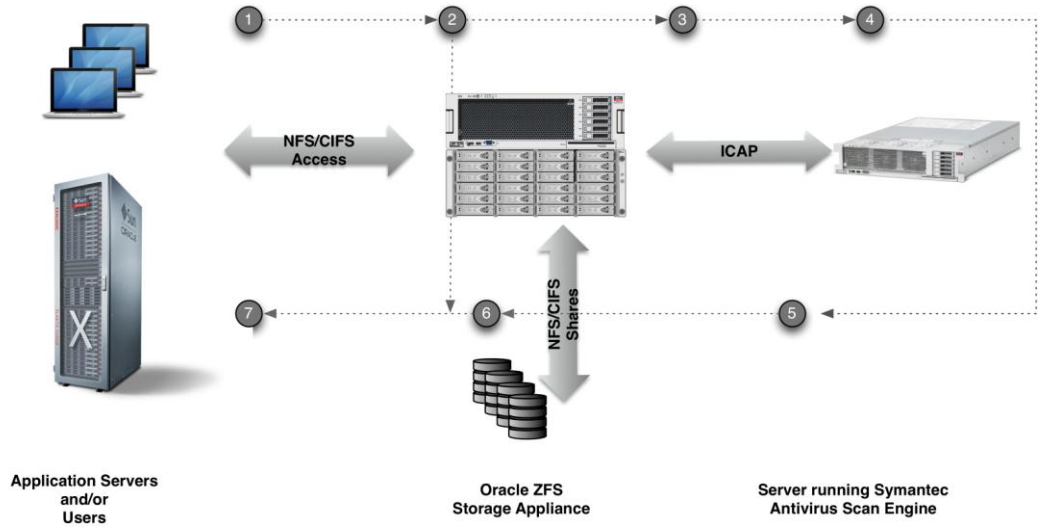

Figure 1. File virus scan steps

The following sequence of steps takes place when a file is accessed/created by a client on an NFS/CIFS file share while using the Symantec antivirus scan engine (SPE):

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 (so the following steps are not required).

3. If the file needs to be scanned; a scan request is issued to the SPE for NAS.
4. The SPE scan engine scans the file.
5. The SPE 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 SPE 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 'Scan Only'. These settings will be shown later in this paper in the Best Practices section.
6. The Oracle ZFS Storage Appliance takes one of the following actions, depending on the SPE scan engine response listed in step 5:
   a) corresponding to result a: File stored/read.
   b) corresponding to result b: av_quarantined set in ESA to deny further client access.
   c) corresponding to result c: av_quarantined 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:
   a) corresponding to result a: Client access is allowed.
   b) corresponding to result b: Client access is denied.
   c) corresponding to result c: Client access is denied.

Note: As mentioned earlier, using NSF v3 will not trigger scan requests. However, files marked as infected cannot be accessed over NFS v3.

Installing Symantec Protection Engine for NAS and Configuring the Oracle ZFS Storage Appliance

The Symantec Protection Engine for Network-Attached Storage (SPE for NAS) software contains the Symantec scan engine that is integrated with a module to communicate with network attached storage devices.

The SPE for NAS package is supported on Oracle Solaris SPARC platforms, as well as various Linux and Microsoft Windows platforms. For this paper, a virtual machine running Windows 2003 Server is used as the antivirus scan server.

The SPE for NAS package contains the antivirus scanning engine and a Web console that allows users to configure, monitor, and set maintenance functions for the AV scanning environment. The SPE for NAS component's ICAP protocol option handles the interface between the Oracle ZFS Storage Appliance and the SPE for NAS antivirus scan engine.

The software can be installed on both virtual environments, like Oracle VM Server and Oracle VM 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 SPE for NAS has been used.

You can find the installation images using the 'Trialware' option on the Symantec web site's Symantec Protection Engine for Network-Attached Storage product pages.

Deployment of the SPE for NAS Scanner Appliance

Ensure that you have met the following prerequisites before deploying the Symantec Protection engine software on the Oracle ZFS Storage Appliance.

Prerequisites

- 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 *Symantec Protection Engine for Network-Attached Storage Getting Started Guide* and the *Symantec Protection Engine for Network-Attached Storage Implementation Guide* available at the Symantec web site.
- Download the Symantec SPE for NAS package for the relevant platform.
- Verify that the hardware requirements for the Symantec SPE for NAS product meet your (virtual) hardware platform specs.

- In case a corporate proxy server is required for Internet access to Symantec's update server, verify support for virus update requests from your machine using the proxy server to Symantec's update server.
- Verify web browser access to the Oracle ZFS Storage Appliance and the SPE for NAS scan engine.
- Verify that shares on the Oracle ZFS Storage Appliance you plan to protect are using either CIFS or NFS v4 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 SPE for NAS server using port 1344 pass-through.

Planning Network Topology

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

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 impacting data I/O performance between Oracle ZFS Storage Appliance and clients, use a separate subnet for the ICAP connection.

Installing the SPE for NAS Virus Scanner

Make sure the server you use for the antivirus software installation is at the latest patch level for the installed operating system. 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:

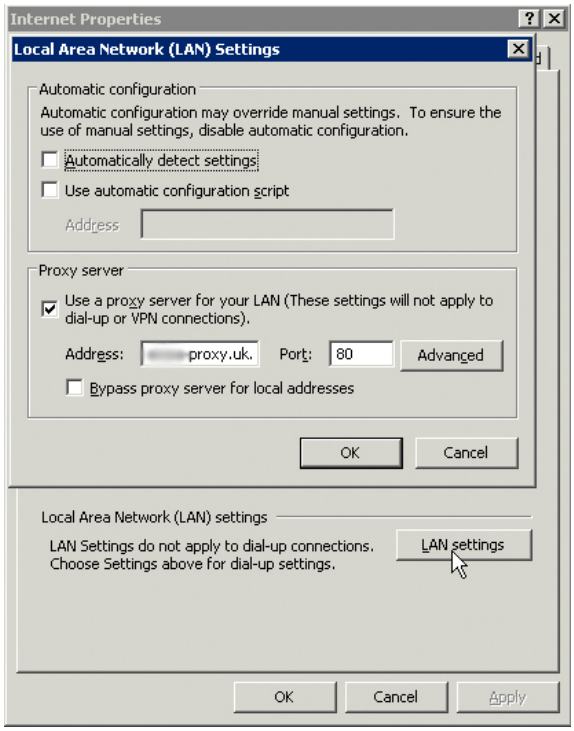

Figure 2. Internet proxy server setup in Windows

Install the Symantec SPE for NAS package.

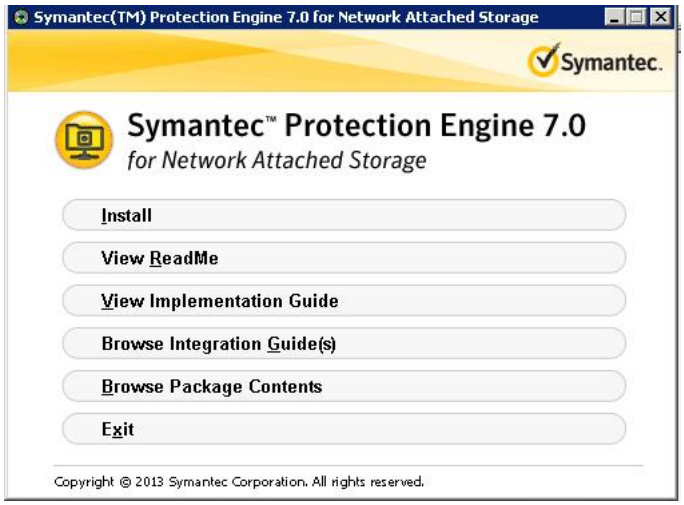

Figure 3. Symantec SPE for NAS setup window to initiate installation

The installation wizard will guide you through the installation of the Symantec SPE for NAS package.

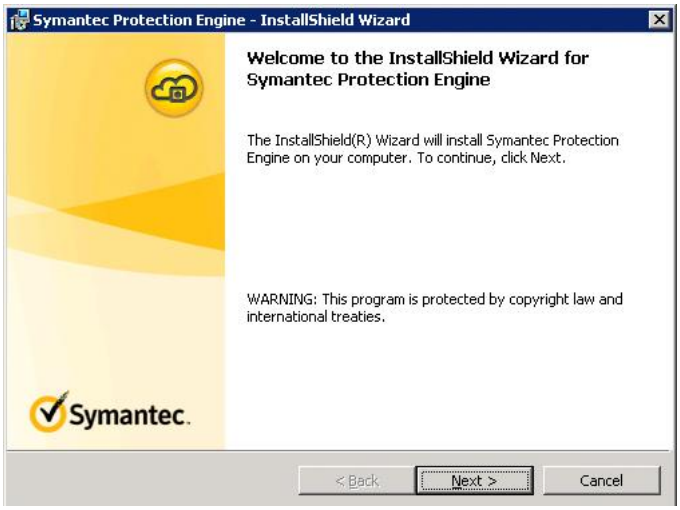

Figure 4. Symantec SPE for NAS setup wizard

Use Symantec's LiveUpdate option from the SPE WebConsole to make sure the latest virus definitions and patches are loaded.

Bring up the VirusScan WebConsole using the URL https://localhost:8004 (note the https) and verify that the update was successfully completed.

The next step is to configure the ICAP SPE scanner for use with the Oracle ZFS Storage Appliance. By default, SPE binds to all interfaces. Selecting 127.0.0.1 for the Bind address option in the following Web Console window disables external ICAP access requests. Verify that the ICAP option is selected as Communication Protocol, as shown in this screenshot. Also select **Scan only** for the Scan policy.

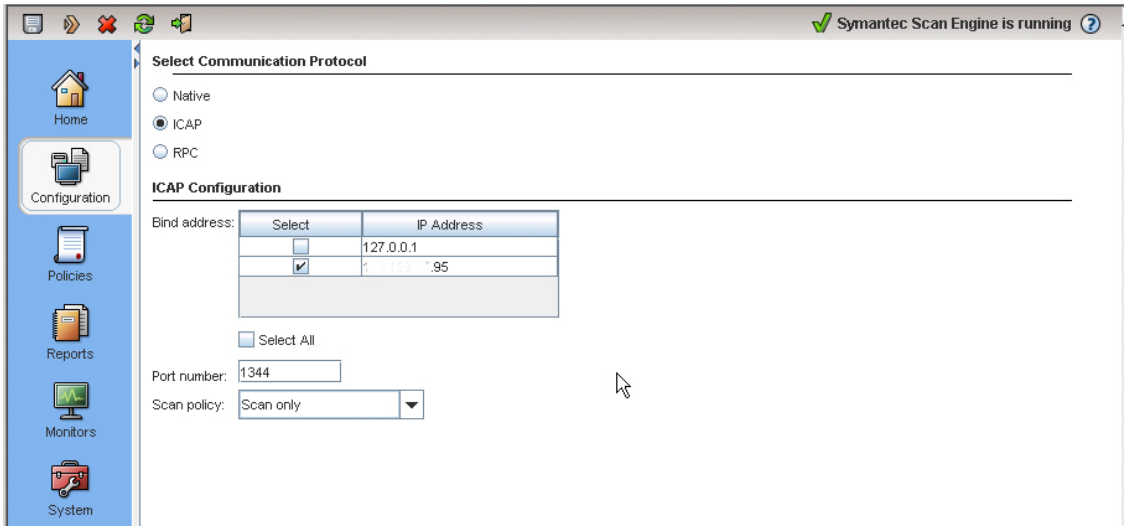

Figure 5. Symantec Scan Engine configuration in Web Console

Connecting the Oracle ZFS Storage Appliance to the Virus Scan Service

Now that the SPE for NAS 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 SPE for NAS 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).

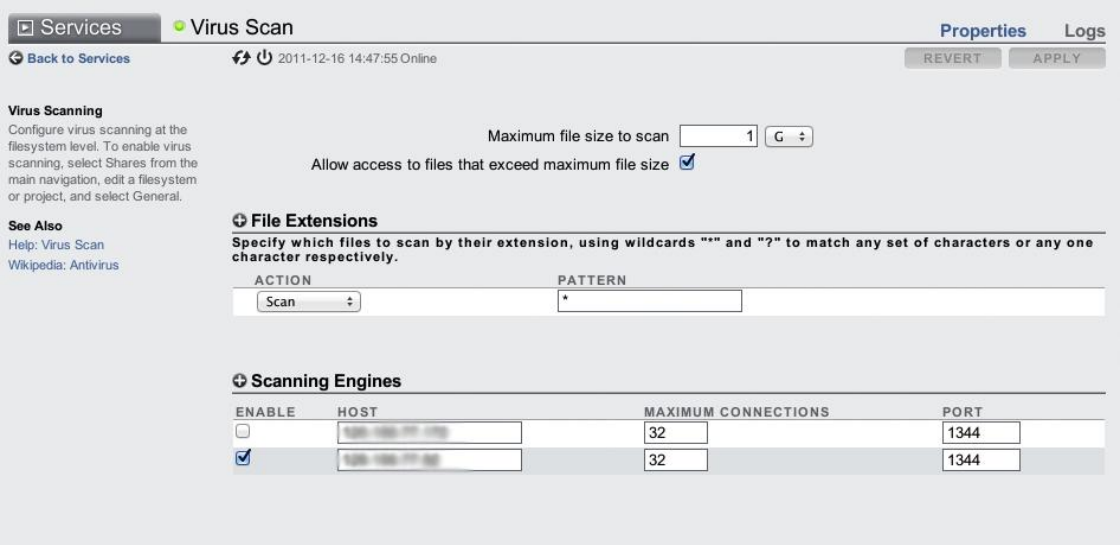

Figure 6. Oracle ZFS Storage Appliance scan engine(s) through ICAP setup

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.

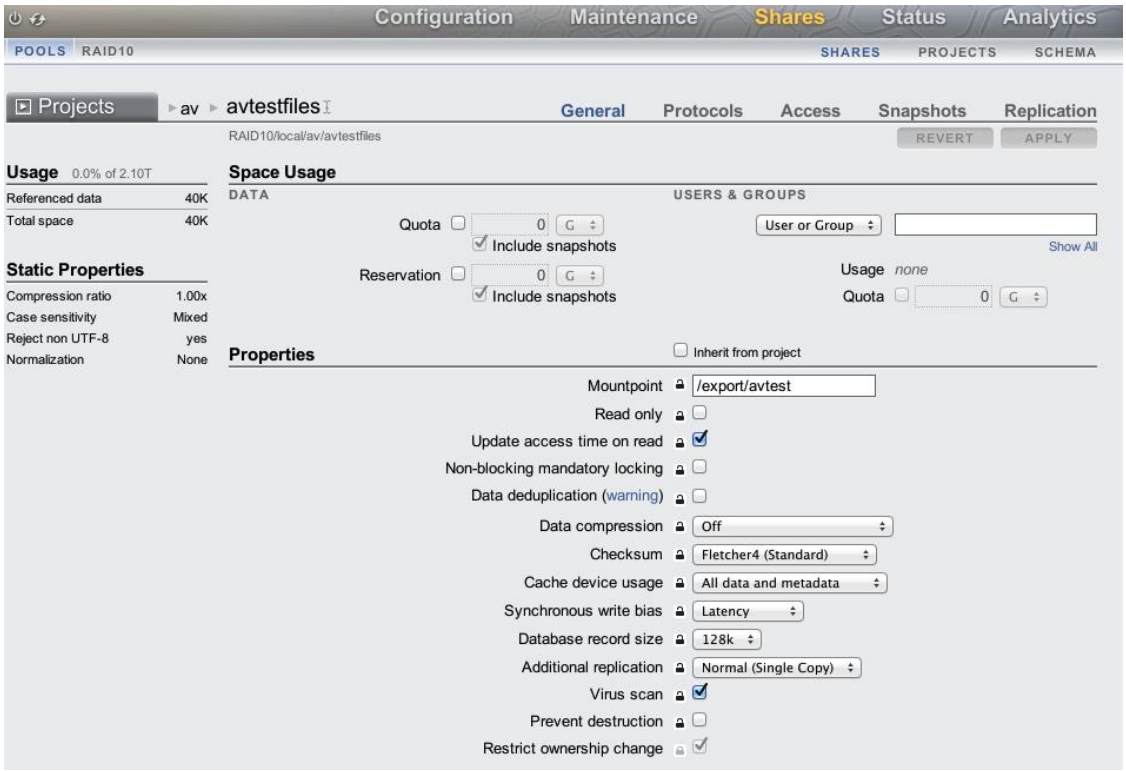

Figure 7. Oracle ZFS Storage Appliance share setup for virus protection

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/CIFS 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 status of the SPE scanner to see if the files containing viruses were detected.

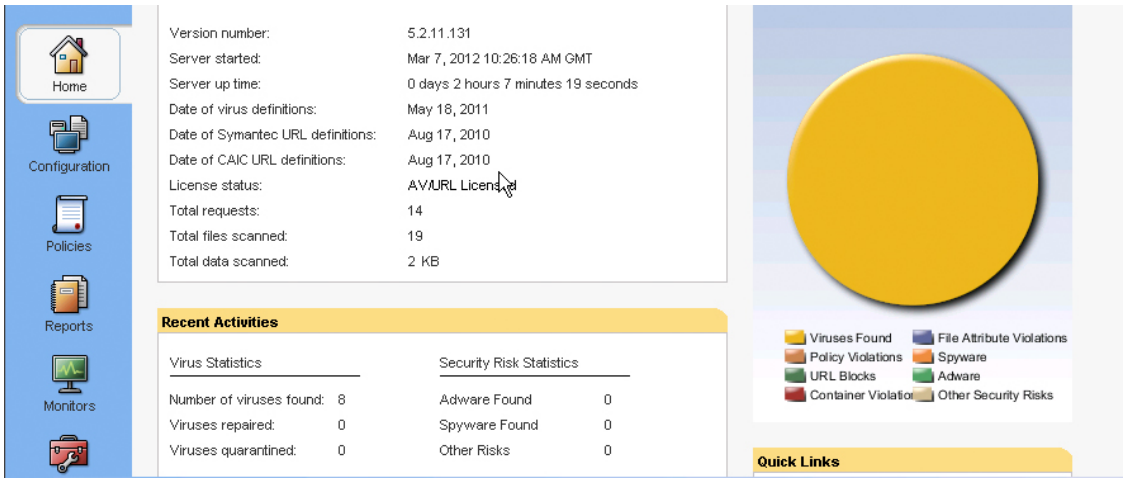

Figure 8. SPE scanner status showing found viruses

In the Reports option tab, use the Generate Report option under Tasks to receive detailed information on the found viruses.

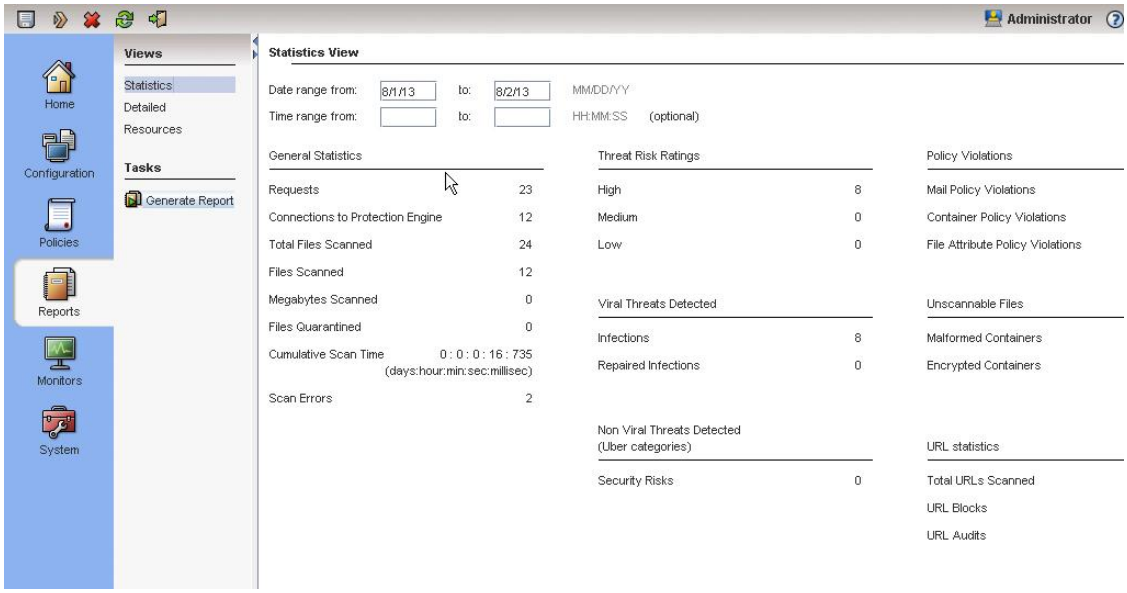

Figure 9. Virus detection reporting from the SPE scanner

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.

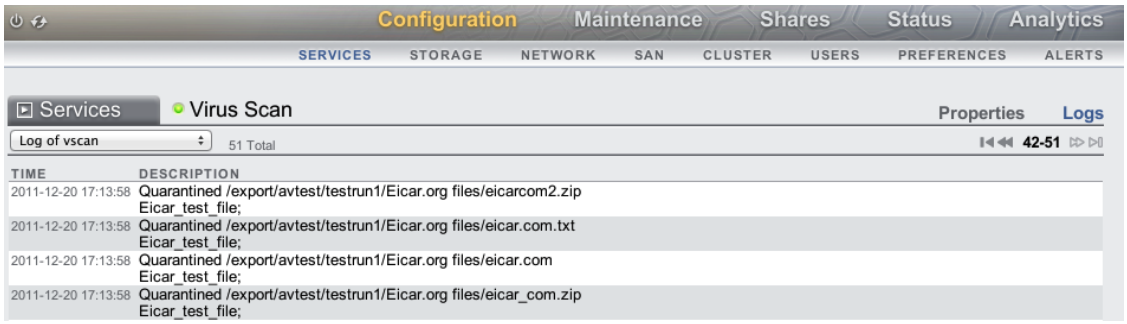

Figure 10. Virus scan logs in the Oracle ZFS Storage Appliance BUI

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.

Symantec Protection Engine for NAS can manage both archive scan approaches; its default is to scan all file types. You can configure it to exclude archive type files by setting up exclusions in the Policies window. Best practice, however, is to use the file exclusion option within the Oracle ZFS Storage Appliance, because it spares the need for issuing a scan request to the SPE scan engine.

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 SPE for NAS from executing any repair actions on the file, set up the scan engine to scan only instead of repairing/deleting a file. Under ICAP Configuration, set Scan policy to **Scan only**.

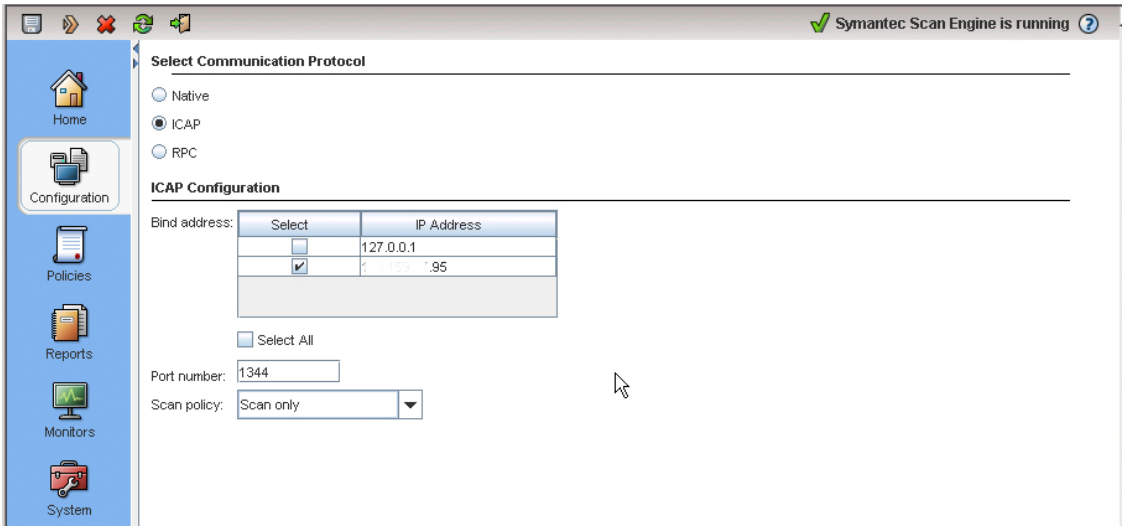

Figure 11. SPE for NAS Scanner, specifying scan only

Synchronizing System Time

It is a best practice to keep the time between the Oracle ZFS Storage Appliance and the SPE for NAS 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 SPE for NAS server.

Conclusion

Using Symantec Protection Engine for Network Attached Storage 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 Symantec Protection Engine for Network-Attached Storage solution to perform scanning of files.

Additionally, this solution takes advantage of the integrated VSCAN virus scanning service of the Oracle ZFS Storage Appliance to manage file quarantining based on scan results from the Symantec Protection Engine for Network Attached Storage engine.

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 product documentation
  http://www.oracle.com/technetwork/documentation/oracle-unified-ss-193371.html
- The Sun *ZFS Storage Appliance Administration Guide* is available through the Oracle ZFS Storage Appliance help context.
  The Help function in Oracle ZFS Storage Appliance can be accessed through the browser user interface.
- Oracle ZFS Storage Appliance Product Information
  http://www.oracle.com/us/products/servers-storage/storage/nas/overview/index.html
- Product Wiki Pages
  https://wikis.oracle.com/display/FishWorks/Fishworks
- Symantec Protection Engine for Network-Attached Storage Product Guide and documentation, including:
  - Symantec Protection Engine for Network-Attached Storage Getting Started Guide
  - Symantec Protection Engine for Network Attached Storage 7.0 Release Notes
  - Symantec Protection Engine for Network-Attached Storage Implementation Guide
  - Oracle VM VirtualBox
    http://www.oracle.com/technetwork/serverstorage/virtualbox/overview/index.html
  - Oracle VM Server
    http://www.oracle.com/us/technologies/virtualization/oraclevm/index.html

How to Configure Symantec Protection Engine for Network Attached Storage 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

Hardware and Software, Engineered to Work Together