ORACLE

ZFS STORAGE APPLIANCE

An Oracle Technical White Paper
January 2014

How to Configure Sophos Endpoint Protection 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 Sophos Endpoint Protection software as the external virus scanning engine.

Sophos Endpoint Protection 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 [Common Internet File System] or NFS [Network File System]).

This document describes the installation and configuration of Sophos Endpoint Protection 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, Sophos Endpoint Protection 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.

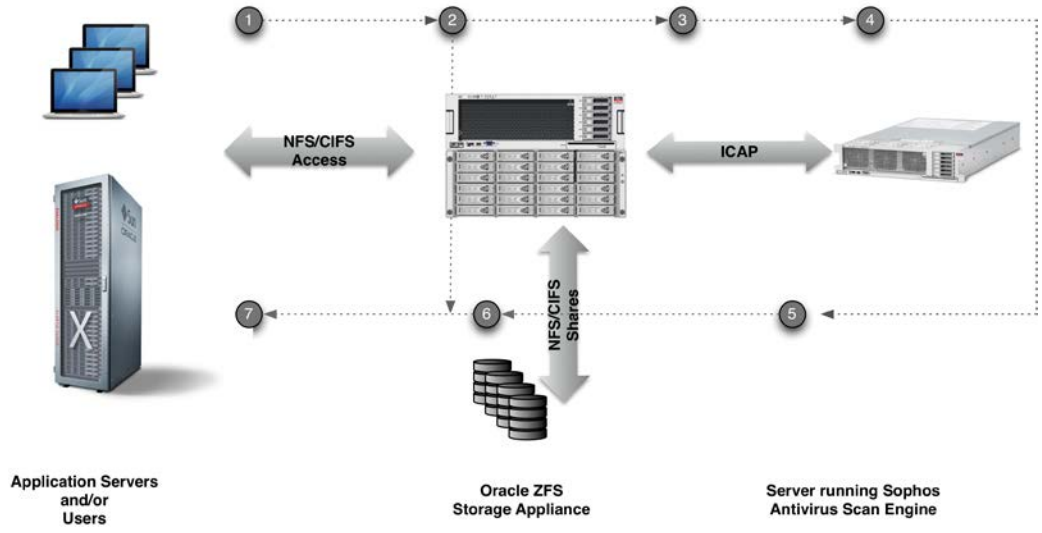

Figure 1. File virus scan steps

The following sequence of steps is followed when a file is accessed/created by a client on an NFS v4/CIFS file share when using the Sophos 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 (so the following steps are not required).

3. If the file needs to be scanned; a scan request is issued to the SESC.
4. The SESC scan engine scans the file.
5. The SESC scan engine responds back to the Oracle ZFS Storage Appliance with one of the following results:
   a) File OK.
   b) Virus found; file quarantined.
6. The Oracle ZFS Storage Appliance takes one of the following actions, depending on the SESC response:
   a) File stored/read.
   b) av_quarantined set in ESA to deny further client access.
7. The Oracle ZFS Storage Appliance responds, for the associated action, to the client:
   a) Client access is allowed.
   b) Client access is denied.

Note: As mentioned earlier, using NSFv3 will not trigger scan requests. However, files marked as infected cannot be accessed over NFSv3.

Installing SESC and Configuring the Oracle ZFS Storage Appliance

The Sophos Endpoint Protection product suite contains Sophos Endpoint Security and Control (SESC), used in combination with the Sophos Antivirus Dynamic Interface (SAVDI) to create an antivirus scanning solution for the Oracle ZFS Storage Appliance.

The SESC and SAVDI components are supported on various platforms. The SESC component is located in the Standalone install package option, with specific versions for different operating system platforms. The SADV component is located in the Anti-Virus for Network Storage package; select the Oracle platform version.

For this paper, a machine running Microsoft Windows 2003 Server is used.

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

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 SESC has been used.

You can find the installation images on the Sophos web site's Endpoint Protection pages. Sophos Endpoint Protection is also referred to as Sophos Endpoint Security and Control.

Deployment of the SESC and SAVDI Software

Ensure that you have met the following prerequisites before deploying the Sophos Endpoint Protection 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 A: References).
- Download and study the *Sophos Endpoint Security and Control* documentation and the *Sophos SAVDI Quick Start Guide* available at the Sophos web site.
- Download the Endpoint Security and SAVDI packages for the required platform.
- Verify that the hardware requirements for the SESC and SAVDI packages meet your (virtual) hardware platform specs.
- In case a corporate proxy server is required for Internet access to Sophos, verify support for virus update requests from your machine using the proxy server to Sophos.
- 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 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 SESC 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 SESC. A minimal configuration requires one network connection to the Oracle ZFS Storage Appliance and one network connection to the SESC. 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 SESC.

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 SESC to separate the SESC 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 SESC server, the admin and Internet traffic can be split up.

Installing the SESC Virus Scanner

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

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

First, install the SESC package.

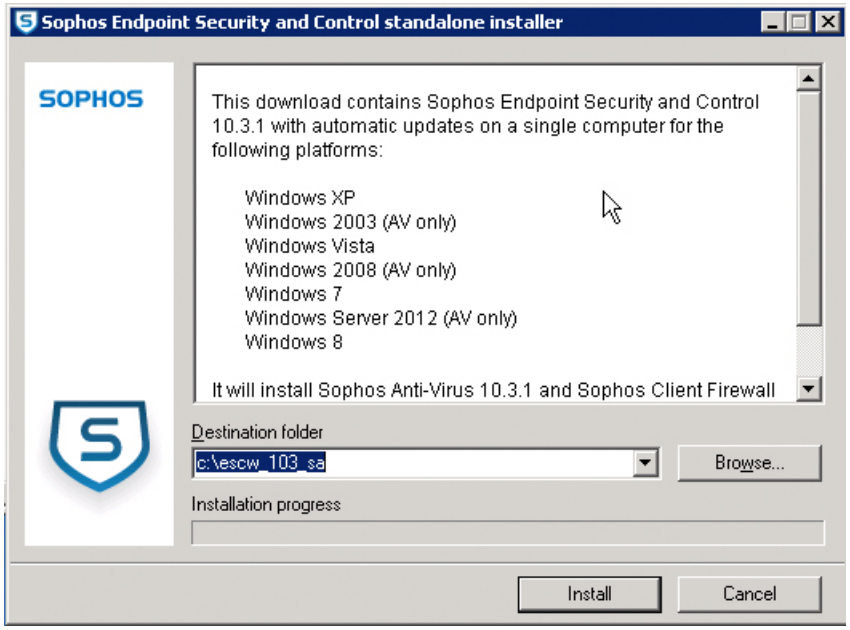

Figure 2. SESC standalone installer

The installation wizard will guide you through the installation of the SESC package and the Sophos Autoupdate package.

Figure 3. SESC installation wizard

Enter the Sophos provided license login credentials.

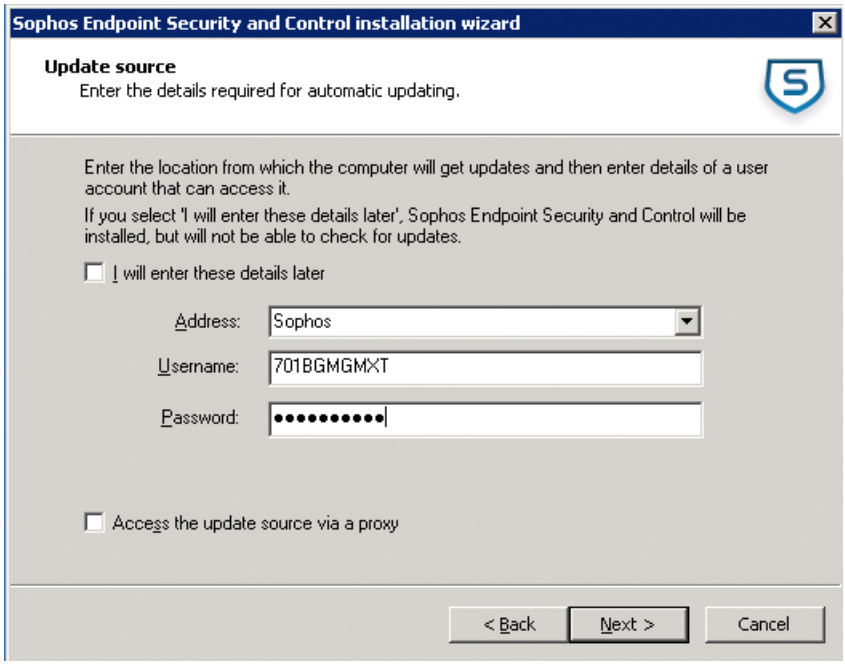

Figure 4. Entering the Sophos license login credentials

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:

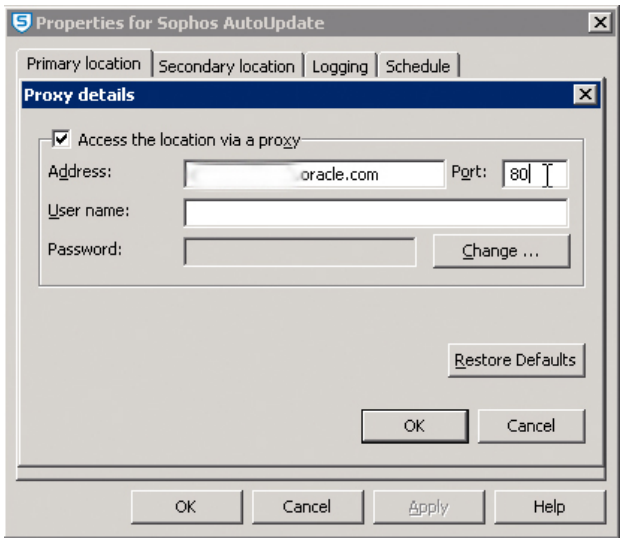

Figure 5. Specifying proxy information for Sophos auto-update

The next step is to install the SAVDI component.

Figure 6. SAVDI component installation using the setup wizard

Once the installation completes, you can test the Internet connection used by the auto-update function of the SESC by requesting a virus signature file update using 'Update now', as seen in the following screen menu option.

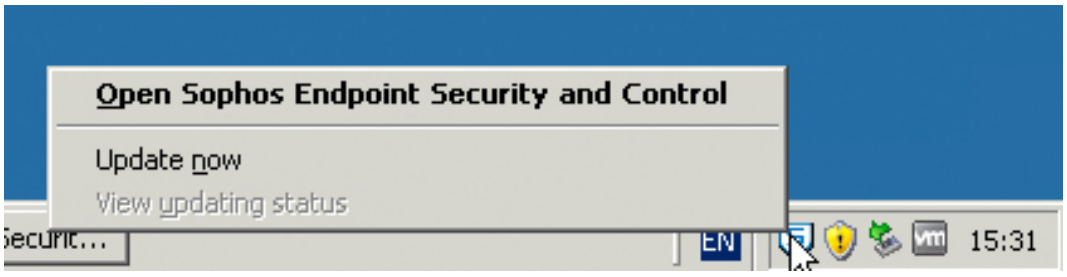

Figure 7. SESC Update Now activation

At the end of the installation process, the SESC shows the current status of the antivirus scan environment.

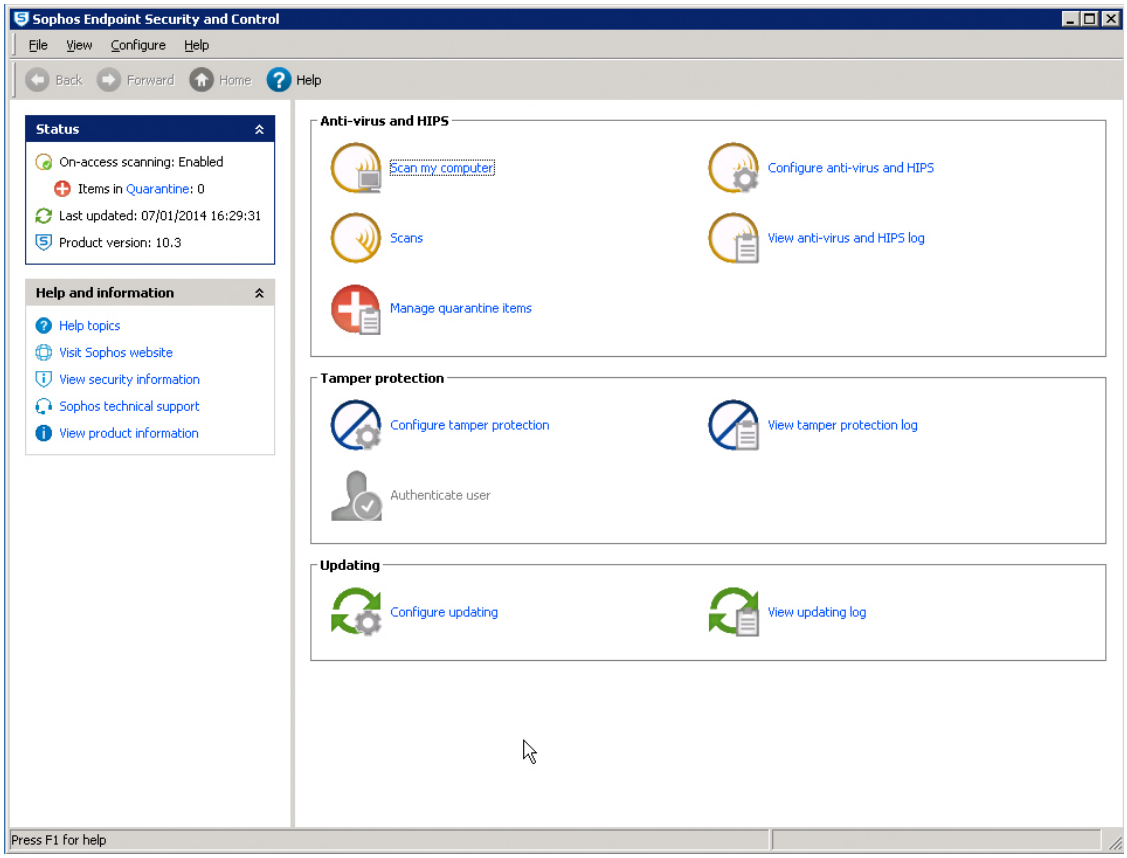

Figure 8. SESC scanning status screen

Note that ‘Items in Quarantine' in the Status section of the console shows the files quarantined by the scan engine on the local server, not files quarantined through the SAVDI interface. See the chapter “Verifying the Virus Scan Server Configuration” for how to monitor virus detection through SAVDI/ICAP on the Oracle ZFS Storage Appliance.

Connecting the Oracle ZFS Storage Appliance to the Virus Scan Service

Now that the SESC 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 SESC can be reached.

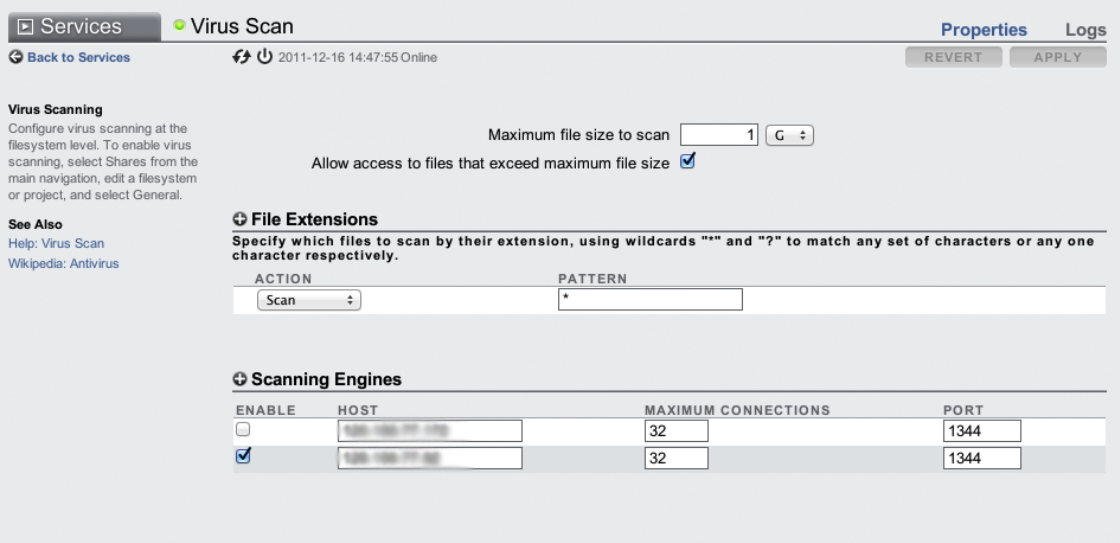

Figure 9. Oracle ZFS Storage Appliance scan engine(s) through ICAP

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

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. For a reference, use the SAVDI ICAP test guide in the Sophos SAV Dynamic Interface.

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

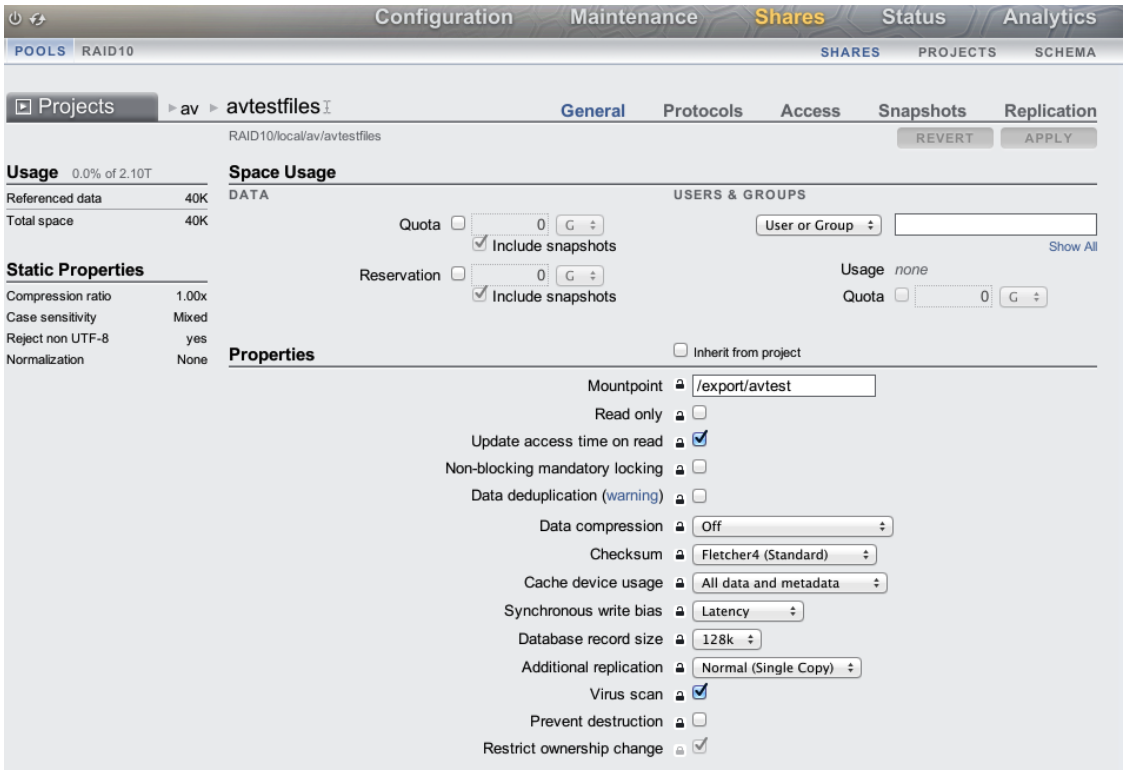

Figure 10. Oracle ZFS Storage Appliance share setup for virus protection

On the machine running SESC, set up the SAVDI daemon to run in debug mode. To do so, locate the file `savdid.conf` in the directory `C:\Program Files\Sophos\SAV Dynamic Interface`. Change the line containing the text `loglevel: 0` to `loglevel: 2` in the file. After this change is made, restart the SAVDID daemon in interactive mode using the following commands from the Command Prompt tool:

```
C:\> cd \Program Files\Sophos\SAV Dynamic Interface
C:\>Program Files\Sophos\SAV Dynamic Interface>net stop savdid
C:\>Program Files\Sophos\SAV Dynamic Interface>savdid.exe -uninstall
C:\>Program Files\Sophos\SAV Dynamic Interface>savdid.exe -l -c savdid.conf
120130:142245 0003407 Process starting
PID: 3460
```

The Sophos SAVDID process keeps a log file in the directory `C:\Documents and Settings\All Users\Application Data\Sophos\SAV Dynamic Interface\Logs`.

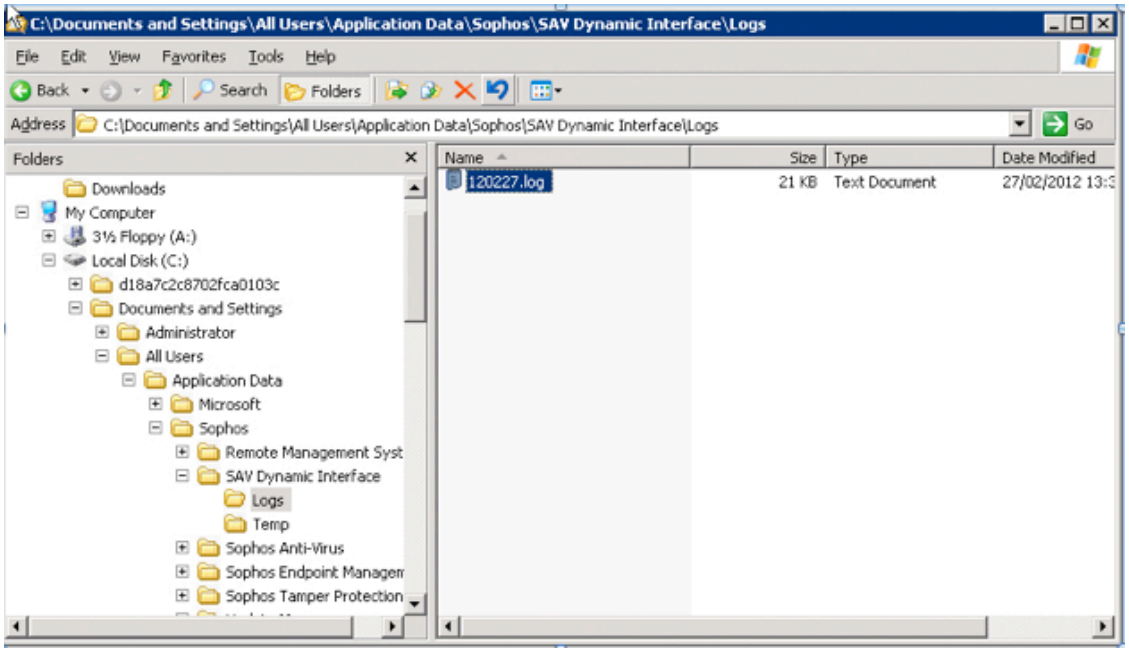

Figure 11. Folder structure for SAV Dynamic Interface Logs folder

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 shows a CLI session running 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 log file in the directory `C:\Documents and Settings\All Users\Application Data\Sophos\SAV Dynamic Interface\Logs` of the SAVDID to see if the files containing viruses were detected.

```
120227:154011 [4F4B9B54/3] 20040203 Virus found during virus scan 120227:154207
[4F4B9B55/1] 00030406 Client request RESPMOD icap://XXX.XXX.XXX.108:1344/avscan
ICAP/1.0 120227:154207 [4F4B9B55/1] 00030406 Client request Host: aie-ss7210-1 Allow:
204 Encapsulated: req-hdr=0, res-hdr=73, res-body=120 120227:154207 [4F4B9B55/1]
00030406 Client request GET http://aie-ss7210-1/export/avtest/testrun1/eicar_com.zip
HTTP/1.1 120227:154207 [4F4B9B55/1] 00030406 Client request HTTP/1.1 200 OK Transfer-
Encoding: chunked 120227:154207 [4F4B9B55/1] 00030406 Client request b8 120227:154207
[4F4B9B55/1] 00030406 Client request 120227:154207 [4F4B9B55/1] 00030405 Threat found
Identity: 'EICAR-AV-Test' "\eicar.com"
120227:154207 [4F4B9B55/1] 20040203 Virus found during virus scan
```

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

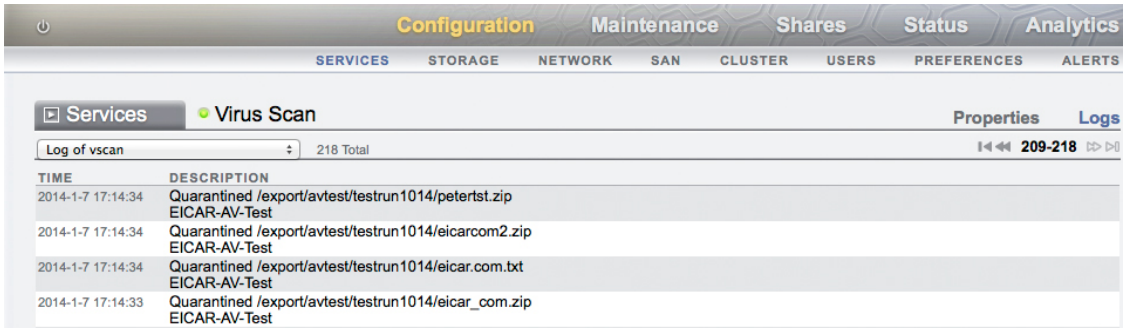

Figure 12. ICAP scan logging file

Configuration Best Practice

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

Using a Configuration File Optimized for the Oracle ZFS Storage Appliance

Included in the Sophos SAVDI component is a configuration file optimized for use with the Oracle ZFS Storage Appliance. This configuration file's max number of scan threads is increased to 32 and only configures a service listener to the Oracle ZFS Storage Appliance vscan request through the ICAP interface.

The following procedure, which must be executed on the Windows command line, shows how to stop the scan service, replace the `config` file and restart the scan service using the Oracle ZFS Storage Appliance optimized configuration file.

```
C:\> cd \Program Files\Sophos\SAV Dynamic Interface
C:\>Program Files\Sophos\SAV Dynamic Interface>net stop savdid
C:\>Program Files\Sophos\SAV Dynamic Interface>savdid.exe -uninstall
C:\>Program Files\Sophos\SAV Dynamic Interface>rename savdid.conf savdid.conf.org
C:\>Program Files\Sophos\SAV Dynamic Interface>copy icap-sun-w32.conf savdid.conf
C:\>Program Files\Sophos\SAV Dynamic Interface>savdid.exe -install
C:\>Program Files\Sophos\SAV Dynamic Interface>net start savdid
The SAV Dynamic Interface service is starting..
The SAV Dynamic Interface service was started successfully
C:\>Program Files\Sophos\SAV Dynamic Interface>
```

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. 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.

The default configuration files do not enable the option to let the scan engine unpack zip archives and scan their contents for viruses. To add this option, edit the `savdid.conf` file to include the option
`savigrp: GrpArchiveUnpack 1` in the scanner section of the `config` file, as seen in the following:

```
Scanner {
# See SAVDI Documentation for details for configuring
# SAVDI
type: SAVDI
inprocess: YES
savists: EnableAutoStop 1
# savdigrp: grpuser 1
savigrp: GrpArchiveUnPack 1

# maxscantime: 60
}
```

Follow the preceding CLI procedure to stop the scan engine, edit the configuration file as noted, and then restart the scan engine.

Synchronizing System Time

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

Conclusion

Using the Sophos Endpoint Protection 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 Sophos Endpoint Protection antivirus solution to perform scanning of files for worms, viruses, and Trojan horse threats.

Additionally, this solution takes advantage of the integrated VSCAN virus scanning service of the Oracle ZFS Storage Appliance to manage quarantining of files based on scan results from the 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 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
- Oracle ZFS Storage Appliance White Papers and Subject-Specific Resources
  http://www.oracle.com/technetwork/server-storage/sun-unified-storage/documentation/index.html
- Product Wiki Pages
  https://wikis.oracle.com/display/FishWorks/Fishworks
- Sophos web site
  http://www.sophos.com
- Sophos SAVDI ICAP Test Guide
  `http://www.sophos.com/en-us/medialibrary/PDFs/install_guides/SAVDIICAP_Test_Guide.pdf`
- Sophos SAV Dynamic Interface documentation
  http://www.sophos.com/support/docs/SAV_Dynamic_Interface-all.html
- Sophos Endpoint Security Control Windows documentation
  http://www.sophos.com/support/docs/Endpoint_Security_Control_Windows-all.html
- Sophos Endpoint Protection Enterprise documentation
  http://www.sophos.com/support/docs/Endpoint_Security_Data_Protection-all.html

- Oracle VM VirtualBox
  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 Sophos Endpoint Protection 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