



ZFS STORAGE
APPLIANCE

An Oracle Technical White Paper
January 2014

How to Configure the Trend Micro IWSA Virus Scanner for the Oracle ZFS Storage Appliance

Table of Contents

Introduction	2
How VSCAN Works.....	3
Installing IWSA and Configuring the Oracle ZFS Storage Appliance	6
Deployment of the IWSA Scanner Appliance.....	6
Prerequisites.....	6
Planning Network Topology	7
Installing the IWSA/IWSVA Virus Scanner	7
Connecting the Oracle ZFS Storage Appliance to the Virus Scan Service	13
Verifying the Virus Scan Service Configuration.....	14
Conclusion	17
Appendix: References	18

Table of Figures

Figure 1. File virus scan steps	4
Figure 2. Trend Micro IWSA console	8
Figure 3. Trend Micro IWSA web login page	8
Figure 4. Selecting ICAP mode	9
Figure 5. ICAP settings.....	9
Figure 6. Network settings	10
Figure 7. System time settings	11
Figure 8. Summary of settings.....	12
Figure 9. AV Scan Appliance setup completed	13
Figure 10. Oracle ZFS Storage Appliance Scan Engine(s) through ICAP setup	13
Figure 11. Oracle ZFS Storage Appliance Share setup for virus protection	14
Figure 12. Scanner dashboard showing detected virus count.....	15
Figure 13. Security Risk Report tab display	16
Figure 14. Detailed virus scan report	16
Figure 15. Oracle ZFS Storage Appliance virus scan logs	16

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 Trend Micro InterScan Web Security Appliance antivirus software as the external virus scanning engine.

Trend Micro InterScan Web Security Appliance (IWSA) antivirus scanner 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 Trend Micro InterScan Web Security Appliance (IWSA) 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, IWSA 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. Note that the terms IWSA and IWSVA (signifying the virtual appliance version installation of the IWSA software) are interchangeable in the following image.

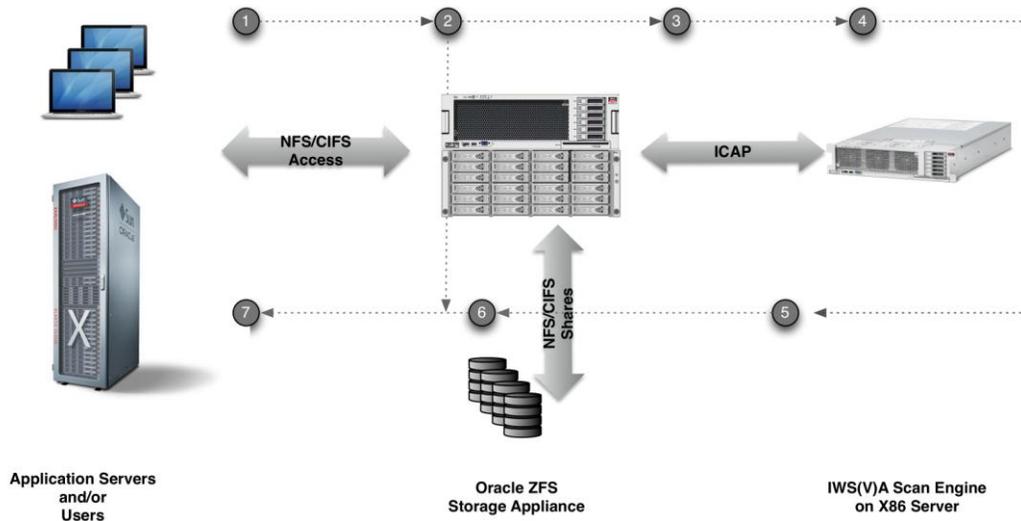


Figure 1. File virus scan steps

The following sequence of steps is followed when a file is accessed/created by a client on an NFS/CIFS file share when using an IWSA or IWSVA 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 IWSA.
4. The IWSA scan engine scans the file.
5. The IWSA 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.
6. The Oracle ZFS Storage Appliance takes one of the following actions, depending on the corresponding IWSA scan engine response from step 5:
- a) File stored/read.
 - b) av_quarantined set in ESA to deny further client access.
 - 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) Client access is allowed.
 - b) Client access is denied.
 - 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 IWSA and Configuring the Oracle ZFS Storage Appliance

The Trend Micro InterScan Web Security Appliance (IWSA) is available for installation on 'bare metal' or as a virtual appliance (IWSVA). Both installations use a Linux kernel as the operating system for the Oracle ZFS Storage Appliance. For “bare metal” installation, the package is installed directly on an x86-based server. For virtual appliance use, the package is installed in a virtual environment like Oracle VM VirtualBox or Oracle VM.

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.

This paper mainly shows the virtual appliance (IWSVA) version as an example. The acronyms IWSA and IWSVA are used interchangeably in this paper.

The installation ISO images for the InterScan Web Security (Virtual) Appliance can be found in the 'Download' section of Trend Micro's web site under the 'Internet Gateway' set of products.

Deployment of the IWSA Scanner Appliance

Ensure that you have met the following prerequisites before deploying the Trend Micro IWSA 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 *InterScan Web Security (Virtual) Appliance Installation Guide*.
- Download the ISO image of the required IWSA version.
- Verify that the hardware requirements for the IWSA meet your planned (virtual) x86 server.
- In case a proxy server is required for Internet access to Trend Micro's update server, verify support for virus update requests from your machine using the proxy server to Trend Micro's update server.
- Verify web browser access to both the Oracle ZFS Storage Appliance and IWSA.
- 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 IWSA 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 IWSA. A minimal configuration requires one network connection to the Oracle ZFS Storage Appliance and one network connection to the IWSA. 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 IWSA.

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 the Oracle ZFS Storage Appliance and clients, use a separate subnet for the ICAP connection.

You can also configure the IWSA to separate the IWSA 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 IWSA server, the admin and Internet traffic can be split up.

Installing the IWSA/IWSVA Virus Scanner

Prepare the Scan Server or Virtual Scan Server for boot of the scanner software ISO image. When using a virtual environment, set the OS host type to Redhat 64 bits. Follow the IWSA installation instructions for disk partitioning, root and administrators login credentials, and network configuration information.

At the end of the IWSA scanner installation, the following information displays on the scanner appliance console:

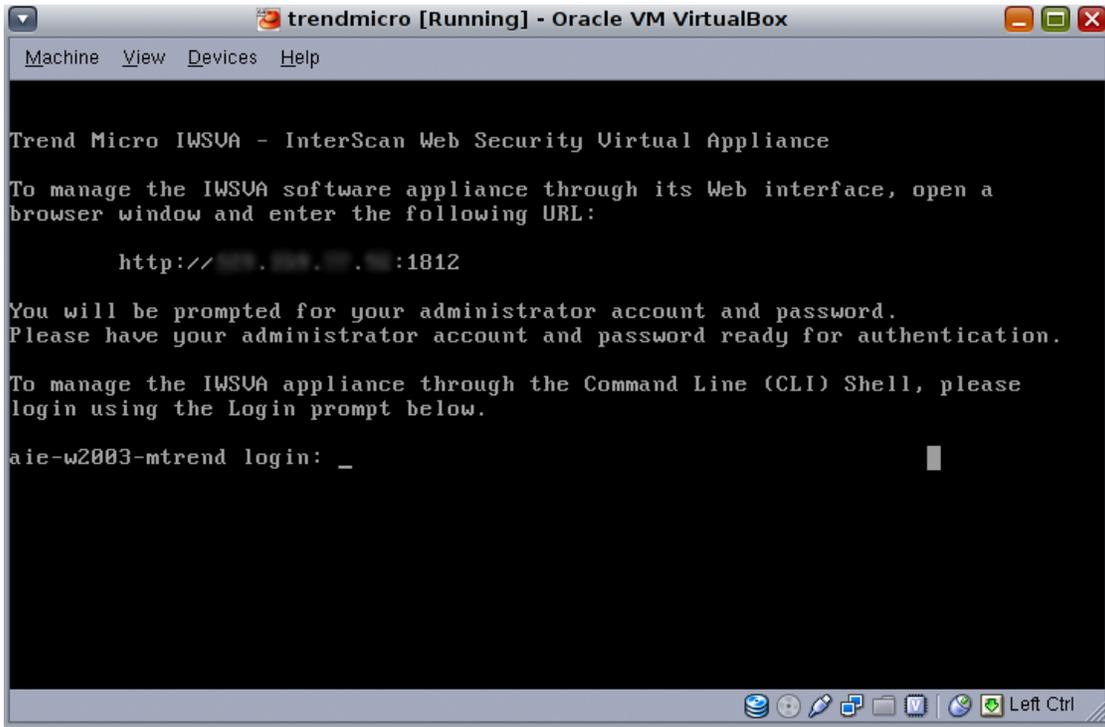


Figure 2. Trend Micro IWSA console

Using the URL provided in the startup screen bring ups the following login page in a browser window.



Figure 1. Trend Micro IWSA web login page

Use user admin and the password specified during the installation process. Under Administration, activate the Deployment Wizard. This prepares the IWSA for ICAP mode. The following information

is needed: the ICAP port that the scanner will monitor for scan requests from the Oracle ZFS Storage Appliance, and network configuration properties, like IP addresses, DNS server, and gateway.

Deployment Mode ?

IWSVA operates in different modes that affect how IWSVA fits into your network and scans traffic. IWSVA operates as a single unit or a cluster. In a cluster, two or more IWSVAs work together to provide fail-tolerance ability.

Steps

1. **Deployment Mode**
2. ICAP Settings
3. Network Interface
4. Static Routes
5. Product Activation
6. System Time
7. Summary
8. Results

Mode Selection

Transparent bridge mode *(This mode requires a minimum of two NICs.)*

Transparent bridge mode - high availability *(Requires a minimum of four NICs.)*

Forward proxy mode

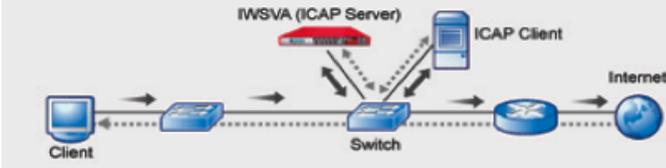
Reverse proxy mode

ICAP mode

Simple transparency mode

Web cache coordination protocol mode(WCCP)

Warning: The HTTPS decryption feature will be disabled in this mode.
ICAP mode In this mode, IWSVA processes requests from any ICAP-compliant client. Internet Content Adaptation Protocol (ICAP) is designed to forward HTTP responses or requests to third-party processors and collect the results.



< Back Next > Cancel

Figure 2. Selecting ICAP mode in the Trend Micro IWSA/IWSVA wizard

The Deployment Wizard starts with setting the mode of operation for the IWSVA server. Set the IWSVA to ICAP mode. The Oracle ZFS Storage Appliance uses this protocol to initiate scan requests for files that should be checked for viruses.

Figure 3. ICAP settings

ICAP Settings ?

Please specify the relevant ICAP settings.

Steps

1. Deployment Mode
2. **ICAP Settings**
3. Network Interface
4. Static Routes
5. Product Activation
6. System Time
7. Summary
8. Results

HTTP Listening Port

Port number:

ICAP Mode

Enable X-Virus-ID ICAP header

Enable X-Infection-Found ICAP header

Enable X-Authenticated-User ICAP header

Enable X-Authenticated-Groups ICAP header

< Back Next > Cancel

Enable both X-Virus-ID and X-Infection-Found header options so that the Oracle ZFS Storage Appliance receives the needed scan results information.

The screenshot shows the default value of 1344 for the listening port. This is the same value as the default value used in the Oracle ZFS Storage Appliance for VSCAN service. If the value is changed here, make sure to also change it in the setup of the VSCAN service in the Oracle ZFS Storage Appliance.

Network Interface ?

Please specify the relevant network interface settings for IWSVA.

Steps
 1. Deployment Mode
 2. ICAP Settings
3. Network Interface
 4. Static Routes
 5. Product Activation
 6. System Time
 7. Summary
 8. Results

Host Information	
Host name: *	<input type="text" value="aie-uc2007-network-08.sun.com"/>
Interface Status	
D=Data M=Management H=High Availability 	
Data Interface	
Ethernet Interface: *	<input type="text" value="eth0"/>
IP address:	<input type="text" value="Static IP address"/>
IP address: *	<input type="text" value="139.198.77.10"/>
Netmask: *	<input type="text" value="255.255.255.0"/>
<input type="checkbox"/> Enable ping	
Separate Management Interface	
Ethernet Interface: *	<input type="text" value="--select--"/> <input type="checkbox"/> Enable ping
Static IP address: *	<input type="text" value="139.198.77.10"/>
Netmask: *	<input type="text" value="255.255.255.0"/>
Miscellaneous Settings	
<input type="checkbox"/> Obtain from DHCP	
Gateway: *	<input type="text" value="139.198.77.254"/>
Primary DNS server: *	<input type="text" value="139.198.99.99"/>
Secondary DNS server:	<input type="text" value="139.198.99.99"/>

Figure 4. Network settings

Set the network parameters shown in the network interface screen according to the network topology used.

Note that if you need a proxy server to reach the Internet, you must configure the proxy server in the IWSVA under Updates>Connection Setting.

System Time ?

Please specify the system time settings.

Steps

1. Deployment Mode
2. ICAP Settings
3. Network Interface
4. Static Routes
5. Product Activation
- 6. System Time**
7. Summary
8. Results

System Time Settings

Current system time: **12/19/2011 14:07:21**
mm/dd/yyyy hh:mm:ss

Synchronize with NTP server

 Primary NTP server: *

 Secondary NTP server:

 Automatically synchronize every :

 Synchronize after deployment

Manually:
mm/dd/yyyy hh:mm:ss

Time Zone

Continent: City:

< Back
Next >
Cancel

Figure 5. System time settings

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

Results

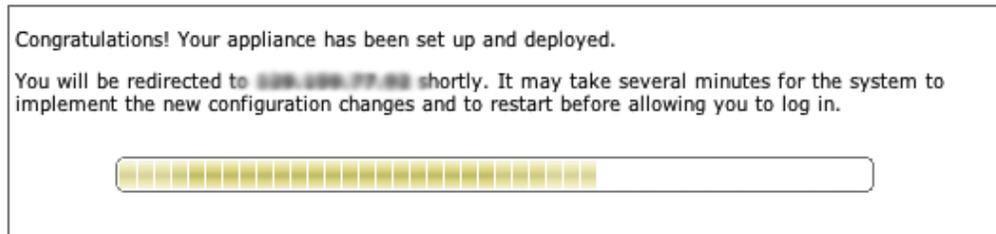


Figure 7. AV Scan Appliance setup completed

During the configuration process, the IP address used to access the Oracle ZFS Storage Appliance through a browser displays. The IP address appears again in the console message after the reboot is complete.

Next, log in to the IWSVA, set up the proxy server for Internet if needed and, using a web browser, update the virus signatures to the latest version available from Trend Micro's servers.

Connecting the Oracle ZFS Storage Appliance to the Virus Scan Service

Now that the IWSVA 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 IWSA can be reached.

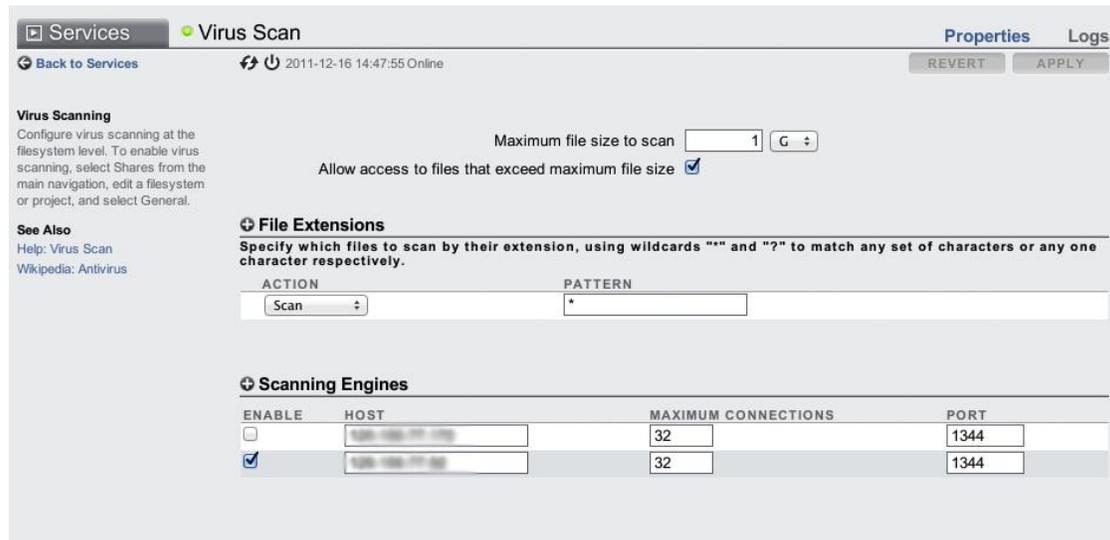


Figure 8. Scan Engine(s) through ICAP setup in the Oracle ZFS Storage Appliance BUI

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

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.

The screenshot shows the Oracle ZFS Storage Appliance web interface. The top navigation bar includes 'Configuration', 'Maintenance', 'Shares', 'Status', and 'Analytics'. The 'Shares' tab is active, and the 'Projects' sub-tab is selected. The share path is 'RAID10/local/av/avtestfiles'. The 'General' tab is active, showing 'Usage' (0.0% of 2.10T), 'Space Usage', 'Static Properties', and 'Properties'. The 'Properties' section is expanded, showing various settings. The 'Virus scan' option is checked, indicating that virus scanning is enabled for this share. Other settings include 'Mountpoint' (/export/avtest), 'Read only' (unchecked), 'Update access time on read' (checked), 'Non-blocking mandatory locking' (unchecked), 'Data deduplication (warning)' (unchecked), 'Data compression' (Off), 'Checksum' (Fletcher4 (Standard)), 'Cache device usage' (All data and metadata), 'Synchronous write bias' (Latency), 'Database record size' (128k), 'Additional replication' (Normal (Single Copy)), 'Prevent destruction' (unchecked), and 'Restrict ownership change' (checked).

Figure 9. 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 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.

```
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 #
    
```

The next step is to check the dashboard and the logging details of the IWSA to see if the files containing viruses were detected.

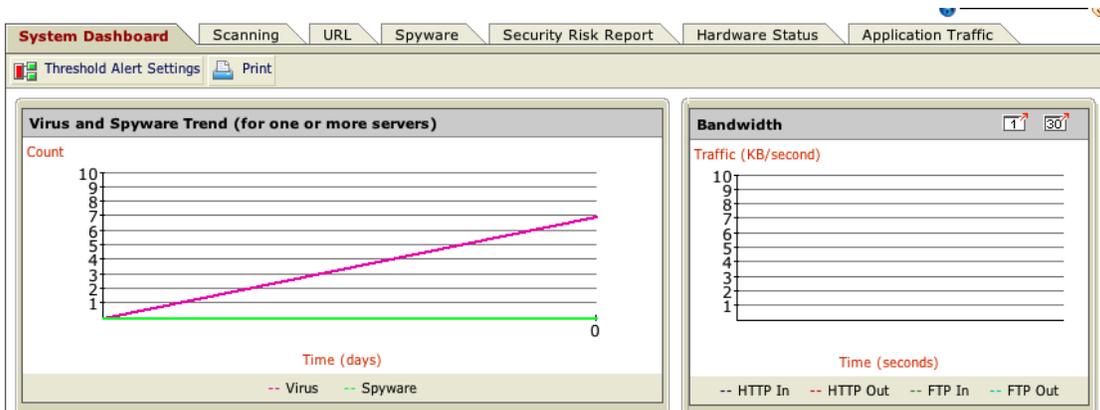


Figure 10. Scanner dashboard showing detected virus count

The security risk report in the IWSA gives more detailed history information about detected infections.



Figure 11. Security Risk Report tab display

Using the log query option in the IWSA shows further details on the files in which viruses were detected.

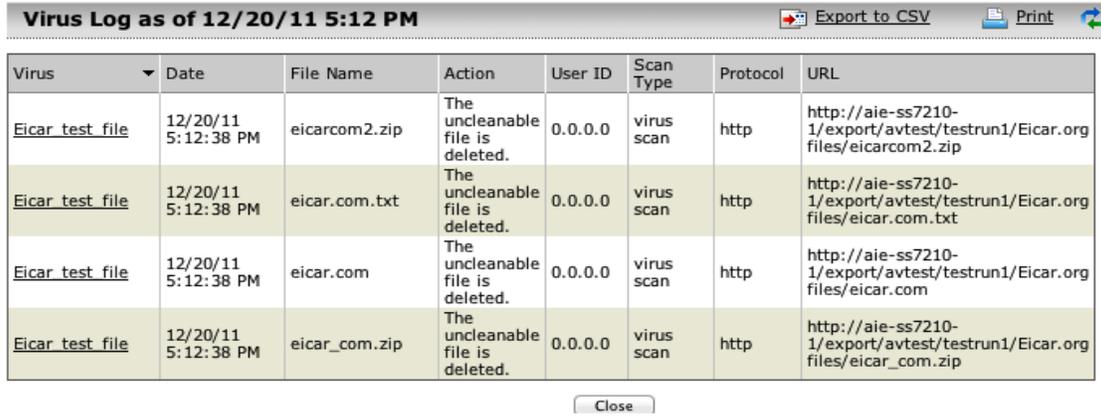


Figure 12. Detailed virus scan report

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.

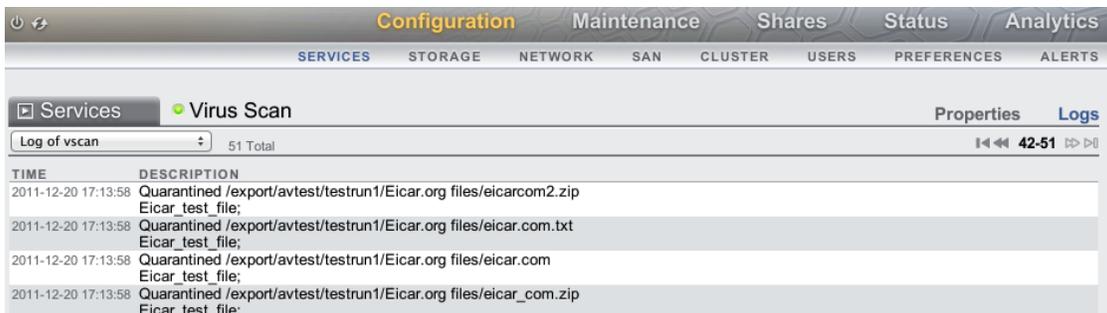


Figure 13. Oracle ZFS Storage Appliance virus scan logs

Conclusion

Using the Trend Micro InterScan 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 Trend Micro InterScan 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 Trend Micro InterScan 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>
- Oracle ZFS Storage Appliance Wiki Pages
<https://wikis.oracle.com/display/FishWorks/Fishworks>
- Trend Micro InterScan Web Security Product information;
Trend Micro InterScan Web Security Virtual Appliance, Installation Guide
<http://www.trendmicro.co.uk/products/interscan-web-security/>
- 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 the Trend Micro IWSA Virus Scanner 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