ORACLE

ZFS STORAGE APPLIANCE

An Oracle Technical White Paper
May 2015

How to Configure Kaspersky Anti-Virus Software for the Oracle ZFS Storage Appliance

ORACLE

Table of Contents

Introduction 2
How VSCAN Works 3
Installing Kaspersky Anti-Virus Software and Configuring the Oracle ZFS Storage Appliance 5
Deploying the Kaspersky Anti-Virus and Kaspersky Administrative Tools 6
Prerequisites 6
Planning Network Topology 6
Installing the Kaspersky Anti-Virus Software 7
Connecting the Oracle ZFS Storage Appliance to the Virus Scan Service 12
Verifying the Virus Scan Service Configuration 12
Configuration Best Practices 15
Handling Archive Type Files 15
Synchronizing System Time 16
Conclusion 17
Appendix: References 17

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 Kaspersky Anti-Virus Windows Servers Enterprise Edition software as the external virus scanning engine.

The Kaspersky Anti-Virus software 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 Kaspersky Anti-Virus Enterprise Edition Software 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, the Kaspersky anti-virus 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 NFSv4, are candidates for virus protection using the VSCAN service. A share that is published using NFSv3 cannot be scanned using VSCAN because NFSv3 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 anti-virus 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 NSFv4 or CIFS protocol.

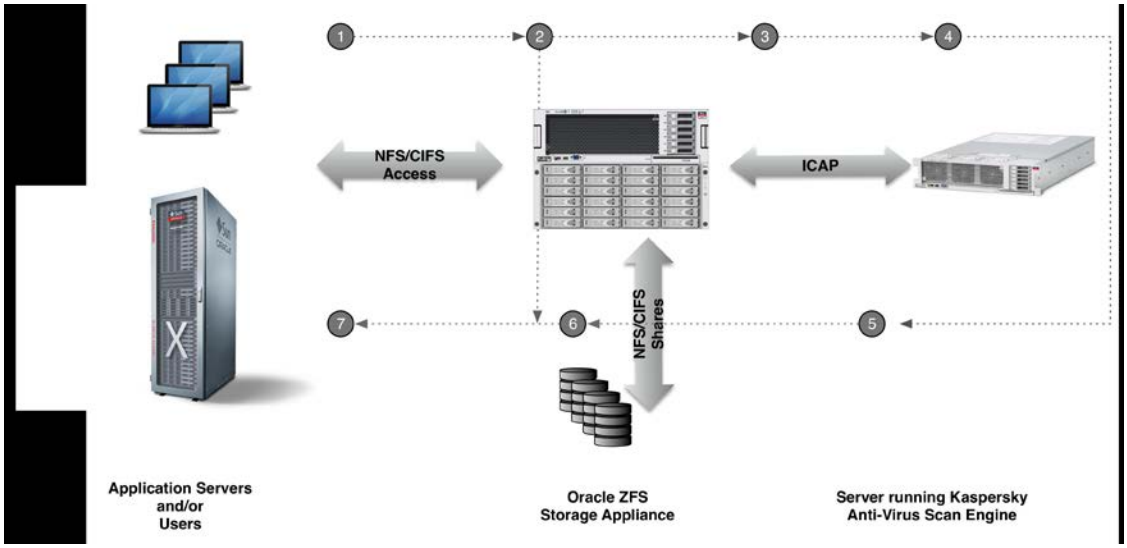

Figure 1. File virus scan steps

The following sequence of steps is followed when a file is accessed/created by a client on an NFSv4/CIFS file share when using the Kaspersky Anti-Virus 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 needs 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 Kaspersky Anti-Virus scan engine.
4. The Kaspersky Anti-Virus scan engine scans the file.
5. The Kaspersky Anti-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.
6. The Oracle ZFS Storage Appliance takes one of the following actions, depending on the Kaspersky Anti-Virus 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 Kaspersky Anti-Virus Software and Configuring the Oracle ZFS Storage Appliance

The Kaspersky Anti-Virus Enterprise Edition product suite contains Kaspersky Anti-Virus scanner environment and Administrative Tools to create an anti-virus scanning solution for the Oracle ZFS Storage Appliance.

For this paper, the Kaspersky Anti-Virus for Windows Servers Enterprise Edition was used, installed on a machine running Windows 2003.

The Kaspersky Anti-Virus Administrative Tools component contains a Console function that allows users to configure, monitor, and set maintenance functions for the AV scanning environment. The Anti-Virus component contains the Network Storage protection function that provides the interface between the Oracle ZFS Storage Appliance and the anti-virus scan engine using the ICAP protocol.

You can find the installation images using the 'Try it for free' option on the Kaspersky web site. See Appendix for reference to Kaspersky’s web pages.

Download and study the Kaspersky Anti-Virus Enterprise Edition documentation from the Kaspersky web site.

Deploying the Kaspersky Anti-Virus and Kaspersky Administrative Tools

Be sure to follow these prerequisite steps before deploying the Kaspersky Anti-Virus software:

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 Oracle's Oracle ZFS Storage Appliance product pages (See Appendix A: References).
- Download and study the *Kaspersky Anti-Virus Enterprise Edition* documentation from the Kaspersky web site.
- Download the Kaspersky Anti-Virus Enterprise Edition software for the required platform.
- Verify that the hardware requirements for the Kaspersky Anti-Virus Enterprise Edition and Administrative Tools packages meet your (virtual) hardware platform specs.
- In case a corporate proxy server is required for Internet access to Kaspersky update services, verify support for Kaspersky update requests from your machine using your proxy server to Kaspersky update services.
- 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 Kaspersky Anti-Virus 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 Kaspersky Anti-Virus server. A minimal configuration requires one network connection to the Oracle ZFS Storage Appliance and one network connection to the Kaspersky Anti-Virus 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 Kaspersky Anti-Virus server.

For the Oracle ZFS Storage Appliance, best practice is to separate client data and administrative IO traffic. The virus scan service generates extra data traffic with the ICAP

interface. To prevent this IO impacting data IO performance between Oracle ZFS Storage Appliance and clients, use a separate subnet for the ICAP connection.

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

Installing the Kaspersky Anti-Virus Software

Make sure the server you use for the anti-virus software installation is at the latest patch level for the installed OS.

The next step is to install the Kaspersky Anti-Virus Windows Server Enterprise Edition (KAVWSEE) software package. The Kaspersky installation wizard will guide you through the installation of the software package.

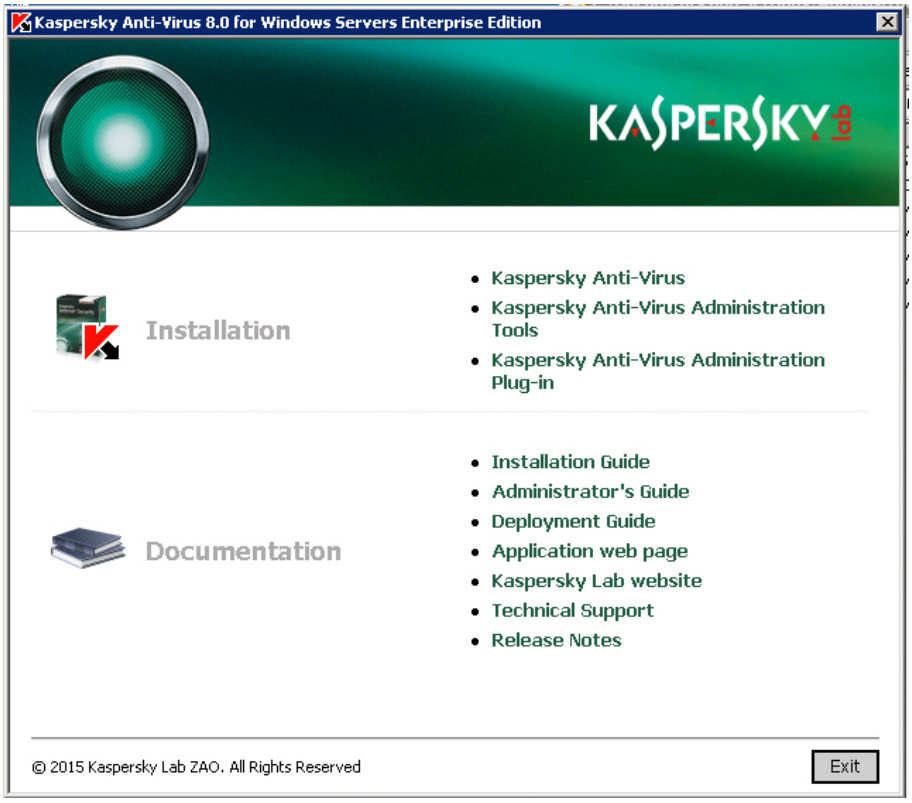

Figure 2. Installation wizard for Kaspersky Anti-Virus for Windows Servers Enterprise Edition

Use the ‘Kaspersky Anti-Virus’ and ‘Kaspersky Anti-Virus Administrative tools’ installation options to install the required Kaspersky Anti-Virus Enterprise Edition components.

For the Kaspersky Anti-Virus software to update its software components and the anti-virus signature database (application database in the Kaspersky update menu) access to the external Internet is required. The Kaspersky software manages access for each update component through its ‘Connection Settings’ menu using the Properties option in each Update service. The Update services can be found in the navigation pane on the left of the Kaspersky Console window.

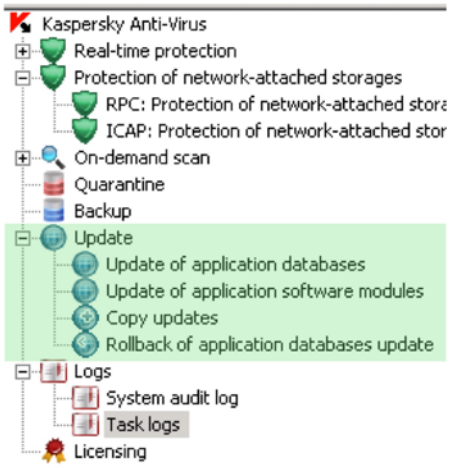

Figure 3. KAVWSEE console showing update services

When a proxy server is needed to access an external web site, make sure the Kaspersky Anti-Virus server is set up accordingly through the Security tab in the Properties dialog windows as shown in the next screen illustration.

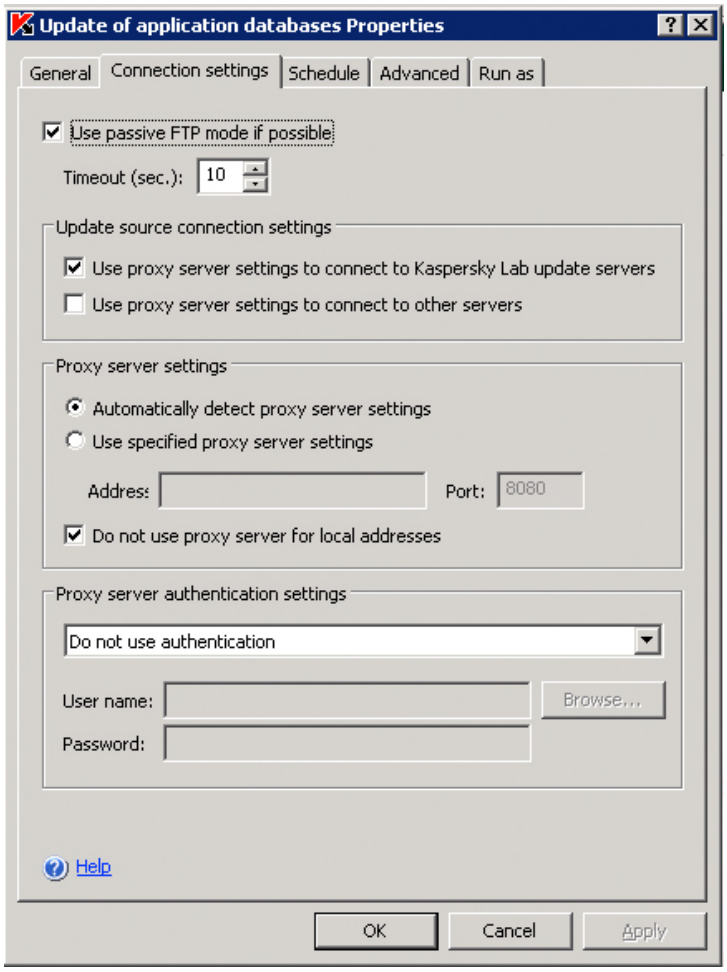

Figure 4. Specifying proxy information for KAVWSEE virus signatures auto-update

Once access to the Kaspersky update servers is set up, the 'Update of Application databases' and Update of application software modules' can be started to ensure the latest virus signatures are present and the Kaspersky Anti-Virus software components are updated to the latest release level.

The last step is to enable and verify the ICAP option in the ‘Protection of network-attached storage’ function.

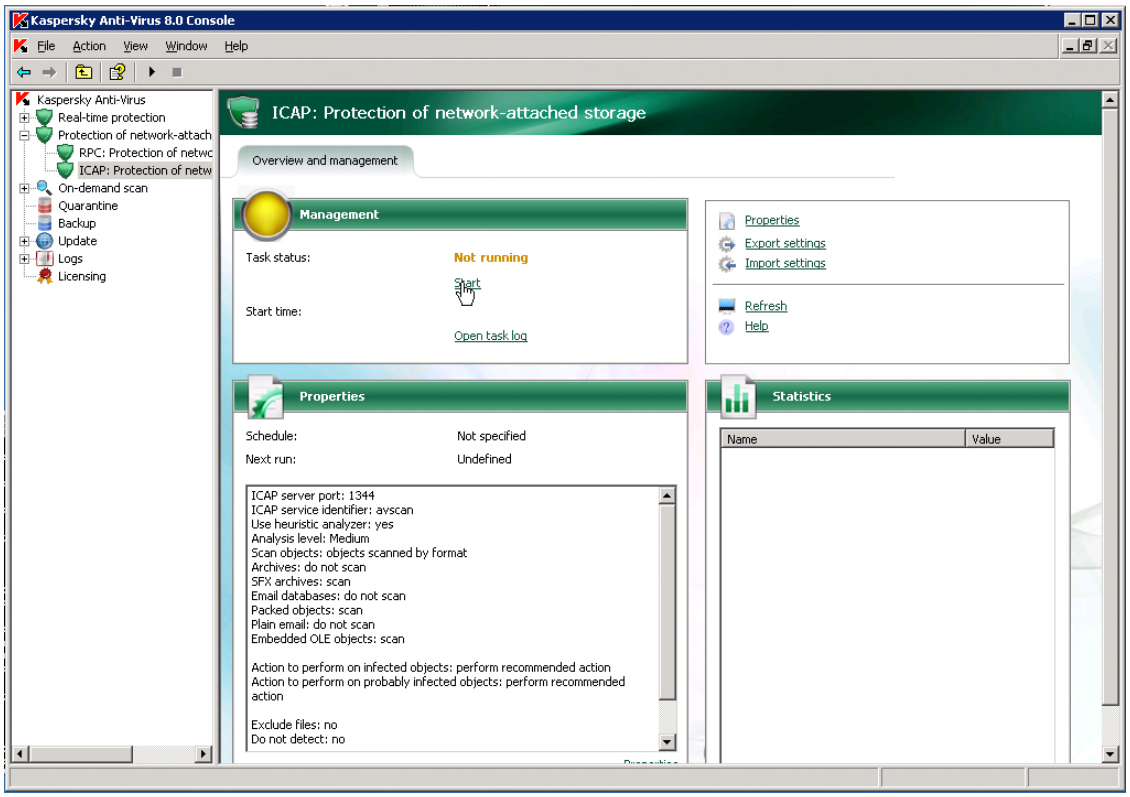

Figure 5. ICAP: Protection of network-attached storage option

Use the Properties option to configure the required Heuristic analyze level and the required Protection level.

The Oracle ZFS Storage Appliance supports the Quarantine infected files option in the ICAP protocol, so for the Kaspersky Anti-Virus the related actions need to be set.

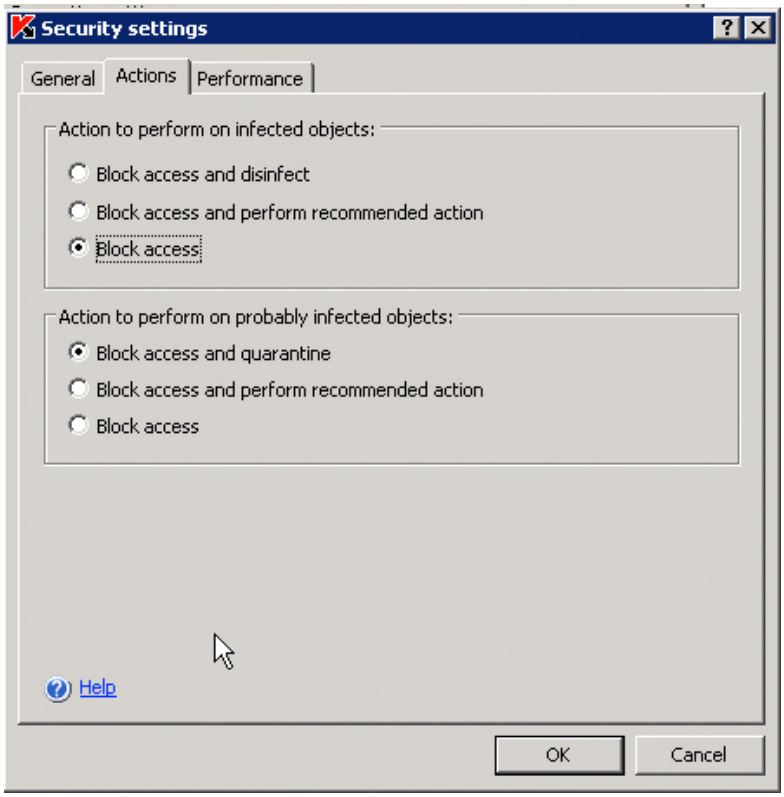

Figure 6. ICAP network storage scan actions setup

For scanning compressed archives, see suggestions in the Best Practices section of this document.

Connecting the Oracle ZFS Storage Appliance to the Virus Scan Service

Now that the Kaspersky Anti-Virus 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 In the Oracle ZFS Storage Appliance BUI. Use the + button in front of Scanning Engines and specify the IP address and port number through which the Kaspersky Anti-Virus can be reached.

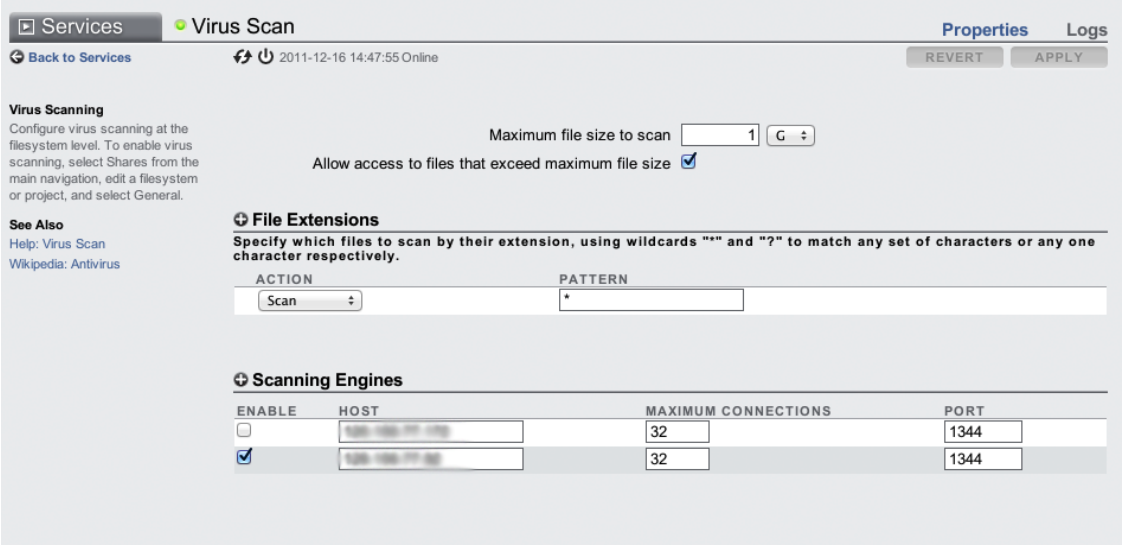

Figure 7. Oracle ZFS Storage Appliance scan engine(s) through ICAP

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

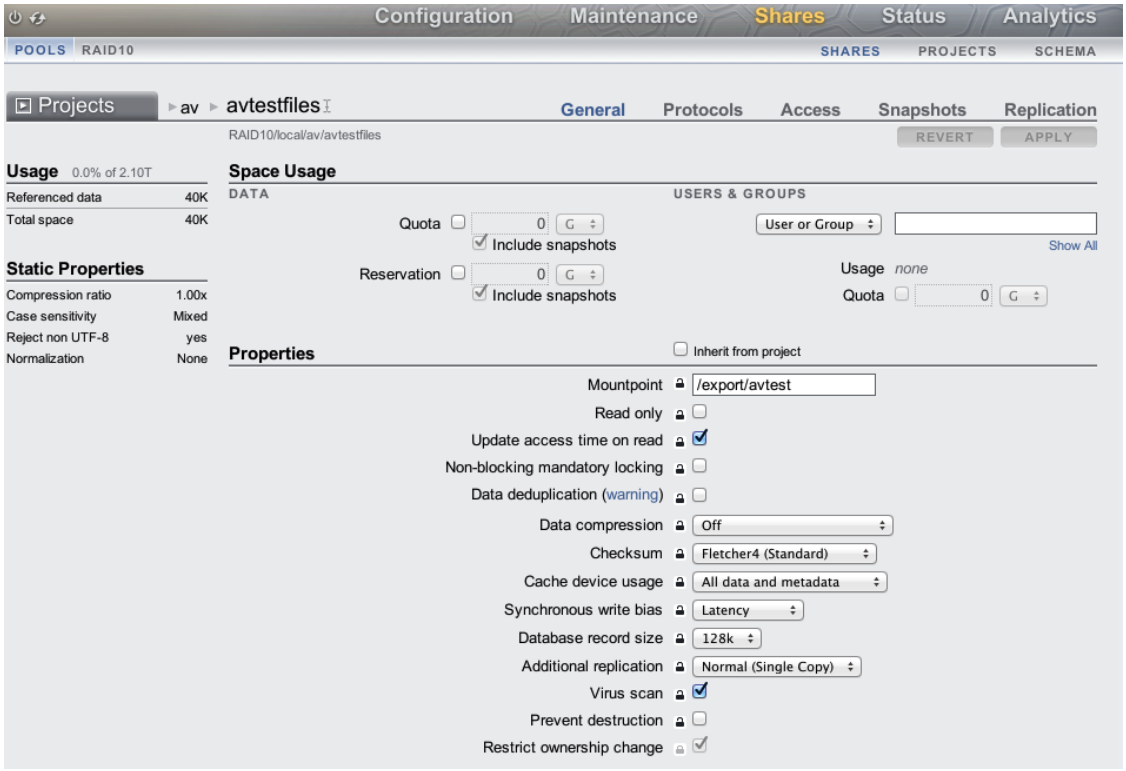

Figure 8. Oracle ZFS Storage Appliance share setup for virus protection

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 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/run7
root@edinburgh # cd /av/avtest/run7/Eicar.org files
root@edinburgh # pwd
/av/avtest/run7/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
-rw-r--r--   1 root     root          68 Apr 14  2015 eicar.com
-rw-r--r--   1 root     root          68 Apr 14  2015 eicar.com.txt
-rw-r--r--   1 root     root         184 Apr 14  2015 eicar_com.zip
-rw-r--r--   1 root     root         308 Apr 14  2015 eicarcom2.zip
```

```
-rwxr-xr-x   1 root     root           7 Apr 14  2015 normal_file.txt
-rwxr-xr-x   1 root     root          63 Apr 14  2015 website.txt
root@edinburgh #
```

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.

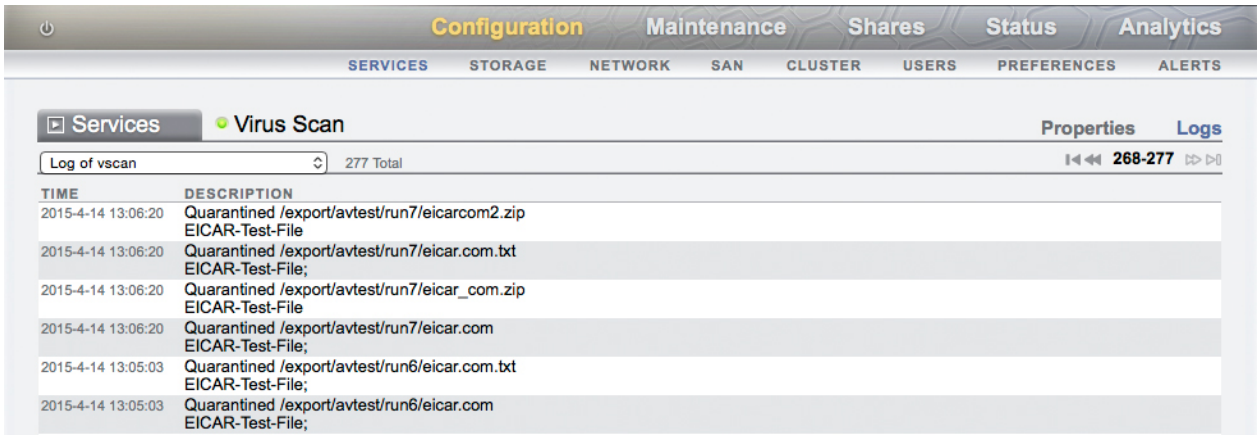

Figure 9. ICAP scan logging file

Two tests were run, one with and one without the scan archives object option.

The verify the detection of the virus infected files on the Kaspersky Anti-Virus Server, use the Kaspersky Anti-Virus Console, and select the Task logs window from the left console pane.

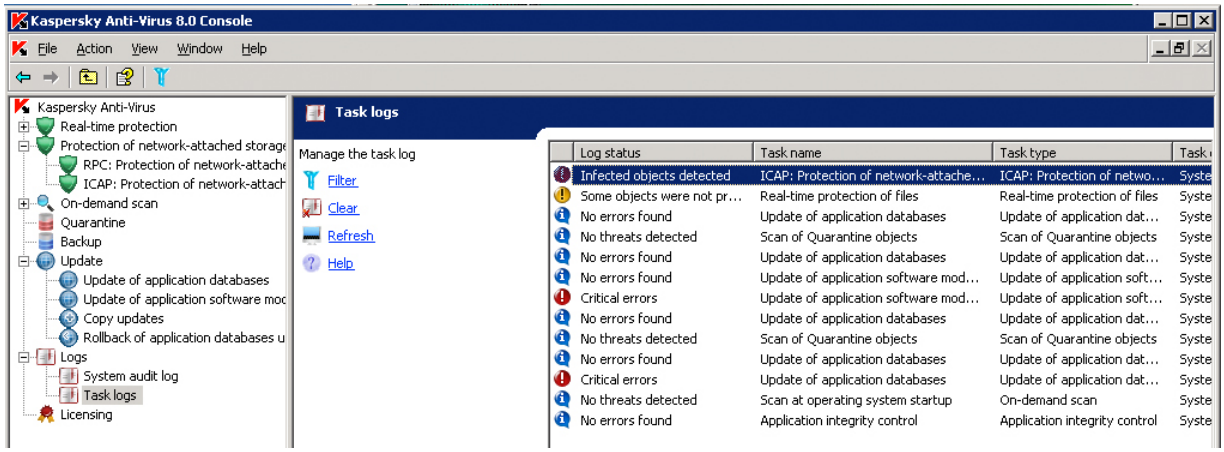

Figure 10. Task logs option from Kaspersky Anti-Virus Console

Select the Infected Objects Detected in the Events tab and verify that the infected test files have been detected and quarantined.

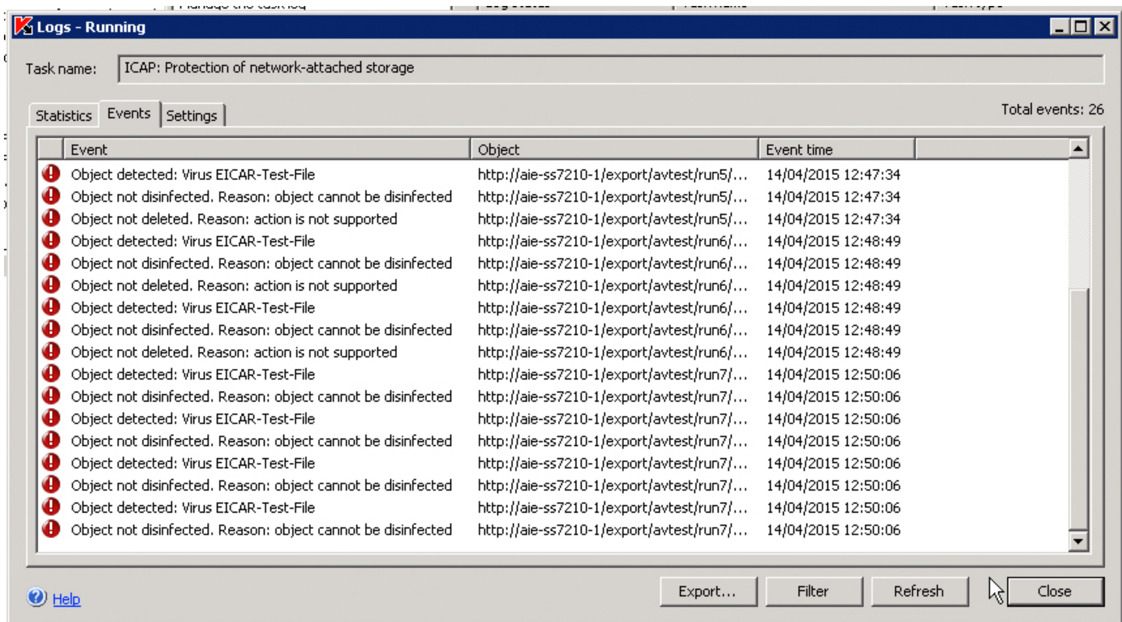

Figure 11. Virus Scan logging on Kaspersky Anti-Virus Console

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. 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 settings enable the option to let the scan engine unpack zip archives and scan their contents for viruses. To add this option, use the Properties option for the 'ICAP protection of network attached storage' service as found in the left-side navigation pane of the Kaspersky console window. Select the *settings* option in the *Protection Level* screen to specify the type of objects to enable for scanning as shown in the following screenshot.

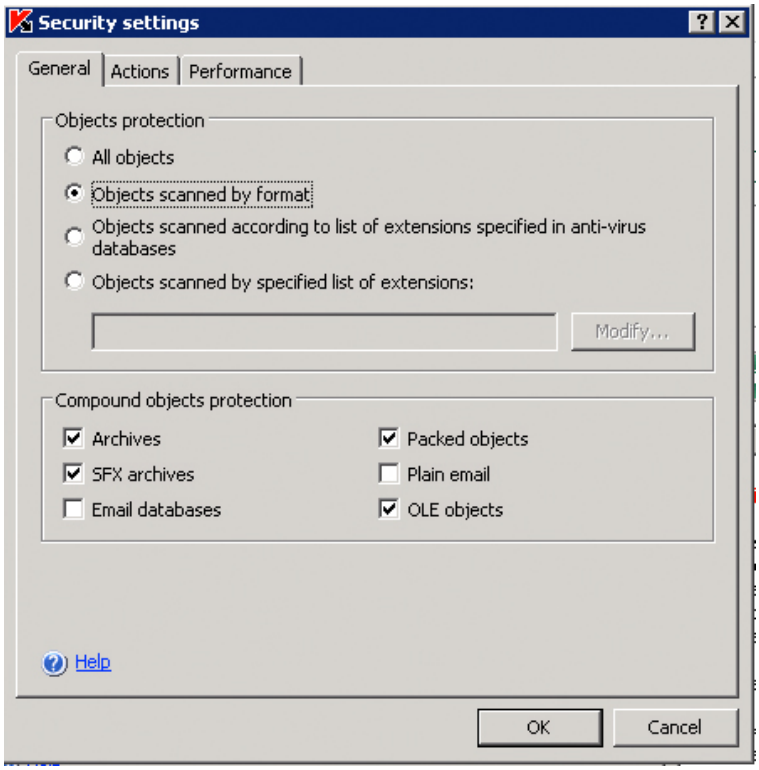

Figure 12. Selecting type of objects for protection

Synchronizing System Time

It is a best practice to keep the time between the Oracle ZFS Storage Appliance and the Kaspersky Anti-Virus 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 Kaspersky Anti-Virus server.

Conclusion

Using the Kaspersky Anti-Virus Enterprise Edition 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 anti-virus scanning platform, thereby maximizing the workload capability on the Oracle ZFS Storage Appliance, while taking advantage of the expertise embedded in the Kaspersky Anti-Virus Enterprise Edition solution to perform scanning of files for worms, viruses, and Trojan horse threats.

Additionally, this solution takes advantage of the Oracle ZFS Storage Appliance's integrated VSCAN virus scanning service to manage quarantining of files based on scan results from the Virus Scan anti-virus platform.

This anti-virus 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

- *Oracle ZFS Storage Appliance documentation Library*
  http://docs.oracle.com/en/storage/
- The *Oracle ZFS Storage Appliance Administration Guide* is also 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 White Papers and Subject-Specific Resources
  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
- Kaspersky Products web site
  http://www.kaspersky.com
- Kaspersky Anti-Virus Enterprise Edition documentation
  located on Kaspersky's Support site:
  http://support.kaspersky.com/wsee8#downloads
- Kaspersky Security for Storage product page
  http://www.kaspersky.com/products/business/targeted-solutions/storage

- Kaspersky Products support site
  http://support.kaspersky.com/

How to Configure Kaspersky Anti-Virus Software for the Oracle ZFS Storage Appliance
May 2015, Version 1.0
Author: Peter Brouwer

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