Implement McAfee VirusScan Enterprise and McAfee VirusScan Enterprise for Storage using ICAP with Hitachi NAS Platform

Implementation Guide

By John Goodman

October 7, 2013
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

Purpose............................................................................................................. 1
Hardware and Software Summary............................................................... 2

**McAfee VirusScan Enterprise Overview**....................................................... 3
System Requirements.................................................................................. 3
Hardware and Operating System............................................................... 3

**Configuration Setup**.................................................................................... 4
Configuration Components......................................................................... 5

**Implementation of McAfee VirusScan Enterprise for Storage**......................... 6
General information.................................................................................... 6
Configure HNAS Using SMU Wizards............................................................ 7
Install a Microsoft® Windows Server® 2008 R2 SP1 Virtual Machine
.................................................................................................................. 13
Install McAfee VirusScan Enterprise 8.8....................................................... 13
Install McAfee VirusScan Enterprise for Storage 1.02.................................. 14
Install any McAfee VirusScan Enterprise HotFixes...................................... 14
Install any McAfee VirusScan Enterprise for Storage HotFixes.................... 14

**Configure McAfee VirusScan Enterprise**..................................................... 15

**Enable Virus Scan on HNAS 3080/3090**....................................................... 18
Enable McAfee VirusScan on HNAS.............................................................. 18
VirusScan Statistics.................................................................................... 20
Implement McAfee VirusScan Enterprise and McAfee VirusScan Enterprise for Storage using ICAP with Hitachi NAS Platform

Implementation Guide

This document describes the implementation and configuration of McAfee VirusScan Enterprise 8.8 and VirusScan Enterprise for Storage 1.02 with Hitachi NAS Platform (HNAS).

Purpose

The purpose of this guide is to demonstrate that McAfee VirusScan Enterprise 8.8 scans files contained on HNAS CIFS shares, and to prove that all components can be integrated and are functional.

This implementation guide is intended for an administrator deploying CIFS protocol via HNAS with McAfee VirusScan 8.8 and VirusScan for Storage 1.0.2. You need to be familiar with the following products to benefit from this document:

- Hitachi NAS Platform System Installation Guide
- Hitachi NAS Platform, and Hitachi High-Performance Platform powered by BlueArc Network Administration Guide
- Microsoft® Windows Server® 2008 R2
- McAfee VirusScan 8.8
- McAfee VirusScan for Storage 1.02
Hardware and Software Summary

The following are the components used in this solution:

- HNAS 3080/3090/4060/4080/4100 — 4U rack mountable storage
- Hitachi Unified Storage 100 Family — powerful, scalable, highly reliable modular storage
- Hitachi Compute Rack CR 220 — 2U rack mountable server
- Dell PowerConnect Force 10 Network Switch — CIFS connectivity to the storage network
- Brocade 5100 SAN Switch — backend Fibre channel connectivity between HNAS and storage subsystem
- VMware vSphere 5.1 — industry-leading virtualization platform for building cloud infrastructures
- Microsoft Windows Server 2008 R2 — multi-purpose server software designed to increase the reliability and flexibility of your infrastructure
- McAfee VirusScan Enterprise — combines anti-virus, anti-spyware, firewall, and intrusion prevention technologies to stop and remove malicious software
- McAfee VirusScan Enterprise for Storage — VirusScan Enterprise console plug-in
McAfee VirusScan Enterprise Overview

McAfee VirusScan Enterprise 8.8 and VirusScan Enterprise for Storage 1.02 are an integrated suite of security software. It is comprised of the following:

- McAfee VirusScan Enterprise 8.8
- McAfee VirusScan Enterprise for Storage 1.02

McAfee VirusScan Enterprise combines anti-virus, anti-spyware, firewall, and intrusion prevention technologies to stop and remove malicious software. It also extends coverage to new security risks and reduces the cost of responding to outbreaks with the industry’s lowest impact on system performance.

System Requirements

The following sections describe the system requirements to implement McAfee VirusScan Enterprise and VirusScan Enterprise for Storage with the Hitachi HNAS Platform. We used HNAS model 4080 for this deployment.

Hardware and Operating System

For hardware and operating system requirements, see the system requirements page of the McAfee website (http://www.mcafee.com/us/products/virusscan-enterprise.aspx#vt=vtab-Requirements).

For more information about McAfee VirusScan Enterprise, see the following:

- VirusScan Enterprise for Storage 1.0.2 Hotfix 874576 [https://kc.mcafee.com/corporate/index?page=content&id=KB78329](https://kc.mcafee.com/corporate/index?page=content&id=KB78329)
Configuration Setup

Figure 1 illustrates the configuration diagram.
Configuration Components

Table 1 describes the hardware used in the configuration.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Detail Description</th>
<th>Version</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>HNAS 3080, 3090, 4060, 4080, 4100</td>
<td>• Cluster configuration</td>
<td>11.2.3319.09 and above</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>• 1 × 1 Gb/sec link aggregation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Managed by external SMU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hitachi Unified Storage 100 Family</td>
<td>• 9 × expansion drive trays</td>
<td>130</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>• 24 × 600 GB SAS drivers per tray</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hitachi Compute Rack, Rack Mount Server</td>
<td>• 2 × 6-core Intel Xeon 2.00 GHz E5-2620</td>
<td>CR220H</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>• 48 GB RAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 × Quad port 1 Gb/sec onboard NIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 × Quad Port 1 Gb/sec PCI NIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 × Dual Port Emulex LPe12002 8 Gb Fibre Channel HBA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brocade 5300 SAN Switch</td>
<td>• 8 Gb/sec Fibre Channel switch</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Dell PowerConnect Force 10 Network Switch</td>
<td>• 1 Gb/sec network switch</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

Table 2 describes the software used in the configuration.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere</td>
<td>5.1.0</td>
</tr>
<tr>
<td>McAfee VirusScan Enterprise</td>
<td>8.8 Patch 2 with HotFix805660</td>
</tr>
<tr>
<td>McAfee VirusScan Enterprise for Storage</td>
<td>1.0.2 with HotFix 874576</td>
</tr>
<tr>
<td>Microsoft Windows Server</td>
<td>2008 R2 Enterprise Edition SP1</td>
</tr>
</tbody>
</table>
Implementation of McAfee VirusScan Enterprise for Storage

General information

Virus Scan Enterprise for Storage utilizes a "plug-in" architecture for its scanners and UI which allows an "add-on" implementation to McAfee VirusScan Enterprise. Virus Scan Enterprise for Storage provides protection to numerous storage devices through both ICAP and RPC clients. This ensures that malware does not proliferate into the enterprise network.

The Virus Scan Enterprise for Storage user interface is implemented as a VirusScan Enterprise console plug in. After installing VSE for Storage two new tasks show up in VSE's console; "Network Appliance Filer AV Scanner" and "ICAP AV Scanner". These new tasks provide the client UI for the VSE for Storage product, as shown in Figure 2.

![Diagram of VirusScan Enterprise for Storage](Figure 2)
Configure HNAS Using SMU Wizards

Hitachi NAS Platform is an advanced and integrated network attached storage (NAS) solution. It is a powerful tool for file sharing as well as file server consolidation, data protection and business critical NAS workloads. Our NAS systems are sized for your needs. Hitachi NAS Platform 4080 and 4100 are well suited to data center environments, while NAS Platform 3090 and 4060 handle the workloads of medium sized organizations. Hitachi NAS Platform 3080 is an optimal solution for lower to midrange environments that require high performance and scalability at a lower total cost of ownership (TCO) and price-to-performance profile. With our NAS platforms, you can solve challenges associated with data growth while achieving a low TCO.

- Powerful hardware-accelerated file system that represents the next generation of multiprotocol file services, dynamic provisioning, intelligent tiering, virtualization and cloud infrastructure
- High performance: Up to 2000 MB/sec and 140,000 input/outputs per second (IOPS) per node
- High scalability: Up to 16 PB of usable capacity
- Seamless integration with Hitachi SAN storage, Hitachi Command Suite and Hitachi Data Discovery Suite for advanced search and index across NAS platforms
- Integration with Hitachi Content Platform for active archiving, regulatory compliance and large object storage for cloud infrastructure

Perform this configuration on HNAS before configuring the other hardware.

A basic configuration is required to ready the system for use. This section explains how to use wizards to complete the basic configuration.

The Web Manager administration tool provides a browser-based interface for managing standalone or clustered servers and their attached storage subsystems. This tool allows you to perform most administrative tasks, from any client on the network using a supported web browser.

Your Hitachi NAS Platform ships with the following preconfigured:

- Default IP addresses set for cluster nodes and administrative virtual server (admin EVS)
- Cluster, if it was ordered as part of the system
- Any purchased licenses
- Depending on the type of storage, system drives (SDs) are created and allowed access
Table 3 describes the factory defaults for preconfigured settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Factory Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Password</td>
<td>nasadmin (Changed during initial configuration)</td>
</tr>
<tr>
<td>Manager Password</td>
<td>nasadmin (Changed during initial configuration)</td>
</tr>
<tr>
<td>Admin Password</td>
<td>nasadmin (Changed during initial configuration)</td>
</tr>
<tr>
<td>Admin EVS private IP address (eth1)</td>
<td>192.0.2.2</td>
</tr>
<tr>
<td>Admin EVS public IP address (eth0)</td>
<td>Example: 192.168.31.x</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Example: 255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>Example: 192.168.31.254</td>
</tr>
<tr>
<td>Hostname</td>
<td>Example: myhost</td>
</tr>
<tr>
<td>Domain</td>
<td>Example: mydomain.com</td>
</tr>
</tbody>
</table>

The server is shipped with some default IP addresses already configured (see Table 3 above).

Before connecting the server into your network, ensure that these IP addresses will not conflict with an existing network.
To view and customize network settings:

1. Either connect the KVM or attach an RS-232 null-modem cable (DB-9 female to DB-9 female) from your laptop to the serial port. If this is a serial connection, start a console session using your terminal emulation (such as PuTTY or Windows HyperTerminal) with the following settings:
   - 115,200 b/s
   - 8 data bits
   - 1 stop bit
   - No parity
   - No flow control
   - VT100 emulation

2. Log in to the server as user manager with default password nasadmin. This provides access to the Bali console. Log in as root, if you use a KVM.

3. Enter evsipaddr -l to display the default IP addresses.

4. Enter evsipaddr -e 0 -a -i admin_IP -m netmask -p eth0 to customize the administrative EVS IP address for your local network.

Customize the other IP addresses now or proceed to using the Server Setup Wizard.
After the server is connected to your network, you may configure the system with Server Setup wizard using a supported browser. To configure the system:

1. From a browser, enter http://Web_Manager_IP to launch the Web Manager, and log in as admin. Web_Manager_IP is the public administrative EVS (eth0) address.

2. Navigate to Server Settings > Server Setup Wizard. When accessing the system for the first time, it might prompt you for the following:
   - New licenses, if none are present
   - Allow access to system drives, if none are configured
   - Create a cluster, if a cluster license is installed but the system is not in a cluster

3. Enter the server information, and then click Apply.

4. Modify the Administrative EVS name, cluster node, and EVS settings as needed, and then click apply.

5. Enter DNS server IP addresses, domain search order, WINS servers, NIS domain, and name services ordering, as needed, and then click apply.

6. Enter DNS server IP addresses, domain search order, WINS servers, NIS domain, and name services ordering, as needed, and then click apply.

7. Modify CIFS settings (register the EVS with a domain controller), and then click apply.

8. Specify the email server to which the server can send and relay event notification emails, and then click apply.

9. Change the supervisor password (default: supervisor), and then click apply.

10. Click apply to create a test file system, share, and export.

11. After successfully navigating all pages of the wizard, a configuration summary is displayed, if restarting the file serving service and internal SMU are not required. If a restart is required, the browser navigates to a wait page, and then returns to the home page.
Now configure your backend storage system and assign LUNs to the Hitachi HNAS. Once you have LUNs assigned, resume Hitachi HNAS configuration by doing the following:

1. From a browser, enter http://Web_Manager_IP to launch the Web Manager, and log in as admin. **Web_Manager_IP** is the public administrative EVS (eth0) address.

2. Navigate to **Storage Management > System Drives**. LUNs assigned from backend storage will show in this page.

3. Create an **EVS** for CIFS if you haven't done so. Go to **Server Settings > EVS Management**. Click on the **Add** button and your browser will jump to the add EVS wizard page.
   - **Label**: Name of your EVS
   - **IP Address**: IP Address for EVS
   - **Subnet Mask**: Subnet Mask for EVS
   - **Port**: Select which port for EVS

4. Navigate back to **Storage Management > Storage Pools**. Click on the **Create** button and your browser will jump to Storage Pool Wizard page.
   - Select the appropriate storage pool and go to the next page.
   - Check the available system drive, enter the storage pool label, select the Guideline Chunk Size, and click Next.
   - Verify everything is correct. Click create to finish creating the storage pool.

5. Go to **Storage Management > File System**. Click on the create button and start the create file system wizard.
   - Select a file system by clicking on File System.
   - Select the storage pool on which to create a file system and go to the next page.
   - Enter the size of your file system. Select Disabled if you don't want auto-expand.
   - Enter the label of the file system.
   - Select the **EVS** that you want to assign to the file system.
   - Select **WORM** type.
   - Pick the proper block size for your application requirement.
   - Click OK when finished.
6. We are now ready to create CIFS server and CIFS shares. Go to File Services > CIFS Setup. Click on the add button to start the Add CIFS Server Names wizard page.

- EVS: Make sure the right EVS name was selected.
- CIFS Server Names: Enter the name of the CIFS Server that you want to use and click the Add button on the right.
- Select ADS. Enter AD Server IP Address, DC Admin User name and password then click OK.

7. Navigate to File Services > CIFS Shares. Make sure the right EVS was selected. Click on the add button to start the Add Share wizard.

- Share Name: Enter the CIFS share name
- Enable Virus Scanning: Check this option

<table>
<thead>
<tr>
<th>Follow Symbolic Links:</th>
<th>☑</th>
<th>Follow Global Symbolic Links:</th>
<th>☐</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force Filename to be Lowercase:</td>
<td>☐</td>
<td>Enable ABE:</td>
<td>☐</td>
</tr>
<tr>
<td>Enable Virus Scanning:</td>
<td>☑</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Everything else can be default.
- Click ok and finish adding CIFS share.

8. Next, navigate to File Services > Local Groups. Click on the add button to start the Add Local Group wizard.

- Group: Use existing local group and select Backup Operators
- Members: Enter Admin User's name and click Add
- Click on OK to finish adding local group wizard

After successfully navigating all pages of the wizard, make sure date and time on Hitachi HNAS is synchronized with DC server and all client servers.
Install a Microsoft® Windows Server® 2008 R2 SP1 Virtual Machine

Do the following to install Microsoft Windows Server 2008 R2 SP1.

1. From VMware vCenter, create a new virtual machine (VM) with 8 vCPUs (2 sockets, 4 cores per socket). Allocate 4 GB of memory to the new VM. Use LSI Logic SAS for the SCSI Controller and allocate 40GB of storage for the Hard disk. Allocate at least one Network adapter. Attach the Network Adapter to a standard vNetwork switch.

2. Place the Windows Server DVD into the DVD-ROM drive of the ESX server and assign the new VM access to the DVD-ROM.

3. Boot the new VM.

4. Follow the install wizard to complete the OS installation.

5. Use a strong password when creating the local administrator account

6. Install all Windows Server service packs and patches, so the installation is up to date.

7. Join this server to an Active Directory domain prior to installing McAfee VirusScan.

For more information, see the Microsoft TechNet article “Installing Windows Server 2008 R2.”

Install McAfee VirusScan Enterprise 8.8

To install McAfee VirusScan 8.8 software, do the following:

1. Open the folder for McAfee VirusScan, double click SetupVSE to start installation.

2. Follow the install wizard to complete the McAfee VirusScan installation.

3. Restart the VirusScan server after installation.

4. After reboot, Navigate to Administrative Tools > Services. Verify McAfee McShield service started and start type is set to Automatic.
Install McAfee VirusScan Enterprise for Storage 1.02

To install McAfee VirusScan Enterprise for Storage 1.02 software, do the following:

1. Open the folder for McAfee VirusScan Enterprise for Storage, double click Setup to start installation.

2. Follow the install wizard to complete the McAfee VirusScan Enterprise for Storage installation.

3. After finishing the installation, navigate to Administrative Tools > Services. Verify McAfee VirusScan Enterprise for Storage service started and the start type is set to Automatic.

Install any McAfee VirusScan Enterprise HotFixes

To install any McAfee HotFixes, do the following:

1. Open the folder for the McAfee HotFix and double click the install application to start the installation.

2. Follow the install wizard to complete the McAfee HotFix installation.

3. After the HotFix has been installed, you may need to reboot the server.

4. Repeat steps 1-3 for all necessary HotFixes.

Install any McAfee VirusScan Enterprise for Storage HotFixes

To install any McAfee HotFixes, do the following:

1. Open the folder for the McAfee HotFix and double click the install application to start the installation.

2. Follow the install wizard to complete the McAfee HotFix installation

3. After the HotFix has been installed, you may need to reboot the server.

4. Repeat steps 1-3 for all necessary HotFixes.
Configure McAfee VirusScan Enterprise

Do the following to configure McAfee VirusScan Enterprise for Storage.

1. Navigate to Start > All Programs > McAfee > VirusScan Console to launch VirusScan Console.

2. Double click on ICAP AV Scanner.

3. Under the Connections and Server tab, click the “Accept scan requests from these ICAP clients only” box, then click the Add button to add the IP address of HNAS EVS. Enter name or IP address the EVS that was created in the previous section, then click OK. Enter the IP address for McAfee VSES server in the Bind address field, then click OK.
4. Go to Scan Items tab. Select All files or add additional file types.

5. Go to the Performance Tab and make the appropriate setting for virus detection.

6. Go to the Actions tab and make the appropriate selection for virus detection.
7. Select the Reports tab. Make any changes if needed. Click OK when finished.
Enable Virus Scan on HNAS 3080/3090

Enable McAfee VirusScan on HNAS

After finished configuring McAfee VirusScan Enterprise for Storage, do the following to enable virus scan on HNAS.

1. From a browser, enter http://Web_Manager_IP to launch the Web Manager, and log in as admin. Web_Manager_IP is the public administrative EVS (eth0) address.
   - Navigate to Data Protection > Virus Scanning.
   - EVS: Select EVS for the CIFS share
   - Enable Virus Scanning: Click on enable button to enable this feature
   - Scan All File Types: Select this option or add additional file extensions
   - Click the Switch to ICAP mode link to enable the ICAP scan engine support
   - Click the Add button to add the IP of McAfee VirusScan Enterprise for Storage. Leave all other fields as the default.
settings, Port:1344 and Service Name: AVSCANRESP. Click the OK button to complete.

- Verify that the Registered Virus Scan Engines Status is OK.

<table>
<thead>
<tr>
<th>Registered Virus Scan Engines</th>
<th>Port</th>
<th>Service Name</th>
<th>Enabled</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.17.29.16</td>
<td>1344</td>
<td>AVSCANRESP</td>
<td>Yes</td>
<td>OK</td>
</tr>
</tbody>
</table>

- From the VirusScan Console right click on ICAP AV Scanner and select Statistics. Verify the correct EVS IP address and that the Status is Receiving scan requests.

- Close ICAP Scanner Statistics and VirusScan Console when done.
VirusScan Statistics

HNAS provides Virus Scan statistics for each registered EVS, as shown in Figure 3. During the scan process, HNAS Virus Scan updates the statistics providing information such as number of virus scans or number of clean scans to name.

**Virus Statistics**

<table>
<thead>
<tr>
<th>EVS: evs1</th>
<th>change...</th>
</tr>
</thead>
</table>

**Last Reset:** 2013-09-29 12:07:10 (UTC-0700)  | **Last Refreshed:** 2013-09-26 11:06:00 (UTC-0700) |

<table>
<thead>
<tr>
<th>Statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of virus scans:</td>
<td>864185</td>
</tr>
<tr>
<td>Number of clean scans:</td>
<td>384598</td>
</tr>
<tr>
<td>Number of errored scans:</td>
<td>13825</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of infections found:</td>
<td>10</td>
</tr>
<tr>
<td>Action taken:</td>
<td></td>
</tr>
<tr>
<td>Number of infections repaired:</td>
<td>0</td>
</tr>
<tr>
<td>Number of files deleted:</td>
<td>0</td>
</tr>
<tr>
<td>Number of files quarantined:</td>
<td>0</td>
</tr>
</tbody>
</table>

**Figure 3**
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.