Data Protection on Hitachi NAS Platform with Kaspersky Anti-Virus

Best Practices Guide

By John Goodman

December 1, 2014
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

Solution Components.................................................................2
  Hardware Components.................................................................2
  Software Components.................................................................4

Best Practices..................................................................................5
  Kaspersky Anti-Virus for Windows Servers Setup Procedure for Remote Program Call.................................................................7
  Kaspersky Anti-Virus for Windows Servers Setup Procedure for ICAP.................................................................16
  Administrative Options and Considerations........................................22

Conclusion......................................................................................30
Data Protection on Hitachi NAS Platform with Kaspersky Anti-Virus

Best Practices Guide

The technical paper describes best practices for Hitachi NAS Platform when using Kaspersky Anti-Virus for Windows Servers Enterprise Edition. Included is information for setup and using this solution to protect data on network-attached storage.

NAS Platform provides integrated antivirus functionality. This allows administrators to manage antivirus behavior from the NAS Platform interface, as well as from the Kaspersky Anti-Virus console to help protect corporate data from the spread of malicious virus code.

You can take advantage of protection from Kaspersky Anti-Virus protection of network-attached storage feature to ensure business continuity by protecting data on network-attached storage devices against viruses and other malware.

---

**Note** — These procedures were developed in a lab environment. Many things affect production environments beyond prediction or duplication in a lab environment. Follow recommended practice by conducting proof-of-concept testing for acceptable results before implementing this solution in your production environment. Test the implementation in a non-production, isolated test environment that otherwise matches your production environment.
Solution Components

These are the hardware and software components used in the Hitachi Data System labs to develop this best practices document.

Hardware Components

Table 1 lists the hardware components used in testing to prepare these best practices.

Table 1. Hardware Components

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Detail Description</th>
<th>Version</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hitachi NAS Platform 3080, 3090, 4080, 4100</td>
<td>Clustered and single node configurations</td>
<td>For RPC:</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1 Gb/sec and 10 Gb/sec link aggregations</td>
<td>11.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11.3</td>
<td>11.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Managed by external SMU</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For ICAP and RPC:</td>
<td>12.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.1</td>
<td>12.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2</td>
<td>12.2</td>
<td></td>
</tr>
<tr>
<td>Hitachi Unified Storage 100 Family</td>
<td>32 GB cache</td>
<td>0930/A-S</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>113 TB raw capacity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hitachi Unified Storage VM</td>
<td>118 GB cache</td>
<td>73-03-01-00/00</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>32 TB physical capacity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hitachi Virtual Storage Platform G1000</td>
<td>86.25 GB cache</td>
<td>80-02-00-00/04</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>201.50 TB physical capacity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hitachi Compute Rack 220H</td>
<td>2 x 6-core Intel Xeon E5-2620 processor, 2.00 GHz</td>
<td></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>
</tbody>
</table>
Hitachi NAS Platform

Hitachi NAS Platform is an advanced and integrated network attached storage (NAS) solution. It provides a powerful tool for file sharing, file server consolidation, data protection, and business-critical NAS workloads.

- Powerful hardware-accelerated file system with multi-protocol file services, dynamic provisioning, intelligent tiering, virtualization, and cloud infrastructure
- Seamless integration with Hitachi SAN storage, Hitachi Command Suite, and Hitachi Data Discovery Suite for advanced search and index
- Integration with Hitachi Content Platform for active archiving, regulatory compliance, and large object storage for cloud infrastructure

NAS Platform with antivirus protection enabled scans files as they are created, modified (writes) and opened (reads). This method is more effective at detecting viruses before they can spread and compromise data. These scans occur as needed. This minimizes the server and network loads when compared to intensive file system scans.

To communicate with the Kaspersky Anti-Virus server, this Hitachi NAS Platform antivirus solution uses one of the following:

- Internet content adaptation protocol (ICAP)
- An authenticated CIFS connection via remote procedure call (RPC)

---

**Figure 1**

1. Client attempts to open, create, or modify a file
2. The HNAS determines if the file needs to be scanned based on the extension and notifies the AV server
3. The AV server processes the file and notifies HNAS of the result
4. Client file access is granted or denied by HNAS based on the scan results
Software Components

Table 2 lists the hardware components used in testing to prepare these best practices.

Table 2. Software Components

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere</td>
<td>5.5.0</td>
</tr>
<tr>
<td>Kaspersky Anti-Virus for Windows Servers Enterprise Edition</td>
<td>RPC only:</td>
</tr>
<tr>
<td></td>
<td>▪ 8.0.1.923 with Hitachi NAS Platform patch</td>
</tr>
<tr>
<td></td>
<td>▪ 8.0.2.x</td>
</tr>
<tr>
<td></td>
<td>RPC and ICAP supported:</td>
</tr>
<tr>
<td></td>
<td>▪ 8.0.2.xx</td>
</tr>
<tr>
<td>Microsoft® Windows Server®</td>
<td>2012 R2 Standard</td>
</tr>
</tbody>
</table>

Version 8.0.1.923 of Kaspersky Anti-Virus for Windows Servers Enterprise Edition must have the patch for Hitachi NAS Platform. Download the patch from this URL: [http://support.kaspersky.com/11514](http://support.kaspersky.com/11514)

**Kaspersky Anti-Virus for Windows Servers Enterprise Edition**

*Kaspersky Anti-Virus for Windows Servers Enterprise Edition* ensures business continuity by protecting data on network-attached storage devices against viruses and other malware. This high-performance scanning solution deploys on one or more servers running Microsoft Windows Server or on virtual machines with a VMware vSphere High Availability cluster.

Kaspersky Anti-Virus deploys in affordable multi-filer or high-availability multi-scanner configurations to deliver the power of parallel processing for optimal load balancing and flexible failover protection.
Best Practices

To detect and stop viruses before they spread, Hitachi NAS Platform integrates antivirus functionality into the NAS Platform system software. NAS Platform integrated antivirus software communicates with Kaspersky Anti-Virus to provide protection against viruses by scanning files produced by Microsoft Windows® clients and other CIFS/SMB clients.

Virus scanning activity is in real-time and transparent to end users. It occurs when either of the following happens:

- A requesting user or application opens or reads a file
- A file is created or written

If a virus is found, NAS Platform marks the file as infected. It then deletes or denies access to the file.

NAS Platform provides as much information as possible to the storage administrator, making the behavior easily configurable. This information includes the following, among other things:

- Statistics about the status of a virus scans
- Information about the virus scan servers
- The list of file types to be scanned

Virus scanning on NAS Platform is enabled and individually configured for each enterprise virtual server (EVS). After the initial configuration, CIFS shares that belong to an EVS can be disabled from virus scanning on an individual basis.

The EVS is a virtual or logical NAS system with an individual IP address. Each EVS has its own set of CIFS shares and network file system (NFS) exports.

When using the RPC protocol, do the following:

- Enter each EVS that is to be scanned for malicious code in the Kaspersky Anti-Virus protection scope settings. This is under the protection of network-attached storage within the Kaspersky Anti-Virus console.

When using ICAP, do the following:

- Change the scan mode on the EVS to ICAP.
- Register the Kaspersky Anti-Virus server as a scan engine in the SMU management interface, under Registered Virus Scan Engines.
NAS Platform proactively submits files for scanning to Kaspersky Anti-Virus on both of the following:

- Read (open)
- Modifications associated with a write (close).

If a file has not been verified by a scan engine as clean, it needs to be scanned before the file can be accessed. However, scanning for viruses when a client is trying to access the file takes time, even on read only. To reduce this latency, files are automatically added to a scan queue as soon as they are created or modified, and when files are closed (on writes).

Queued files are scanned promptly, expediting the detection of viruses in new or modified files. This makes it unlikely that a virus-infected-file will remain dormant on the system for a long period of time.

If virus scanning is temporarily disabled, files continue to be marked as needing to be scanned. In this scenario, when virus scanning is re-enabled, files that were changed are rescanned the next time they are accessed by a client or user.

If virus scanning is enabled but no virus scan servers are available, access to files marked as needing to be scanned will be denied until a virus scan server becomes available. When a virus scan server is available, the user can access the file after it has been scanned.

Kaspersky Anti-Virus registers with Hitachi NAS Platform using one of the following:

- A remote procedure call (RPC)
- Microsoft NTLM
- A CIFS connection
- ICAP

You can register multiple instances of Kaspersky Anti-Virus to register with the same NAS Platform instance to provide for redundancy and performance.

When deploying multiple instances of Kaspersky Anti-Virus, NAS Platform automatically distributes scanning activity among them using a round robin load-balancing scheme. By load balancing across multiple scan servers, performance and scan throughput can be increased as well as scan engine redundancy.

Obtain high availability of Kaspersky Anti-Virus scan engines using a VMware vSphere High Availability cluster when installing Kaspersky Anti-Virus on a virtual machine within the cluster. Additionally, NAS Platform actively monitors connections to registered scan engines. If a scan engine fails or goes down, NAS Platform automatically distributes that server's pending scans between the remaining scan servers. Using vSphere High Availability and NAS Platform provides a higher level of antivirus redundancy and availability.
Kaspersky Anti-Virus for Windows Servers Setup Procedure for Remote Program Call

The following are the three major steps to the initial configuration and setup:

1. "Shared Local User Group Configuration," starting on page 7

Shared Local User Group Configuration

For Kaspersky Anti-Virus for Windows Servers Enterprise Edition to work with Hitachi NAS Platform, create a shared account. This account must have the appropriate permissions in the administrative domain for managing access to the shares that will have virus scanning enabled.

Because virus scanning is a form of data protection, it is recommended that the same shared account be used for the following:

- The setup of the backup operator local group on Hitachi NAS Platform
- The protection of network-attached storages in Anti-Virus for Windows Servers.

On Hitachi NAS Platform systems, you can assign an account for each EVS. If the EVS inherits the global configuration, then you can set the backup operator local group once. Then, any EVS that uses the global configuration inherits the backup operator local group settings.

To configure a shared account, do the following.

1. From the SMU home page, on the **File Services** menu, click **Local Groups**.
2. Set the EVS security context by clicking **Change**.
   - If the EVS to be scanned inherits its file system security from the global configuration, then click **Global Configuration**.
   - If the EVS to be scanned does not inherit its file system security from the global configuration, click the EVS to be scanned.
3. In the **Action** section, click **Add**.
4. Select the existing Backup Operators group. This is used for virus scanning.
5. In the Members text box, type the user name of the domain user. Use the following format when entering the domain user:
   \texttt{Domain\username}

   In the figures below, user \texttt{ISVLAB\avuser} the virus scan user. This user is also a member of the Backup Operators group within the domain.

6. Click \textbf{Add}.

7. Click \textbf{OK}.

Figure 2 on page 8 shows the \textbf{Local Groups} page from Hitachi NAS Platform.

![Figure 2](image1)

**Figure 2**

Figure 3 shows the \textbf{Add Local Group} page on Hitachi NAS Platform.

![Figure 3](image2)

**Figure 3**
Kaspersky Anti-Virus for Windows Servers Enterprise Edition Setup Procedure for Hitachi NAS Platform using RPC

Remote procedure call (RPC) is one of the protocols used for communication between Hitachi NAS Platform and Kaspersky Anti-Virus for Windows Servers Enterprise Edition for scanning requests of files. When a request is sent to the scan engine to scan a file, the scan engine then uses the CIFS protocol to access the file and perform any scan operations.

NAS Platform does not support scanning of files on NFS shares. If sharing an NAS Platform file system is between NFS and CIFS, enable virus scanning on the CIFS share to ensure protection of all CIFS clients. To ensure proper antivirus protection using the RPC option, you must install Kaspersky Anti-Virus as follows:

- Only on a Microsoft Windows Server
- Located in the same domain as the Hitachi NAS Platform system.

Kaspersky Anti-Virus for Windows Servers Enterprise Edition system requirement include the following:

- One of the following versions of Microsoft Windows Server
  - 2003 Standard or Enterprise Edition (x86/x64)
  - 2003 R2 Standard or Enterprise Edition (x86/x64)
  - 2008 Standard, Enterprise, or Datacenter edition, including Core mode (x86/x64)
  - 2008 R2 Standard, Enterprise or Datacenter edition, including Core mode (x86/x64)
  - 2008 Microsoft Hyper-V® R2 Release
  - 2012 Standard or Enterprise Edition
  - 2012 R2 Standard or Enterprise Edition

- Intel Xeon 51xx processor or Intel Xeon 53xx processor, 1.86 GHz or faster
- 2 GB RAM
- 1 GB disk space recommended.

A single Kaspersky Anti-Virus for Windows Servers Enterprise Edition scan engine can support multiple EVS clients. For sites with larger scan volumes, you can use multiple scan engines to support one or more EVS clients.
After installing Kaspersky Anti-Virus for Windows Servers Enterprise Edition and the relevant patch for Hitachi NAS Platform compatibility, configure the antivirus server and EVS clients using the following procedures.

**Configure NetApp Storage System Properties**

Before adding an EVS to Kaspersky Anti-Virus for Windows Servers Enterprise Edition, configure the properties of the real-time protection of NetApp storage systems. Do this by adding the domain user that was added in the Shared Local Group configuration on Hitachi NAS Platform.

The user name is entered as the user name in “Shared Local User Group Configuration,” starting on page 7, `<domain>\<user name.`

To add the domain user, do the following.

1. Open **Real-time protection of NetApp storage systems**.
   - (1) From the Kaspersky Anti-Virus console, select and expand **Protection of network-attached storages**.
   - (2) Click **Real-time protection of NetApp storage systems**.

   Figure 4 shows **Real-time protection of NetApp storage systems** on Kaspersky Anti-Virus.

2. Under **Properties**, click the **Properties** link.

   Figure 5 on page 11 shows the **Properties** area on **Real-time protection of NetApp storage systems**.
3. Under **NetApp storage systems connection** settings, type the user name as used in “Shared Local User Group Configuration,” starting on page 7, then click **Apply** and **OK**.

- Use this format when typing the user name:

  `<domain>\<user name>`

Figure 6 on page 12 shows the **Real-time protection of NetApp storage systems properties configuration** dialog box.
Add an EVS to Kaspersky Anti-Virus for Windows Servers Enterprise Edition

To add an EVS to Kaspersky Anti-Virus for Windows Servers Enterprise Edition, do the following.

1. Open **Real-time protection of NetApp storage systems**.
   
   (1) From the Kaspersky Anti-Virus Console, select and expand **Protection of network-attached storages**.
   
   (2) To view the properties, click **Real-time protection of NetApp storage systems**.

   Figure 7 on page 13 shows the location of **Real-time protection of NetApp storage systems**.
2. Add the EVS on Hitachi NAS Platform.

(1) Under **Properties**, click the **Configure protection scope** link:

Figure 8 shows the **Properties** area on the **Real-time protection of NetApp storage systems** page.
(2) On the **Protection scope settings** tab, do the following:

i. Anywhere under **Protection scope**, right-click in the blank area (Figure 9).

ii. Click **Add protection scope**.

iii. Type the IP address of the EVS on Hitachi NAS Platform to be scanned on the **Add protection scope** dialog box and then click **OK** (Figure 10).

![Figure 9](image1)

![Figure 10](image2)
Figure 11 shows the newly added EVS to the **Protection scope settings** tab.

![Real-time protection of NetApp storage systems](image)

**Figure 11**

**Hitachi NAS Platform Setup Procedure for Kaspersky Anti-Virus for Windows Servers Enterprise Edition for RPC**

To setup Hitachi NAS Platform for use with Kaspersky Anti-Virus Anti-Virus for Windows Servers Enterprise Edition, do the following.

1. From the Hitachi NAS Platform home page, click **Data Protection** and then click **Virus Scanning**.
2. On the Virus Scanning page, select the EVS on which to enable virus scanning.
3. If **Mode** is set to **ICAP**, click the **Switch to RPC Mode** link to change to **RPC** mode.

**Figure 12** shows the **Switch to RPC mode link**.

**Note** — Virus scanning cannot be enabled on an EVS until a virus scan server has been registered.
4. Enable Virus Scanning: From the CIFS Share Detail page

   (1) From Home on Hitachi NAS Platform, click File Services.

   (2) Click CIFS Shares.

   (3) Click CIFS Share Details.

   (4) Select the Enable Virus Scanning text box.

   This enables virus scanning services on Hitachi NAS Platform for each selected share on an EVS. Virus scanning can be stopped on an individual share by unchecking (clearing) the Enable Virus Scanning check box for that share.

   Figure 13 shows the check boxes available on CIFS Share Details.

   ![Check Boxes](image)

   **Figure 13**

   Kaspersky Anti-Virus for Windows Servers Enterprise Edition automatically registers with Hitachi NAS Platform. Once registered, the scan engine is displayed in the Registered Virus Scan Engines list.

5. To enable virus scanning for the selected EVS after Kaspersky Anti-Virus for Windows Servers Enterprise Edition is registered, click Enable on the Virus Scanning page.

   The virus scan engine now actively scans the EVS shares on Hitachi NAS Platform.

   **Kaspersky Anti-Virus for Windows Servers Setup Procedure for ICAP**

   The following are the two major steps to the initial configuration and setup:


   In addition to RPC, Hitachi NAS Platform can send scan requests using Internet content adaptation protocol (ICAP) to Kaspersky Anti-Virus for
Windows Servers Enterprise Edition. When sending a request to the scan engine to scan a file, information about the file is sent using ICAP to the scan engine to perform any scan operations. If the file is infected, Kaspersky Anti-Virus sends a response to Hitachi NAS Platform of infection, and the NAS Platform processes the file.

NAS Platform does not support scanning of files on NFS shares. If sharing a NAS Platform file system between NFS and CIFS, enable virus scanning on the CIFS share to ensure protection of all CIFS clients.

Kaspersky Anti-Virus for Windows Servers Enterprise Edition system requirements include the following:

- One of the following versions of Microsoft Windows Server
  - 2003 Standard or Enterprise Edition (x86/x64)
  - 2003 R2 Standard or Enterprise Edition (x86/x64)
  - 2008 Standard, Enterprise, or Datacenter edition, including Core mode (x86/x64)
  - 2008 R2 Standard, Enterprise or Datacenter edition, including Core mode (x86/x64)
  - 2008 Microsoft Hyper-V R2 Release
  - 2012 Standard or Enterprise Edition
  - 2012 R2 Standard or Enterprise Edition
  - Intel Xeon 51xx processor or Intel Xeon 53xx processor, 1.86 GHz or faster

- 2 GB RAM
- 1 GB disk space recommended.

A single Kaspersky Anti-Virus for Windows Servers Enterprise Edition scan engine can support multiple EVS clients. For sites with larger scan volumes, multiple scan engines can be used to support one or more EVS clients.

After installing Kaspersky Anti-Virus for Windows Servers Enterprise Edition configure the antivirus server and EVS clients using the following procedures.
Configure Real-time Protection of ICAP Storage Systems

Before registering Kaspersky Anti-Virus for Windows Servers Enterprise Edition with an EVS, configure the properties for the real-time protection of ICAP storage systems. Do this by setting the protection setting for ICAP storage.

To configure real-time protection of ICAP storage systems, do the following.

1. Open Real-time protection of ICAP storage systems.
   (1) From the Kaspersky Anti-Virus console, select and expand Protection of network-attached storages.
   (2) Click Real-time protection of ICAP storage systems.
   (3) Figure 14 shows Real-time protection of ICAP storage systems on Kaspersky Anti-Virus.

2. Under Properties, click the Properties link.
   Figure 15 shows the Properties area on Real-time protection of ICAP storage systems.
3. Under the **General** tab, click **Protection settings**.

   Figure 16 shows the **General** tab with the **Protection settings** button.

![Figure 16](image)

4. On the **General** tab, under **Compound objects protection**, select all the check boxes.

   Figure 17 on page 20 shows all compound objects marked for protection.
5. On the **Actions** tab, do the following:

   - Select the **Block access and disinfect** check box.
   - Select the **Block access and quarantine** check box.

6. On the **Protection settings for ICAP storage** dialog box, click **OK** to save the settings.

7. On the **Real-time protection of iCAP storage system** dialog box, click **OK** to save the properties.

8. To start **Real-time protection of iCAP storage systems**, click the **Start** link under **Management**.

   Figure 18 shows **Real-time protection of iCAP storage systems** running.

---

**Figure 17**

**Figure 18**
Hitachi NAS Platform Setup Procedure for Kaspersky Anti-Virus for Windows Servers Enterprise Edition for ICAP

To setup Hitachi NAS Platform for use with Kaspersky Anti-Virus Anti-Virus for Windows Servers Enterprise Edition, do the following.

1. From the Hitachi NAS Platform home page, click Data Protection and then click Virus Scanning.

2. On the Virus Scanning page, select the EVS on which to enable virus scanning.

3. If Mode is set to RPC, click the Switch to ICAP Mode link to change to ICAP mode.

   Figure 19 shows the Switch to ICAP mode link.

4. Enable virus scanning from the CIFS Share Detail page.

   (1) From Home on Hitachi NAS Platform, click File Services.

   (2) Click CIFS Shares.

   (3) Click CIFS Share Details.

   (4) Select the Enable Virus Scanning text box.

This enables virus scanning services on Hitachi NAS Platform for each selected share on an EVS. Virus scanning can be stopped on an individual share by unchecking (clearing) the Enable Virus Scanning check box for that share.

   Figure 20 shows all the check boxes available on CIFS Share Details.

Figure 21 shows registration of new Kaspersky Anti-Virus server using ICAP


The virus scan engine now actively scans the EVS shares on Hitachi NAS Platform.

Administrative Options and Considerations

These are options and considerations you should take into account when using Kaspersky Anti-Virus for Windows Servers Enterprise Edition in Hitachi NAS Platform.

Availability

When virus scanning is enabled, Hitachi NAS Platform must receive notification from a virus scan engine that a file is clean before allowing access to a file. As a result, if virus scanning is enabled and there are no virus scan engines available to service the virus scan requests, CIFS clients might experience a temporary loss of data access.

To ensure maximum accessibility of data, configure multiple virus scan engines to service each EVS on which virus scanning has been enabled. This allows for a higher level of availability.

For example, two Kaspersky Anti-Virus for Windows Servers Enterprise Edition servers could be used to service five EVS servers to provide redundancy. When no Anti-Virus for Windows Servers Enterprise Edition servers are available, the storage simply fails all access to protected files with an “access denied” error.
If access is denied, the administrator can choose to do one of two following actions.

- **Disable virus scanning.**
  
  This stops all virus scanning until resolving the problem with the Anti-Virus for Windows Servers Enterprise Edition server or servers.
  
  The status of the file is tracked, even with virus scanning disabled. When virus scanning is re-enabled, the storage forces a scan on all protected files that were modified or created while scanning was disabled.

- **Enable best effort scanning.**
  
  During periods of heavy use, Hitachi NAS Platform could possibly overload Anti-Virus for Windows Servers Enterprise Edition with scan requests. When this happens Anti-Virus for Windows Servers Enterprise Edition may stop responding for a period, which may deny users access to files.
  
  When best effort scanning is enabled, if a scan engine is not available to service the scan requests, Hitachi NAS Platform allows the file to be opened but still tracks the file as being un-scanned.
  
  This can lead to possible infections of CIFS clients or user workstations. This is why the recommendation is for CIFS clients and user workstations have antivirus protection installed on them as well.
  
  Enable or disable best effort scanning at the Hitachi NAS Platform command line with the `virusscan` command.

To ensure an even greater level of availability, use VMware vSphere High Availability in conjunction with Kaspersky Anti-Virus for Windows Servers Enterprise Edition and Hitachi NAS Platform. When multiple instances of Anti-Virus for Windows Servers Enterprise Edition are installed on virtual machines within a vSphere High Availability cluster, this reduces the risk of scan engine downtime due to hardware failure. Coupled with the ability of Hitachi NAS Platform to load balance across scan engines, you can guarantee a higher level of antivirus protection.

**Network Considerations**

Network connectivity requirements between Hitachi NAS Platform and the antivirus scan engine will vary depending on which Hitachi NAS Platform model is used.

- Hitachi NAS Platform 3080, 3090 and 4040 models support both 1 gigabit Ethernet and 10 gigabit Ethernet connectivity.

- Hitachi NAS Platform 4060, 4080 and 4100 models only support 10 gigabit Ethernet connectivity.

Because of this, it is important to understand the rate of data being stored and changed on the Hitachi NAS Platform.
While data rates remain low, it may be perfectly fine for the antivirus scan engine to reside on a 1 gigabit network while the EVS is on a 10 gigabit network. However there is always the risk that data access spikes could overwhelm the antivirus scan engine. Because of this, it is recommended that the antivirus scan engine have the same connection speeds as the Hitachi NAS Platform.

If the antivirus scan servers are on a 1 gigabit network and Hitachi NAS Platform is on a 10 gigabit port, then verify the enabling of flow control on the clients as well as the NAS Platform switch links.

**Deregistration**

When adding the IP address of Hitachi NAS Platform to a virus scan engine's list of RPC clients, the virus scan engine automatically registers itself with the Hitachi NAS Platform system.

Virus scan engines also automatically deregister themselves when their local virus scanning service is restarted, stopped, or when removing the IP address of the EVS on Hitachi NAS Platform from the IP address list of the virus scan engine.

---

**Note** — When using ICAP, there is no registration or deregistration process. When a starting or stopping a virus scan server, Hitachi NAS Platform reports the virus scan server is unavailable in the NAS Platform event log and moves to an available virus scan engine.

---

**Updates and Full Rescans**

With the appearance of a new virus and release of antivirus software updates, it is important to rescan all files, including those that have not changed since the last time they were scanned.

To rescan files, do the following.

1. From the Hitachi NAS Platform system management unit (SMU) home page, click **Data Protection**, and then click **Virus Scanning**.

2. Click **Request Full Scan**.

   This flags all the file types in the inclusion list to be rescanned the next time a user attempts to access them.

To avoid having to manually request a full virus scan every time the antivirus server updates its virus definitions, you can create a cron job on Hitachi NAS Platform to run virusscan from the command line interface to issue a full rescan.
Figure 22 shows the creation of a crontab entry runs the first of every month at 4:42 am.

Figure 22

It is suggested that you update the inclusion list, as required, for each update.

Inclusion List
The default file extension inclusion list is as follows:

- ACE
- ACM
- ACV
- ACX
- ADT
- APP
- ASD
- ASP
- ASX
- AVB
- AX
- BAT
- BO
- BIN
- BTM
- CDR
- CFM
- CHM
- CLA
- ACE
- CLASS
- EML
- LGP
- ACM
- CMD
- EXE
- LNK
- ACV
- CNV
- FON
- MB
- ACX
- COM
- GMS
- MDB
- ADT
- CPL
- GVB
- MHT
- APP
- CPT
- HLP
- MHTM
- ASD
- CPY
- HTA
- MHTML
- ASP
- CSC
- HTM
- MOD
- ASX
- CSH
- HTML
- MPD
- AVB
- CSS
- HTT
- MPP
- AX
- DAT
- HTW
- MPT
- BAT
- DEV
- HTX
- MRC
- BO
- DL
- IM
- MS
- BIN
- DLL
- INF
- MSG
- BTM
- DOC
- INI
- MSO
- CDR
- DOT
- JS
- MP
- CFM
- DVB
- JSE
- NWS
- CHM
- DRV
- JTD
- OBD
- CLA
- DWG
- LIB
- OBT
You can add or remove file extensions from the list to customize it.

### Load Balancing and Performance

If multiple antivirus scan engines are registered, Hitachi NAS Platform issues a new request for each file scan to a different Kaspersky Anti-Virus for Windows Servers Enterprise Edition server. This spreads scan requests and load balancing across the multiple virus scan engines.

Currently, no performance characterization data exists for this system. The use of professional services is suggested to help characterize your workload. Then, use this information to determine the number of scan engines and configuration optimization for individual your deployments at this time.
Large Files

Large files could be temporarily inaccessible to a client or user. While being scanned, access to the large file could be temporarily denied. After the storage scans the large file, it provides access to it, assuming it returns clean after scanning.

By default Kaspersky Anti-Virus for Windows Servers Enterprise Edition sets the protection scope performance settings to stop scanning a file if either of the following is true:

- It takes longer than 60 seconds to scan.
- The object is larger than 8 MB.

If a large file is scanned, Hitachi NAS Platform reports it as a scan error. If you want large file scanning, then do the following under **Advanced settings** (Figure 22):

- Uncheck (clear) the **Stop scanning if it takes longer than (sec)** check box.
- Uncheck (clear) the **Do not scan compound objects larger than (MB)** check box.

![Figure 23](image-url)
Statistics
Hitachi NAS Platform provides virus scan statistics. These include the number of the following:

- Virus scans
- Clean scans
- Scans with errors
- Files infected
- Files repaired
- Files deleted
- Files quarantined

On-Demand and Proactive Virus Scanning
When there is a client read request for a file, typically one of the two things will happen:

- The file is scanned on-demand and marked safe, granting the client access.
- The file is scanned on-demand and marked unsafe, denying the client access.

However, because the storage system can make requests for files to be scanned based on write operations, this allows proactive scanning to occur well before the next read request for it. Proactive scanning, called background scanning, can significantly improve performance of the overall system.

Virus scanning solutions that only scan files when they are opened can allow an infected file to reside on a storage system for a long time without being detected. Although a user would not be able to access the file because of the scan when it was opened, this is suboptimal behavior. The Hitachi NAS Platform system avoids this suboptimal behavior by allowing scan on writes.

Snapshots
Virus scanning rules are different for snapshots. Files that are part of a snapshot cannot be modified. As a result, files containing a virus in a snapshot become inaccessible after scanning.

Command Line Interface
To configuring antivirus scanning on Hitachi NAS Platform, there is an alternative to the web-based graphical user interface. The alternative is the command line interface. It is from the command line interface where you can enable or disable additional options, such as best effort scanning.

Refer to the Hitachi NAS Platform and command line interface guide for a list of commands.
File Accessibility
Currently, a file is scanned when it is opened (read) or closed (write) only when it is opened or closed over CIFS. This is how most viruses are spread.

After the scan, checks are carried out in the following order:
1. If virus scanning is disabled, then grant access to the file.
2. If the file has already been virus scanned, then grant access.
3. If the client is a virus scan server, then grant access.
4. If the file is currently being scanned, then wait for the result of that scan instead of sending a new one.
5. If the file is not in the list of file types to scan, then grant access.
6. If there are not any scan servers available to scan the file, then deny access.
7. Send a request to a scan server to scan the file.
8. If the file is clean, then grant access.
9. If the file is infected, then deny access.

Additional Information
See the Hitachi NAS Platform Antivirus Administration Guide for more information.

Per-Share Virus Scanning: Set Up at the User Interface
Use the CIFS Share configuration page to enable virus scanning on each share to be scanned for malicious code.

To enable virus scanning, do the following.
1. To view the CIFS Share Details window, from Home, click File Services, click CIFS Shares, and then click Details.
2. To enable or disable virus scanning, select or uncheck (clear) the Enable Virus Scanning check box (Figure 23).

Figure 24
Conclusion

You can implement the protection of data against malicious code with hardware and software from Hitachi Data Systems, Kaspersky, and VMware.

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

VMware vSphere High Availability can provide an additional level of availability for antivirus scan engines.

Hitachi NAS Platform, with its integrated antivirus functionality and ability to load balance across virus scan servers, provides an even greater level of protection for your data.
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.