TECHNICAL PAPER

HITACHI
Inspire the Next

Hitachi NAS Platform Protection with Kaspersky Anti-Virus for Microsoft ® Windows Server® Enterprise Edition using Internet Content Adaptation Protocol

Lab Validation Report

By John Goodman

May 6, 2015

Hitachi Data Systems

Feedback

Hitachi Data Systems welcomes your feedback. Please share your thoughts by sending an email message to SolutionLab@hds.com. To assist the routing of this message, use the paper number in the subject and the title of this white paper in the text.

Table of Contents

Hitachi NAS Platform Protection with Kaspersky Anti-Virus for Microsoft ® Windows Server® Enterprise Edition using Internet Content Adaptation Protocol

Lab Validation Report

Without proper antivirus protection, a single virus can spread very quickly throughout a corporate infrastructure. Additionally, with home directories often residing on NAS shares and users storing documents on network shares, a virus can lie dormant on network attached storage only to infect other systems on the network at a later date.

Kaspersky Anti-Virus for Windows Server Enterprise Edition ensures business continuity by protecting data on Microsoft® Windows® operating systems and network-attached storage devices against viruses and other malware.

Hitachi NAS Platform (HNAS) provides integrated antivirus functionality that allows administrators to manage antivirus behavior from the HNAS interface as well as from the Kaspersky Anti-Virus for Windows Server Enterprise Edition console and helps protect corporate data from the spread of malicious virus code.

This lab validation report is for Hitachi NAS Platform 3000 and 4000 series with Kaspersky Anti-Virus for Windows Server Enterprise Edition using Kaspersky's Real-time protection of Internet Content Adaptation Protocol (iCAP or ICAP) storage systems feature. The test validates the stability and functionality of Kaspersky Anti-Virus for Windows Server Enterprise Edition (and Kaspersky HNAS specific patches) on Hitachi NAS Platform 3000 and 4000 series.

The validation of Hitachi NAS Platform 3000 and 4000 series with Kaspersky Anti-Virus for Windows Server Enterprise Edition using ICAP proved successful and consistent with its functions and operations.

This validation report provides information related to the specific configurations of Hitachi NAS Platform 3000 and 4000 series and of Kaspersky Anti-Virus for Windows Server Enterprise Edition for use by data center administrators and system engineers.

Product Features

These products are a part of the tested configuration.

Kaspersky Anti-Virus for Windows Server Enterprise Edition

Developed specifically for high performance corporate servers, Kaspersky Anti-Virus for Windows Server Enterprise Edition (WSEE) provides data protection for mission critical servers running Microsoft Windows operating systems and network attached file servers.

The advantages of Kaspersky Anti-Virus WSEE include:

Always-on antivirus protection and on-demand scanning. The application scans every file that is launched or modified and treats, deletes or quarantines any suspicious object. If new software is installed or a file infection is suspected, the administrator can also launch a targeted antivirus scan of the suspect areas.

Proactive protection from malware. The anti-malware engine incorporates advanced anti-malware protection methods such as an heuristic analyzer capable of identifying malicious programs with a very high degree of accuracy, even if its signature has not yet been added to the antivirus databases.

Scanning the operating system's critical areas. A dedicated task can be run to scan those areas of the operating system that are most exposed to infection. For example, scanning autorun files can help prevent a virus from launching during system startup or detect any hidden processes.

Flexible scan settings. File scan settings enable the administrator to: exempt certain processes from scanning; set the depth of antivirus protection; specify which file types must always be scanned and which should be exempted completely, and preset responses to suspicious and infected objects according to threat type. This approach helps optimize the server load and ensures the flexible management of corporate network security.

Terminal and virtual server protection. The application protects Microsoft Terminal Services and Citrix XenApp servers, ensuring that end-users working in desktop/application publishing modes remain protected and are notified of events using the terminal services. Microsoft Hyper-V®, XenDesktop and VMware environments are also supported.

Cluster support. The application is ideally suited to the complex server cluster architecture typically found in large companies. It protects the local disks of the server's file system as well as the cluster's shared disks currently owned by the protected node.

Hitachi NAS Platform

Hitachi NAS Platform leads the industry in performance and scalability and delivers the most advanced virtualization framework. This NAS solution is ideal for virtualization, file server/NAS consolidation and protection of highly valuable data, reducing management complexity and total cost of ownership (TCO). HNAS seamlessly integrates with Hitachi SAN storage, including Hitachi Command Suite software.

It is also ideal for data intensive, performance driven markets such as Life Sciences, Internet Services, Entertainment, Electronic Document Discovery, Government, Education, Oil and Gas, and Electronic Design, enabling customers to minimize processing cycle times and improve productivity.

To detect and stop viruses before they spread, Hitachi NAS Platform integrates antivirus functionality into Hitachi NAS Platform system software. Hitachi NAS Platform integrated antivirus software communicates with Kaspersky Anti-Virus for Windows Server Enterprise Edition (WSEE) to provide additional protection against viruses by scanning files from Windows and other CIFS/SMB clients. Virus scanning activity is in real-time and transparent to end users and occurs when a requesting user or application opens or reads a file or when a file is created or written. If a virus is found, Hitachi NAS Platform will mark the file as infected and deny access to the file.

Hitachi NAS Platform provides as much information as possible to the storage administrator and makes the behavior easily configurable. This information includes statistics about the status of virus scans, information about the virus scan servers, the list of file types that are being scanned, and so on.Test Environment Configuration

This is the configuration of the test environment for this Lab Validation Report.

Storage Configuration

All of the Hitachi NAS Platforms in this Lab Validation report were attached to a mixture of Hitachi storage.

Table 1. Storage Array Microcode Levels

Storage Array	*Microcode*
Hitachi Virtual Storage Platform	70-06-22-00/00
Hitachi Unified Storage VM	73-03-01-00/00
Hitachi Unified Storage 130	0930/A-S

Table 2. Hitachi NAS Platform Firmware Levels

Hitachi NAS Platform	*Firmware Level*
Hitachi NAS Platform 4100	12.2.3719.02
Hitachi NAS Platform 4060	12.0.3528.01
Hitachi NAS Platform 3090	12.1.1.3613.06

SAN Configuration

All Hitachi NAS Platforms in this Lab Validation report were SAN attached via Brocade 5300 SAN switches.

Network Configuration

Hitachi NAS Platform 3090 was connected to a 1 Gb LAN, while Hitachi NAS Platform 4100 was connected to a 10 Gb LAN.

The Kaspersky virus scan servers, were attached to a 1 Gb LAN network, thus limiting virus scanning throughput to 1 Gb/sec LAN speeds.

Server Configuration

The Kaspersky scan servers were installed on VMware ESXi 5.5 VMs running on a SAN attached Hitachi Compute Rack 220H rack server.

Table 3. Hitachi Compute Rack Component Details

Component	*Model/Capacity*
CPU	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz
CPU Socket/Core	2 CPUs/4 Cores
Memory	48 GB
HBA	Emulex LPe12000 8 Gb Fibre Channel

Virtualized Environment Configuration

Three Kaspersky scan servers were utilized for this Lab Validation Report.

Each Kaspersky scan server VM was configured with two CPUs with two cores per socket, 8 GB memory and was installed on its own SAN volume. Microsoft Windows Server 2012 R2 was installed on each VM as well as Kaspersky Anti-Virus for Windows Server Enterprise Edition.

All of the VMs were attached to a 1 Gb/sec VM Network.

Application Configuration

Kaspersky Anti-Virus for Windows Server Enterprise Edition version 8.0.2.51 was used for this Lab Validation Report.

Kaspersky Anti-Virus for Windows Server Enterprise Edition (WSEE) is able to offer antivirus protection to Hitachi NAS Platform storage systems using the Internet Content Adaptation Protocol (ICAP) as shown in Figure 1.

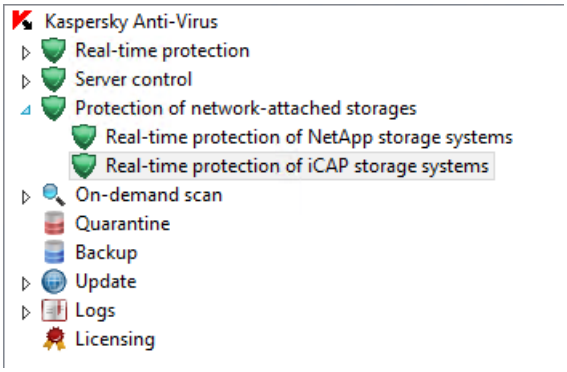

Figure 1

Each instance of WSEE was configured to use the Real-time protection of iCAP storage systems feature. To configure the Real-time protection of iCAP storage systems feature, click the Properties link as shown in Figure 2.

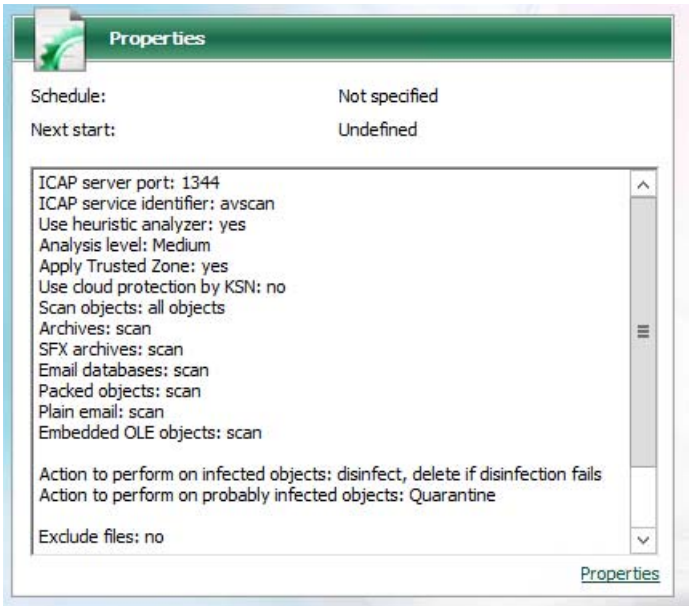

Figure 2

The heuristic analyzer was set to medium (default), the Network port for ICAP-server was set to 1344 and the ICAP service identifier was set to “avscan” (both are default values) as shown in Figure 3.

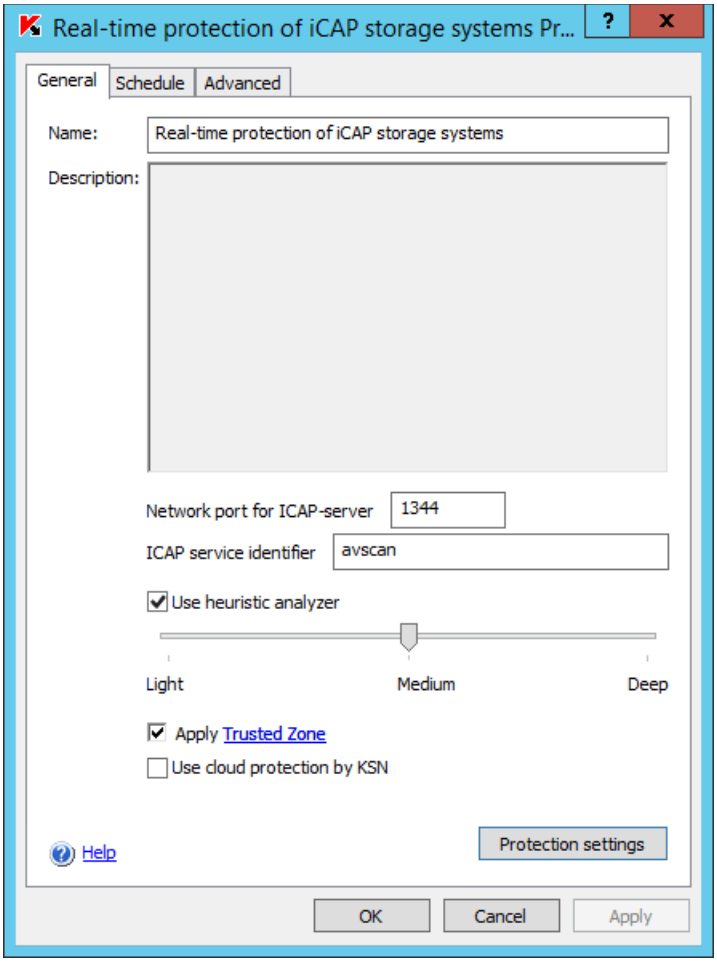

Figure 3

The General settings under Protection settings were set to protect all objects and to scan all compound objects, as shown in Figure 4.

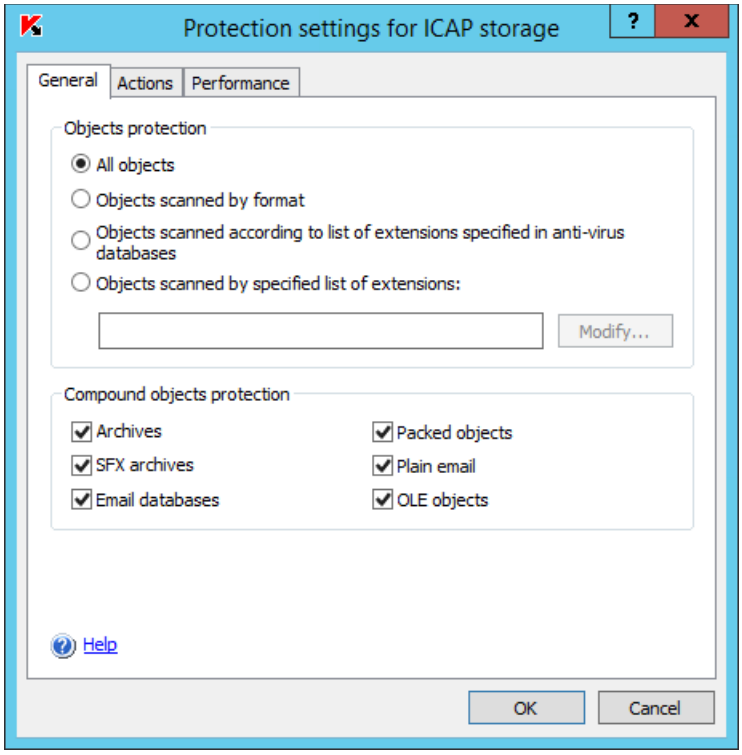

Figure 4

The Actions settings under Protection settings were set to Block access and disinfect infected objects and to Block access and quarantine probably infected objects, as shown in Figure 5.

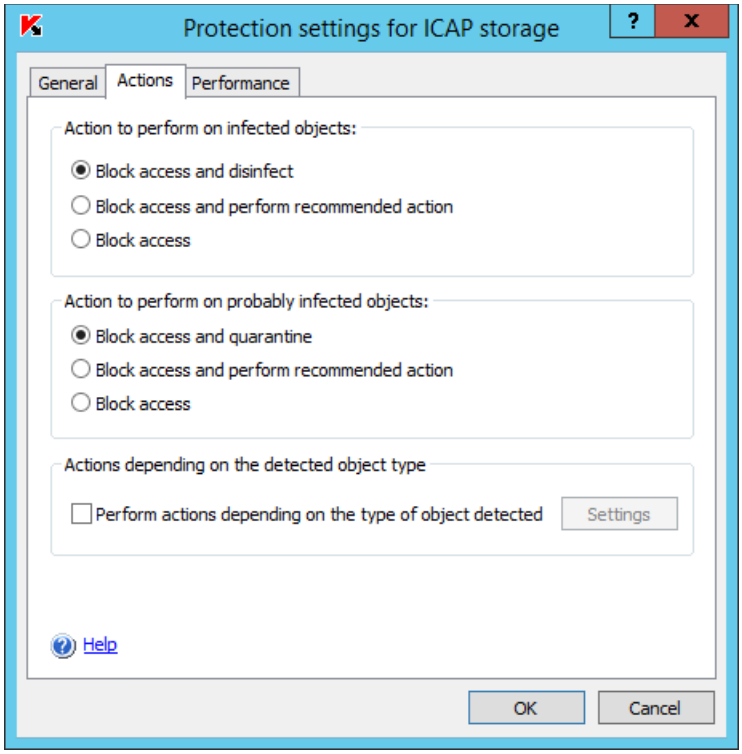

Figure 5

The Performance settings under Protection settings were unmodified and left at the default settings, as shown in Figure 6.

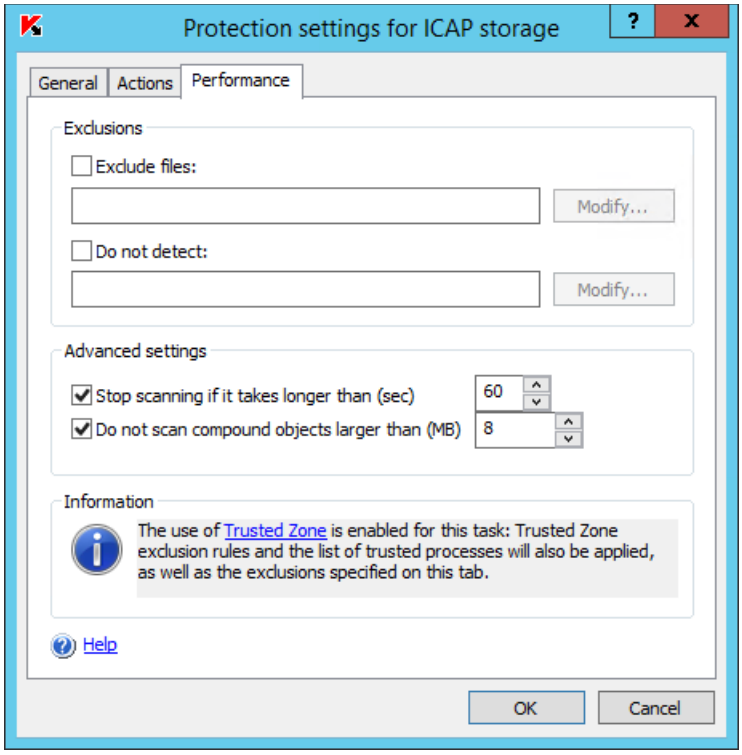

Figure 6

Hitachi NAS Platform Configuration

Hitachi NAS Platform antivirus scanning is configured on a per share, per EVS basis. Each CIFS share to be scanned by Kaspersky Anti-Virus had virus scanning enabled, as shown in Figure 7.

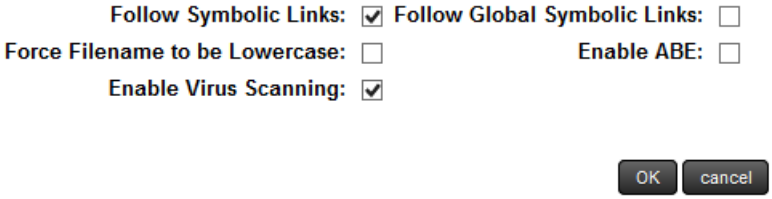

Figure 7

For each EVS with shares to be scanned, ICAP mode was enabled and Scan All File Types was selected, as shown in Figure 8.

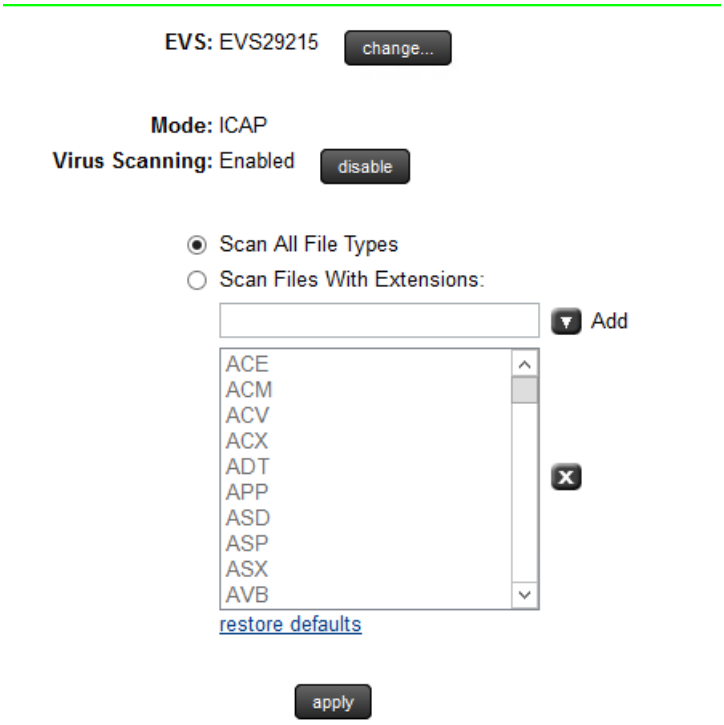

Figure 8

After starting the Kaspersky Real-time protection of iCAP storage systems, the scan engine should be available to add to the Hitachi NAS Platform registered virus scan engines list, as shown in Figure 9.

Kaspersky WSEE was added as an ICAP scan engine within HNAS by clicking the add button on the Virus Scanning page and entering the IP address(es) of the Kaspersky server(s) and the service name.

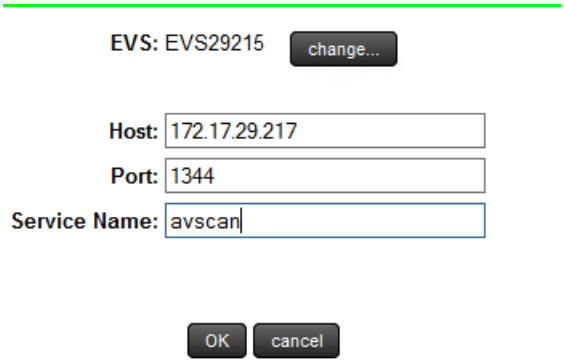

Figure 9

After adding the Kaspersky WSEE ICAP server to the Registered Virus Scan Engines list, its status is displayed as OK, as shown in Figure 10.

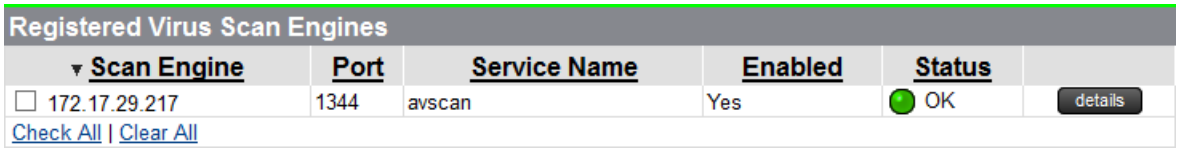

Figure 10

Test Methodology

The objective of this test is to exercise general use cases to qualify Kaspersky Anti-Virus for Windows Server Enterprise Edition (WSEE) using ICAP with Hitachi NAS Platform. The use cases will verify that WSEE can be installed and connected to HNAS using WSEE's Real-time protection of iCAP storage systems feature.

The information collected during testing determined the overall qualification of all involved parts.

Test Cases

Install Kaspersky Anti-Virus for Windows Server Enterprise Edition

Test Case	*Details*
1	Install Kaspersky Anti-Virus
2	Install Kaspersky Anti-Virus Administration Tools

Configure Kaspersky Anti-Virus and start the Real-time protection of iCAP storage systems

Test Case	*Details*
1	From the Kaspersky Anti-Virus Console navigate to Protection of network-attached storage systems, then click Real-time protection of iCAP storage systems, then click Properties. Click the Protection Settings button and the General and Action settings.
2	Verify that the Real-time protection of iCAP storage systems server will start.
3	Verify that ICAP mode is enabled on the EVS for HNAS and that Scan All File Types is selected.
4	Verify that the Kaspersky server can be added to the list of Registered Virus Scan Engines.
5	Verify that the Kaspersky Anti-Virus server is displayed in the Registered Virus Scan Engines on HNAS and that the Status is OK.
6	Verify that the IP address, Port, and Service Names are displayed correctly in the Registered Virus Scan Engines list.

Test scanning with a clean file (10 KB files)

Test Case	*Details*
1	Using the RISE file generator, generate 20, 10 KB files.
2	Verify that the Kaspersky objects processed statistics match the HNAS number of virus scans and number of clean scans.

Test scanning with clean large file (10 MB or more)

Test Case	Details
1	Using the RISE file generator, generate 20, 20 MB files.
2	Verify that the Kaspersky objects processed statistics match the HNAS number of virus scans and number of clean scans.

Test scanning with an EICAR test file

Test Case	Details
1	Download an EICAR test virus sample such as eicar.com from www.eicar.org and copy the file to the CIFS share to be scanned.
2	Check the actions taken and verify logs and statistics. Verify that the EICAR files are deleted from the file system.

Performance Test

Test Case	Details
1	Create a set of sample files around 2 GB of various sizes ranging from 1 KB to 100 MB and copy the files to the CIFS share to be scanned.
2	Record the performance metrics of the anti-virus scan server. Verify that all files were scanned without error.

Analysis

During testing, no interoperability issues were found. The testing executed during this validation proved that Kaspersky Anti-Virus for Windows Server Enterprise Edition using ICAP with Hitachi NAS Platform versions 12.0, 12.1 and 12.2 work as a suitable anti-virus solution for Hitachi NAS Platform. Tests against Hitachi NAS Platform version 11.3 and earlier are not supported with Kaspersky Anti-Virus for Windows Server Enterprise Edition using ICAP.

Test Results

Figure 11 demonstrates the successful binding between HNAS version 12.0 with Kaspersky Anti-Virus.

Registered Virus Scan Engines

Scan Engine	Port	Service Name	Enabled	Status	
172.17.29.121	1344	avscan	Yes	OK	details
172.17.29.217	1344	avscan	Yes	OK	details
172.17.29.218	1344	avscan	Yes	OK	details

Check All | Clear All

Figure 11

Figure 12 demonstrates the successful binding between HNAS versions 12.1 and 12.2 with Kaspersky Anti-Virus.

Registered Virus Scan Engines

Scan Engine	Port	Service Name	Enabled	Status	
172.17.29.121	1344	avscan	Yes	OK	details
172.17.29.217	1344	avscan	Yes	OK	details
172.17.29.218	1344	avscan	Yes	OK	details

Check All | Clear All

Figure 12

Figure 13 shows successful scanning of clean files in HNAS version 12.0. In this case there were 47,881 clean scans.

Virus Statistics

EVS: TSM71-2 change...

Last Reset:
2014-11-11 16:03:15 (UTC-0800) reset

Last Refreshed: 2014-11-11 16:15:13 (UTC-0800)

Statistics

Number of virus scans:	47881
Number of clean scans:	47881
Number of errored scans:	0

Additional statistics

Number of infections found:	0
Action taken:	
Number of infections repaired:	0
Number of files deleted:	0
Number of files quarantined:	0

Figure 13

Figure 14 shows successful scanning of clean files in HNAS version 12.1. In this case there were 67,935 clean scans and no virus infections found.

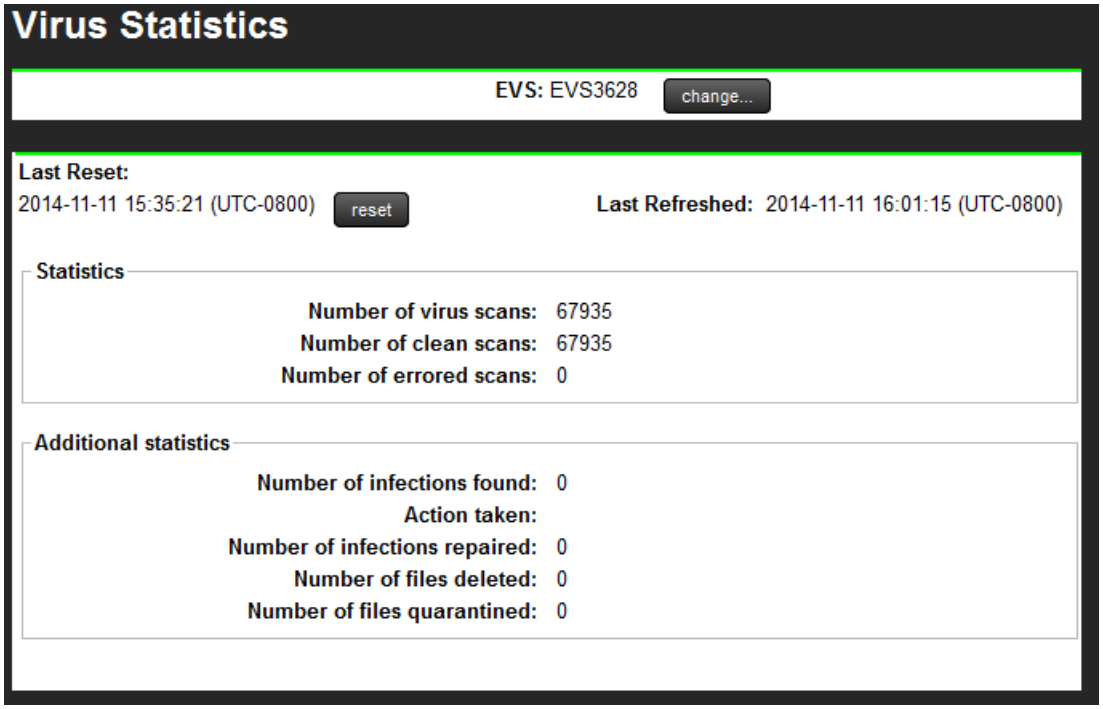

Figure 14

Figure 15 shows the statistics for Real-time protection of iCAP storage systems. Note the successful identification and quarantine of infected objects.

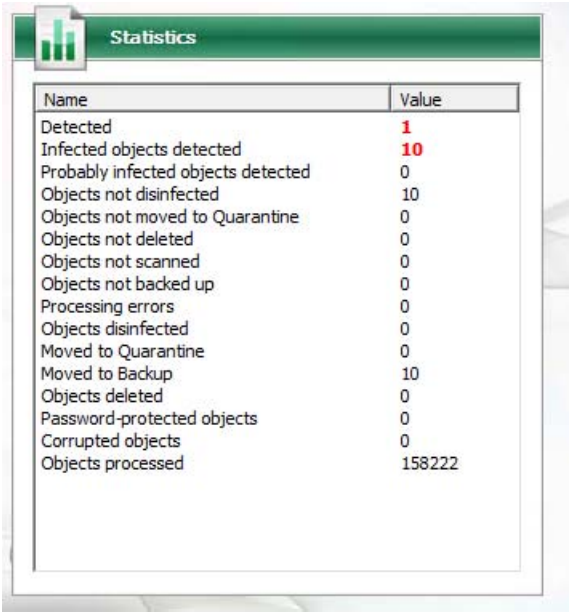

Figure 15

The following performance results are from a Windows server running Kaspersky Anti-Virus while files are being actively generated on an HNAS share and being scanned by Kaspersky Anti-Virus.

Performance Run #1

Memory	
Available KBytes	7,247,979.000
Available MBytes	7,077.750

Process	kavfs	kavfsgt	kavfswp	kavfswp#1
ID Process	2,428.000	920.000	280.000	1,260.000
IO Data Bytes/sec	48,064.182	0.000	12,586,749.146	64.253
Private Bytes	19,714,048.000	1,768,448.000	134,473,728.000	166,902,784.000
Thread Count	6.000	5.000	29.750	19.000
Virtual Bytes	135,225,344.000	54,906,880.000	297,826,304.000	420,397,056.000
Working Set	30,063,616.000	6,347,776.000	40,138,752.000	52,706,304.000

Processor	_Total
% C1 Time	81.175
% C2 Time	0.000
% C3 Time	0.000
% DPC Time	2.135
% Idle Time	81.175
% Interrupt Time	0.430
% Privileged Time	10.543
% Processor Time	15.100
% User Time	4.557
C1 Transitions/sec	758.598
C2 Transitions/sec	0.000
C3 Transitions/sec	0.000
DPC Rate	19.750
DPCs Queued/sec	1,048.010
Interrupts/sec	3,653.791

Processor Information	_Total
% C1 Time	81.175
% C2 Time	0.000
% C3 Time	0.000
% DPC Time	2.135
% Idle Time	84.900
% Interrupt Time	0.430
% of Maximum Frequency	100.000
% Performance Limit	100.000
% Priority Time	14.788
% Privileged Time	10.543
% Privileged Utility	12.576
% Processor Performance	100.000
% Processor Time	15.100
% Processor Utility	18.821
% User Time	4.557
Average Idle Time	2,140,207.379
C1 Transitions/sec	758.608
C2 Transitions/sec	0.000
C3 Transitions/sec	0.000
Clock Interrupts/sec	128.005
DPC Rate	19.750
DPCs Queued/sec	1,048.008
Idle Break Events/sec	758.608
Interrupts/sec	3,653.796
Parking Status	0.000
Performance Limit Flags	0.000
Processor Frequency	2,400.000
Processor State Flags	0.000

Performance Run #2

Memory	
Available KBytes	7,249,577.000
Available MBytes	7,079.250

Process	kavfs	kavfsgt	kavfswp	kavfswp#1
ID Process	2,428.000	920.000	280.000	1,260.000
IO Data Bytes/sec	48,075.288	0.000	12,612,999.443	34.143
Private Bytes	20,258,816.000	1,738,752.000	135,574,528.000	166,912,000.000
Thread Count	6.000	5.000	30.250	19.000
Virtual Bytes	135,225,344.000	54,906,880.000	299,609,088.000	420,397,056.000
Working Set	30,027,776.000	6,340,608.000	41,621,504.000	53,054,464.000

Processor	_Total
% C1 Time	83.673
% C2 Time	0.000
% C3 Time	0.000
% DPC Time	2.175
% Idle Time	83.673
% Interrupt Time	0.339
% Privileged Time	10.793
% Processor Time	15.482
% User Time	4.689
C1 Transitions/sec	487.766
C2 Transitions/sec	0.000
C3 Transitions/sec	0.000
DPC Rate	36.250
DPCs Queued/sec	996.650
Interrupts/sec	3,786.766

Processor Information	_Total
% C1 Time	83.673
% C2 Time	0.000
% C3 Time	0.000
% DPC Time	2.175
% Idle Time	84.518
% Interrupt Time	0.339
% of Maximum Frequency	100.000
% Performance Limit	100.000
% Priority Time	15.234
% Privileged Time	10.793
% Privileged Utility	9.603
% Processor Performance	100.000
% Processor Time	15.482
% Processor Utility	16.326
% User Time	4.689
Average Idle Time	3,430,920.682
C1 Transitions/sec	487.764
C2 Transitions/sec	0.000
C3 Transitions/sec	0.000
Clock Interrupts/sec	128.001
DPC Rate	36.250
DPCs Queued/sec	996.724
Idle Break Events/sec	487.764
Interrupts/sec	3,786.868
Parking Status	0.000
Performance Limit Flags	0.000
Processor Frequency	2,400.000
Processor State Flags	0.000

Performance Run #3

Memory	
Available KBytes	7,237,123.765
Available MBytes	7,067.000

Process	kavfs	kavfsgt	kavfswp	kavfswp#1
ID Process	2,428.000	920.000	280.000	1,260.000
IO Data Bytes/sec	48,018.341	0.000	0.000	46.460
Private Bytes	20,136,658.824	1,764,171.294	137,217,204.706	166,925,733.647
Thread Count	5.000	4.941	33.294	19.000
Virtual Bytes	133,902,336.000	54,829,056.000	304,207,269.647	420,397,056.000
Working Set	29,965,372.235	6,338,198.588	43,232,557.176	53,749,639.529

Processor	_Total
% C1 Time	71.350
% C2 Time	0.000
% C3 Time	0.000
% DPC Time	2.290
% Idle Time	71.350
% Interrupt Time	0.504
% Privileged Time	12.311
% Processor Time	27.601
% User Time	15.290
C1 Transitions/sec	1,396.593
C2 Transitions/sec	0.000
C3 Transitions/sec	0.000
DPC Rate	17.294
DPCs Queued/sec	1,493.143
Interrupts/sec	6,403.168

Processor Information	_Total
% C1 Time	71.350
% C2 Time	0.000
% C3 Time	0.000
% DPC Time	2.290
% Idle Time	72.399
% Interrupt Time	0.504
% of Maximum Frequency	100.000
% Performance Limit	100.000
% Priority Time	26.981
% Privileged Time	12.311
% Privileged Utility	14.721
% Processor Performance	100.000
% Processor Time	27.601
% Processor Utility	28.715
% User Time	15.290
Average Idle Time	1,021,785.687
C1 Transitions/sec	1,396.595
C2 Transitions/sec	0.000
C3 Transitions/sec	0.000
Clock Interrupts/sec	128.001
DPC Rate	17.294
DPCs Queued/sec	1,493.141
Idle Break Events/sec	1,396.595
Interrupts/sec	6,403.165
Parking Status	0.000
Performance Limit Flags	0.000
Processor Frequency	2,400.000
Processor State Flags	0.000

The Hitachi NAS Platform performance results in Figure 16 show the scan performance latency.

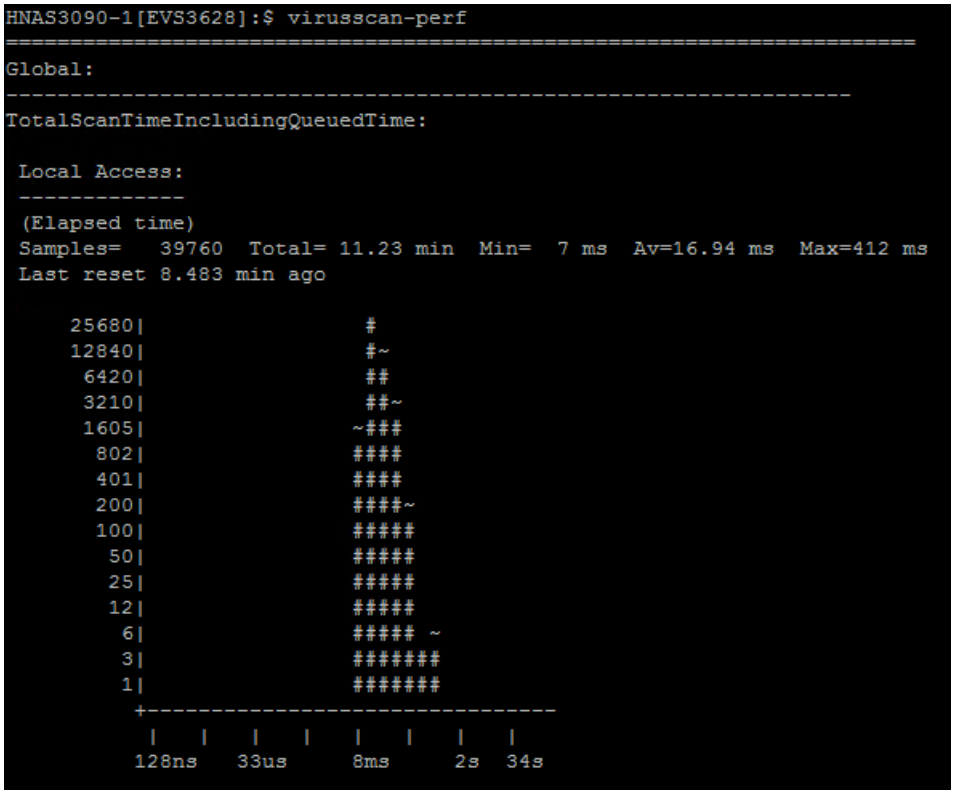

Figure 16

Figure 17 shows the various EICAR infections that were deleted from Hitachi NAS Platform.

```
HNAS3090-1[EVS3628]:$ virusscan-failures
  Status       Path to file
  -----------  ------------------------------------------------------------
  Deleted      \VSPfs00\eicar.com.txt
  Deleted      \VSPfs00\eicar.com
  Deleted      \VSPfs00\eicar.exe
  Deleted      \VSPfs00\eicarcom2.zip
  Deleted      \VSPfs00\eicar_com.zip
  Deleted      \VSPfs00\riserun\eicar.com
  Deleted      \VSPfs00\riserun\eicar.com.txt
  Deleted      \VSPfs00\riserun\eicarcom2.zip
  Deleted      \VSPfs00\riserun\eicar_com.zip
  Deleted      \VSPfs00\riserun\eicar.exe
```

Figure 17

For More Information

Hitachi Data Systems Global Services offers experienced storage consultants, proven methodologies and a comprehensive services portfolio to assist you in implementing Hitachi products and solutions in your environment. For more information, see the Hitachi Data Systems Global Services website.

Live and recorded product demonstrations are available for many Hitachi products. To schedule a live demonstration, contact a sales representative. To view a recorded demonstration, see the Hitachi Data Systems Corporate Resources website. Click the **Product Demos** tab for a list of available recorded demonstrations.

Hitachi Data Systems Academy provides best-in-class training on Hitachi products, technology, solutions and certifications. Hitachi Data Systems Academy delivers on-demand web-based training (WBT), classroom-based instructor-led training (ILT) and virtual instructor-led training (vILT) courses. For more information, see the Hitachi Data Systems Services Education website.

For more information about Hitachi products and services, contact your sales representative or channel partner or visit the Hitachi Data Systems website.

Hitachi Data Systems Corporation

Corporate Headquarters
2845 Lafayette Street, Santa Clara, California 95050-2627 USA
www.HDS.com

Regional Contact Information
Americas: +1 408 970 1000 or info@HDS.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@HDS.com
Asia-Pacific: +852 3189 7900 or hds.marketing.apac@HDS.com

AS-346-01, May 2015