HITACHI
Inspire the Next

Data Protection on Hitachi Virtual Storage Platform Gx00 Models with Kaspersky Security 10 for Windows Server

TECHNICAL PAPER

Best Practice Guide

By Diana Milan

August 2016

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.

Contents

Data Protection on Hitachi Virtual Storage Platform Gx00 Models with Kaspersky Security 10 for Windows Server

Best Practice Guide

This technical paper describes best practices for Hitachi Virtual Storage Platform Gx00 models with NAS Module when using Kaspersky Security 10 for Windows Server. Included is information for setup and using this solution to protect data on network-attached storage.

Hitachi Virtual Storage Platform Gx00 models with NAS Module provides integrated antivirus functionality. This allows administrators to manage antivirus behavior from the Hitachi 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

Storage System

Hitachi Virtual Storage Platform Gx00 Models

Hitachi Virtual Storage Platform Gx00 models are based on industry-leading enterprise storage technology. With flash-optimized performance, these systems provide advanced capabilities previously available only in high-end storage arrays. With the Virtual Storage Platform Gx00 models, you can build a high performance, software-defined infrastructure to transform data into valuable information.

Hitachi Storage Virtualization Operating System provides storage virtualization, high availability, superior performance, and advanced data protection for all Virtual Storage Platform Gx00 models. This proven, mature software provides common features to consolidate assets, reclaim space, extend life, and reduce migration effort. New management software improves ease of use to save time and reduce complexity. The infrastructure of Storage Virtualization Operating System creates a management framework for improved IT response to business demands.

The NAS Module 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.

Servers

Hitachi Compute Rack 210H

Hitachi Compute Rack 210H is a midrange rack mountable server platform, providing advanced systems management and redundancy options. It is data center friendly, with a 1U footprint, while delivering the performance that is required to meet enterprise-level challenges.

The benefits of Hitachi Compute Rack 210H are the following:

- Web-based management interface
- RAID level configuration, with up to six 2.5 inch internal drives
- Sustainable power-saving capabilities
- Configuration flexibility to meet business needs
- Dense 1U rack mountable design

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 Security 10 for Windows Server, this Hitachi Virtual Storage Platform Gx00 with NAS Module antivirus solution uses one of the following:

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

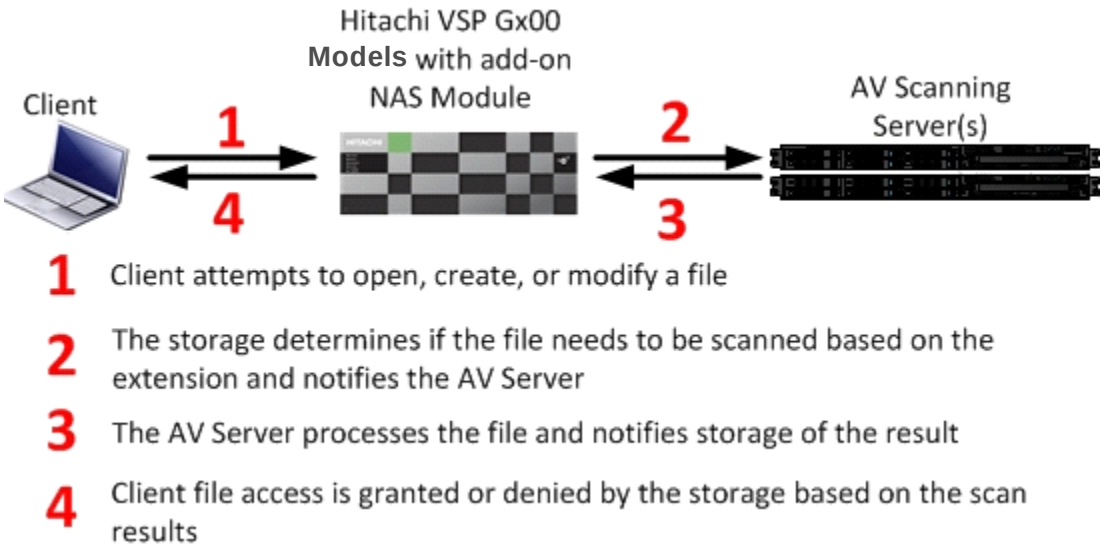

Figure 1

Software Components

Kaspersky Security 10 for Windows Server

Kaspersky Security 10 for Windows Server (the earlier version was known as Kaspersky Anti-Virus Windows Servers Enterprise Edition) is a solution for corporate server security and network attached storage protection.

Hitachi NAS Protection

- Integration with Kaspersky Security Network.
- The application increases server and NAS protection tasks efficacy by the means of Kaspersky Security Network (KSN) cloud services, and the conclusions regarding potential security dangers are based on Kaspersky Lab up-to-date data. KSN Usage task does not imply any personal information transfer, except for the scanned files checksums.
- You can control KSN usage by accepting or denying the KSN Statement conditions.
- Application launch control functionality.
- Windows Server Protection
- The application allows or denies the executable files launch, scripts launch, MSI packages launch, driver loading, and DLL modules loading via defined application launch control rules.
- Blocking untrusted hosts access to shared network file resources on a protected server.
- The application allows you to block access to the network file resources in case any malicious activity from an untrusted host has been detected when running Real-Time File Protection or Anti-Cryptor tasks.
- You can manage the list of untrusted hosts and configure the hosts blocking term.
- Anti-malware cryptors protection functionality.
- The application traces the malicious encrypting attempts targeted on data that are stored in the shared network folders, and lists hosts as untrusted, if they were detected as a source of malicious activity.

Best Practices

To detect and stop viruses before they spread, Hitachi Virtual Storage Platform Gx00 models with NAS Module integrates antivirus functionality into the NAS module system software. NAS module integrated antivirus software communicates with Kaspersky Security 10 for Windows Server 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 module marks the file as infected. It then deletes or denies access to the file.

NAS module 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 scan
- Information about the virus scan servers
- The list of file types to be scanned

Virus scanning on a NAS module 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 module proactively submits files for scanning to Kaspersky Security 10 for Windows Server 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 Security 10 for Windows Server registers with Hitachi Virtual Storage Platform Gx00 models with NAS Module using one of the following:

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

You can register multiple instances of Kaspersky Security 10 for Windows Server to register with the same NAS module instance to provide for redundancy and performance.

When deploying multiple instances of Kaspersky Security 10 for Windows Server, NAS module 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 Security 10 for Windows Server scan engines using a VMware vSphere High Availability cluster when installing Kaspersky Security 10 for Windows Server on a virtual machine within the cluster. Additionally, NAS module actively monitors connections to registered scan engines. If a scan engine fails or goes down, NAS module automatically distributes that server's pending scans between the remaining scan servers. Using vSphere High Availability and NAS module provides a higher level of antivirus redundancy and availability.

Kaspersky Security 10 for Windows Server Setup Procedure for RPC

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

1. Shared Local User Group Configuration
2. Kaspersky Security 10 for Windows Servers Setup Procedure for Hitachi Virtual Storage Platform Gx00 Models with NAS Module for RPC
3. Hitachi Virtual Storage Platform Gx00 Models with NAS Module Setup Procedure for Kaspersky Security 10 for Windows Server for RPC

Shared Local User Group Configuration

For Kaspersky Security 10 for Windows Server to work with Hitachi Virtual Storage Platform Gx00 models with NAS Module, 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 Virtual Storage Platform Gx00 models with NAS Module
- The protection of network-attached storage in Anti-Virus for Windows Servers

On Hitachi Virtual Storage Platform Gx00 models with NAS Module, 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: `Domain\username`

   In the figures below, user ISVLAB\avuser is the virus scan user. This user is also a member of the Backup Operators group within the domain.
6. Click **Add**.
7. Click **OK**.

Figure 2 shows the **Local Groups** page on Hitachi NAS module.

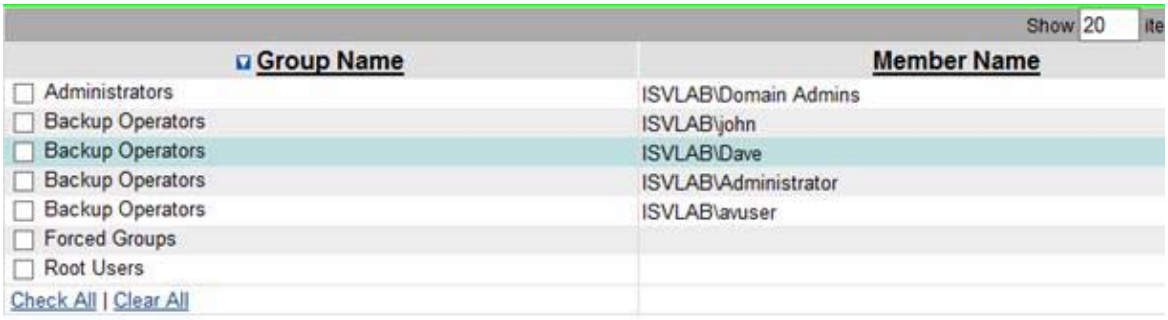

Figure 2

1. Figure 3 shows the **Add Local Group** page on Hitachi NAS module.

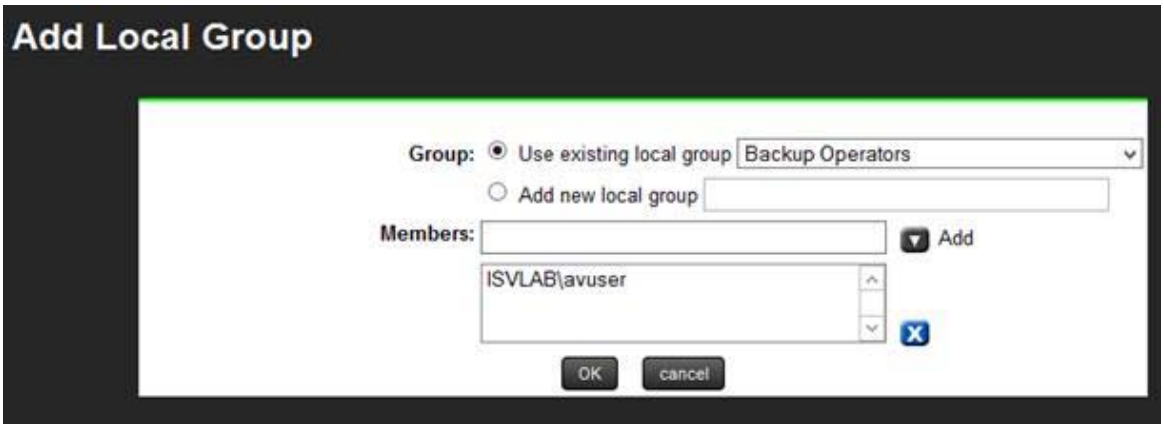

Figure 3

Kaspersky Security 10 for Windows Servers Setup Procedure for Hitachi Virtual Storage Platform Gx00 Models with NAS Module for RPC

Remote procedure call (RPC) is one of the protocols used for communication between Hitachi Virtual Storage Platform Gx00 models with NAS Module and Kaspersky Security 10 for Windows Server for file scanning requests. 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 scan operations.

NAS module does not support scanning files on NFS shares. If sharing a NAS module 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 Security 10 for Windows Server as follows:

- Install only on a Microsoft Windows Server
- It must be located in the same domain as the Hitachi Virtual Storage Platform Gx00 models with NAS Module.

Kaspersky Security 10 for Windows Server requirements include the following:

- One of the following versions of Microsoft Windows Server
  - 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
- 4 GB disk space recommended.
- A single Kaspersky Security 10 for Windows Server 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 Security 10 for Windows Server, configure the antivirus server and EVS clients using the following procedures.

Configure RPC-Network Storage Protection

Before adding an EVS to Kaspersky Security 10 for Windows Server, configure the Network Attached Storage Protection properties. Do this by adding the domain user that was added in the Shared Local Group configuration on NAS module.

The user name entered is the same user name in Shared Local User Group Configuration, <domain>\<user name>.

To add the domain user, do the following.

1. Open **Kaspersky Security Console**.

   (1) From the console, select and expand **Network Attached Storage Protection**.

   (2) Click **RPC-Network Storage Protection**.

   Figure 4 shows **RPC-Network Storage Protection** on Kaspersky Security Console.

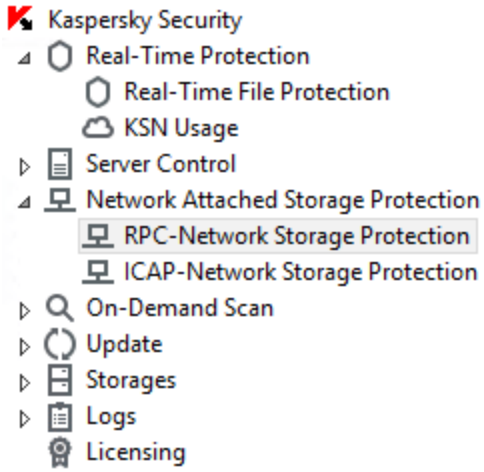

Figure 4

2. On the right hand side under **RPC-Network Protection**, click the **Configure Protection Scope** link.

   Figure 5 shows the **Protection scope** list on **RPC-Network Storage Protection**.

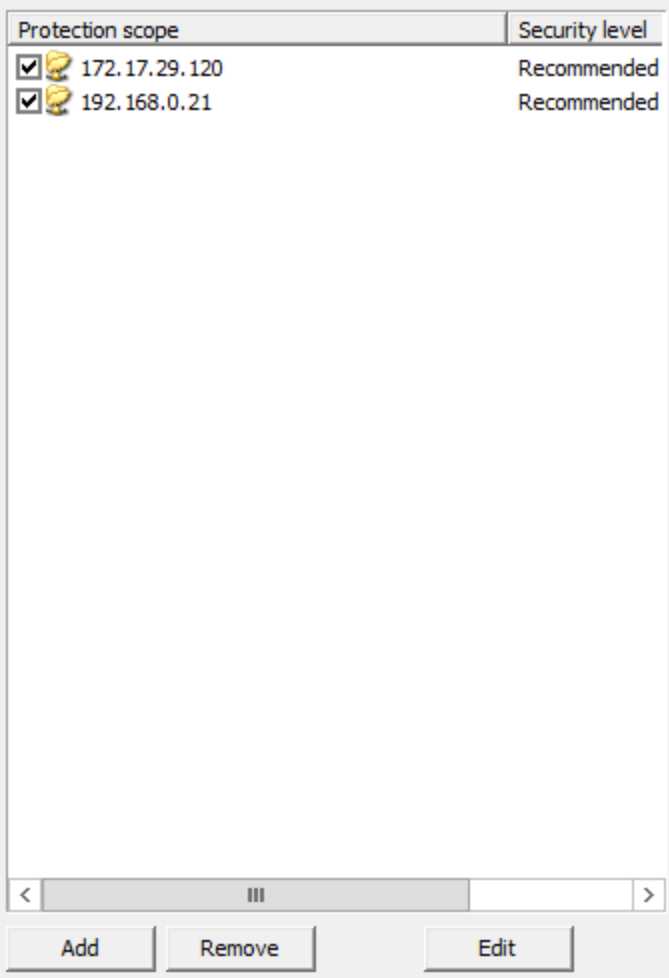

Figure 5

3. Return to **RPC-Network Storage Protection,** click the **Property**, type the user name in Shared Local User Group Configuration, then click **Apply** and **OK**.

   - Use this format when typing the user name:

     `<domain>\<user name>`

Figure 6 shows the **RPC-Network Storage Protection properties configuration** dialog box.

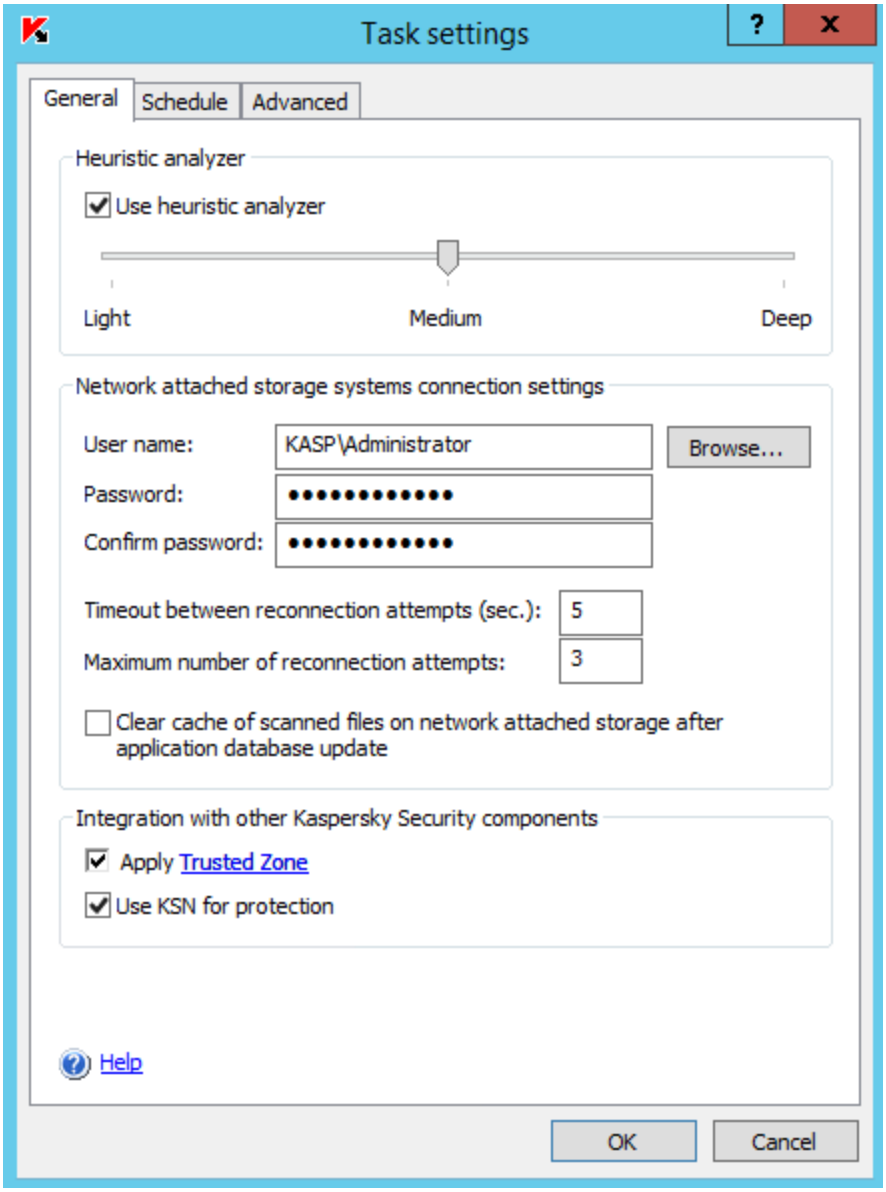

Figure 6

Add an EVS to Kaspersky Security 10 for Windows Servers
To add an EVS to Kaspersky Security 10 for Windows Servers, do the following.

1. Open **Kaspersky Security Console**.

   (1) From the Console, select and expand **Network Attached Storage Protection.**

   (2) To view the properties, click **RPC-Network Storage Protection**.

   Figure 7shows the location of **RPC-Network Storage Protection**.

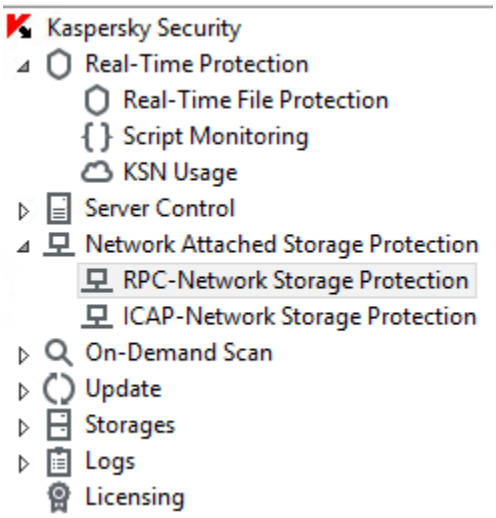

Figure 7

2. Add the EVS on NAS module.

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

Figure 8 shows the **Properties** area on the **RPC-Network Storage Protection** page.

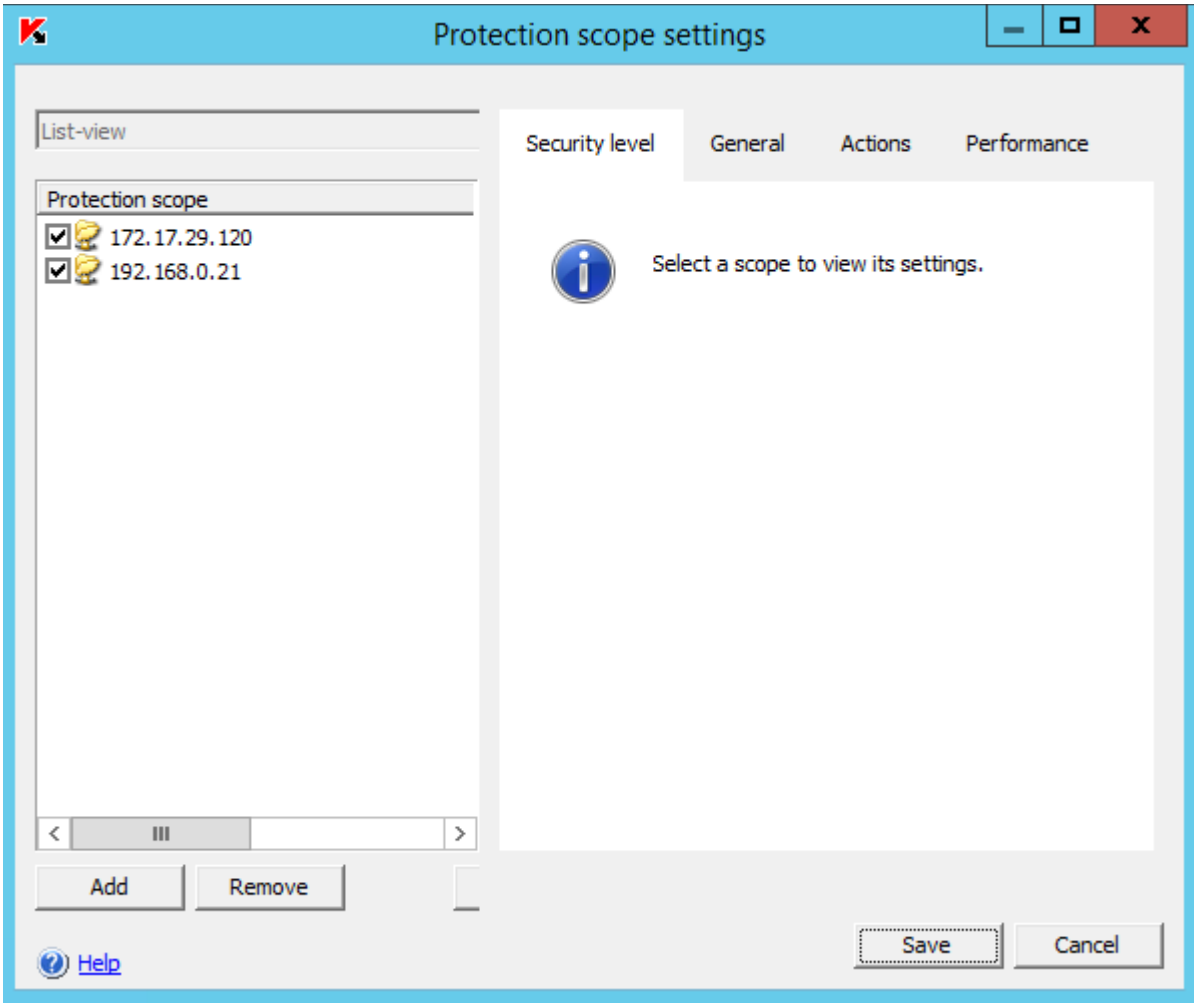

Figure 8

(2) On the **Protection scope settings** tab, do the following:

i. Click the **Add** button on the bottom left hand corner or right-click in the blank area of the **Protection scope pane** (Figure 9).

ii. Click **Add protection scope.**

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

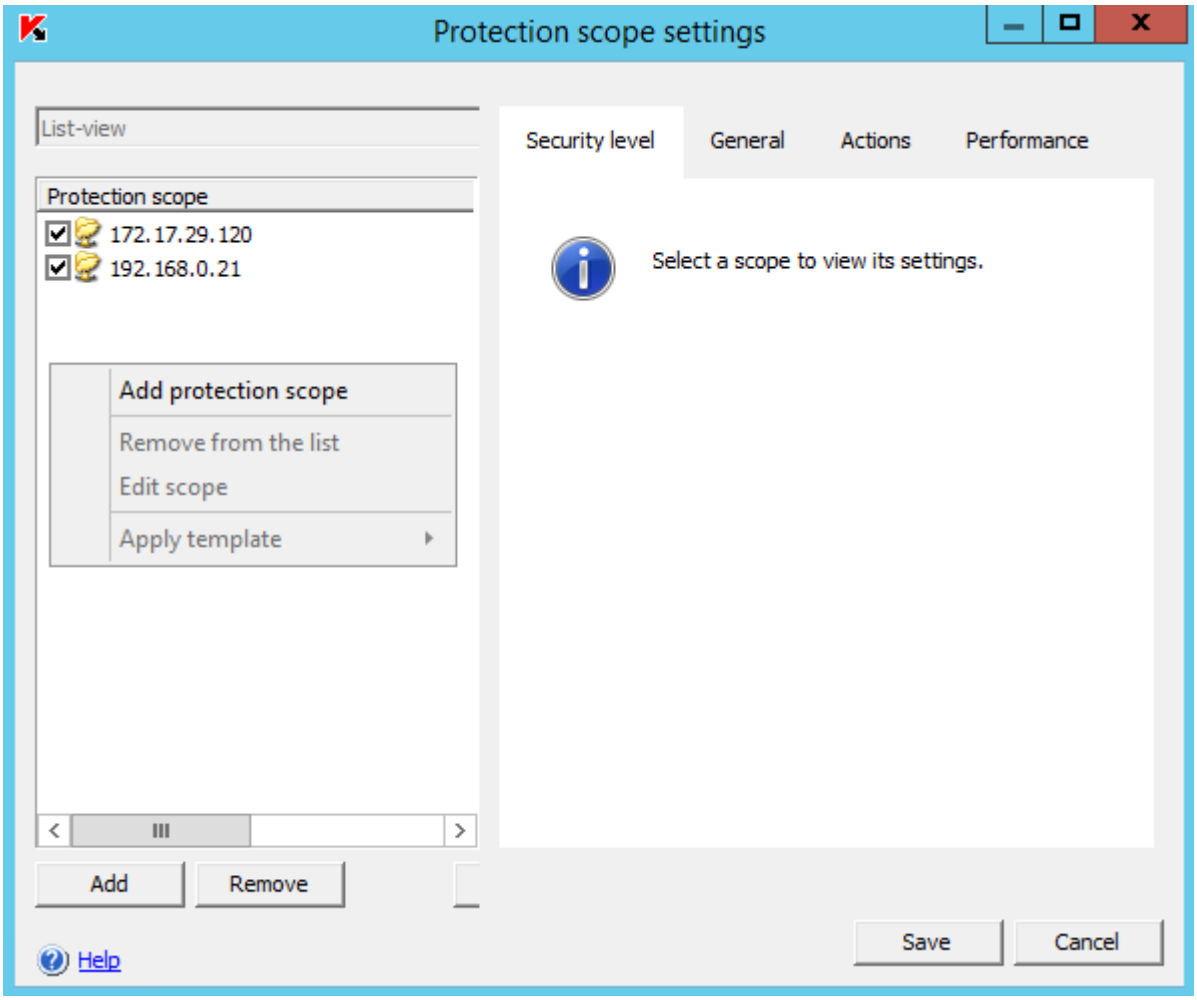
Protection scope settings
List-view
Protection scope
172.17.29.120
192.168.0.21
Add protection scope
Remove from the list
Edit scope
Apply template
Add
Remove
Help
Security level
General
Actions
Performance
Select a scope to view its settings.
Save
Cancel

Figure 9

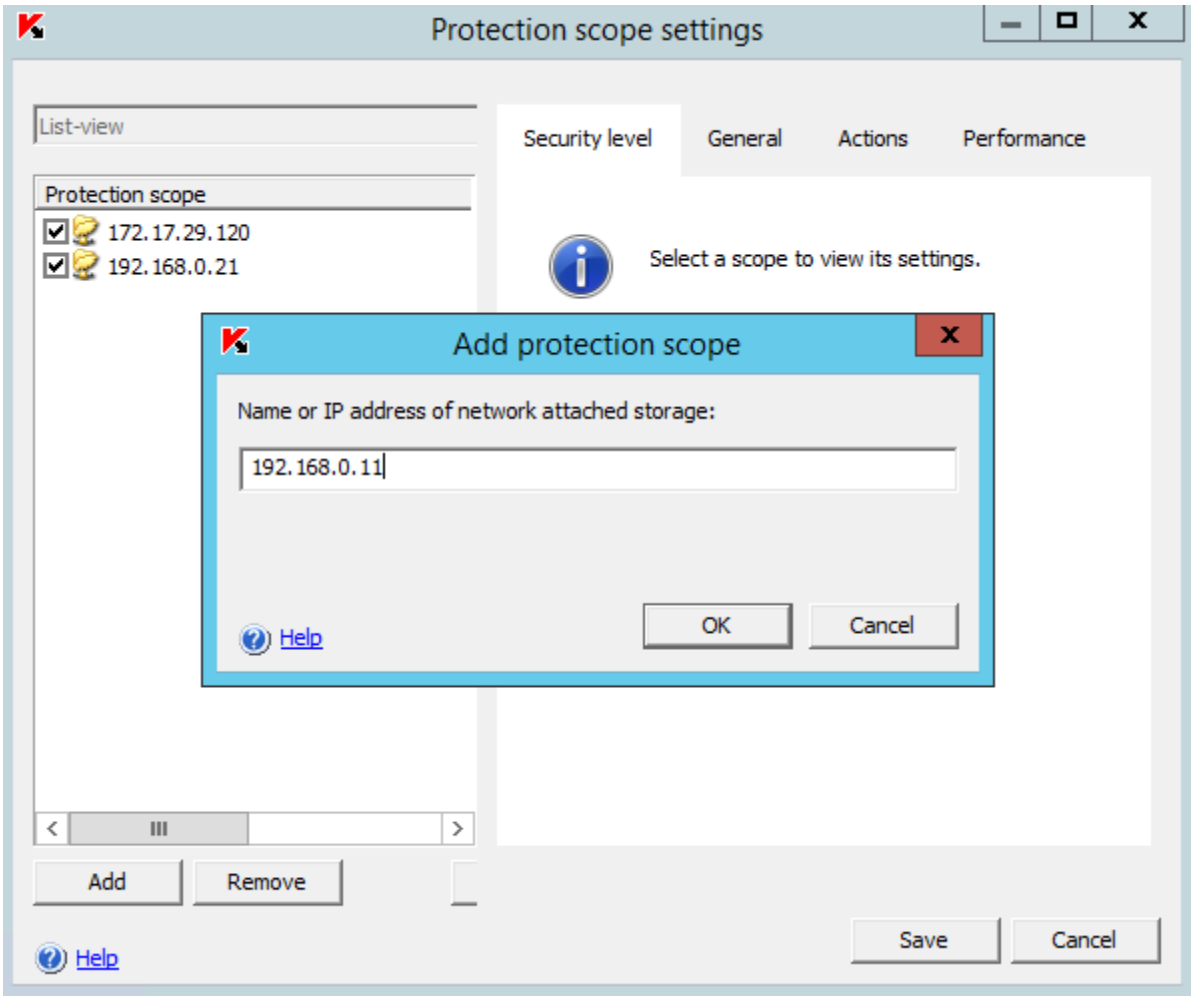
Protection scope settings
List-view
Protection scope
172.17.29.120
192.168.0.21
Security level
General
Actions
Performance
Select a scope to view its settings.
Add protection scope
Name or IP address of network attached storage:
192.168.0.11
Help
OK
Cancel
Add
Remove
Help
Save
Cancel

Figure 10

Figure 11 shows the newly added EVS added to the **Protection scope settings** tab.

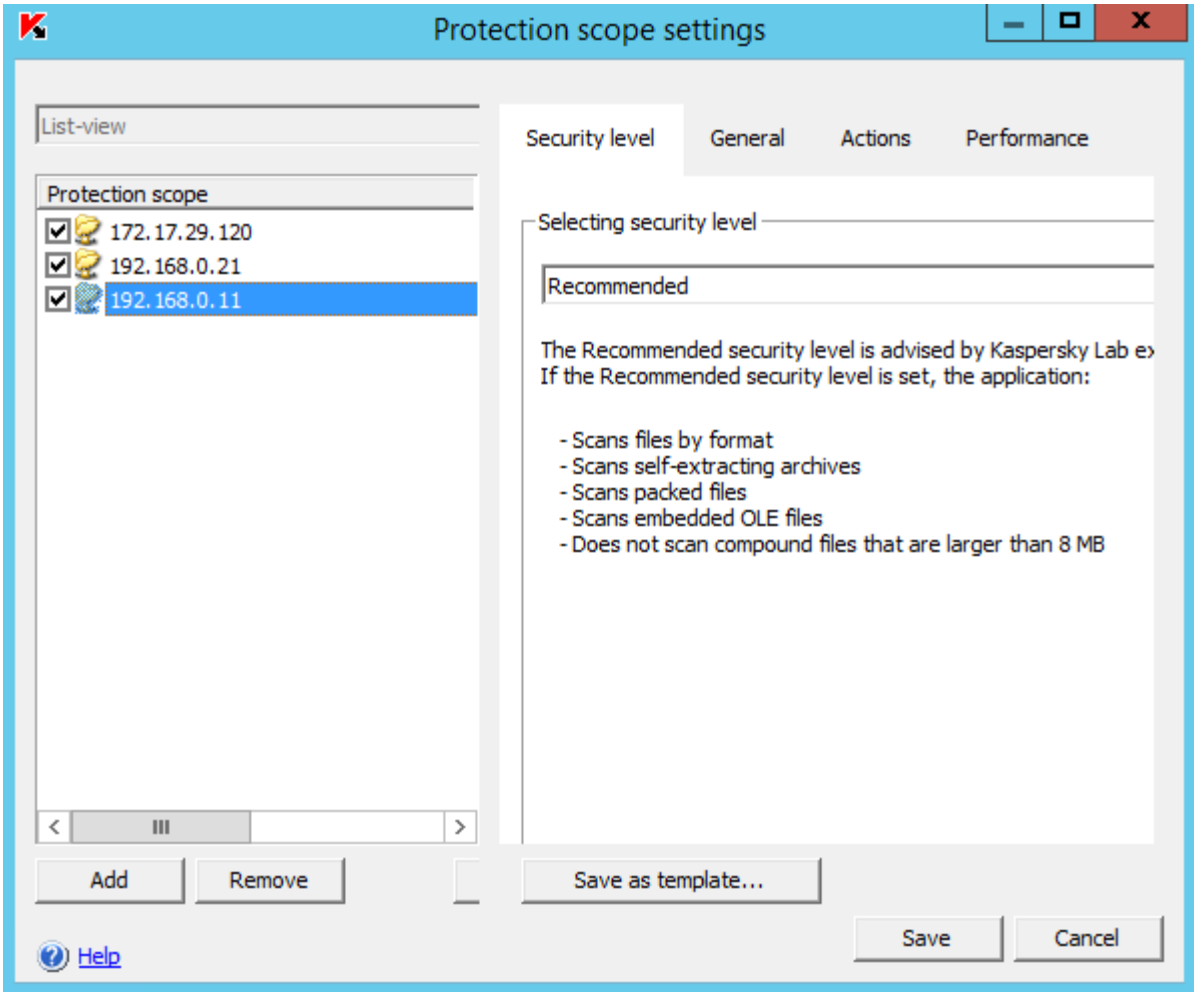

Figure 11

Hitachi Virtual Storage Platform Gx00 Models with NAS Module Setup Procedure for Kaspersky Security 10 for Windows Server for RPC

To setup Hitachi Virtual Storage Platform Gx00 models with NAS Module for use with Kaspersky Security 10 for Windows Server, do the following.

1. From the NAS module 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.**

Figure 12

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 module, click **File Services**.

   (2) Click **CIFS Shares.**

   (3) Select the EVS on which to enable virus scanning.

   (4) Select the **CIFS Share** and click **details.**

   (5) 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.

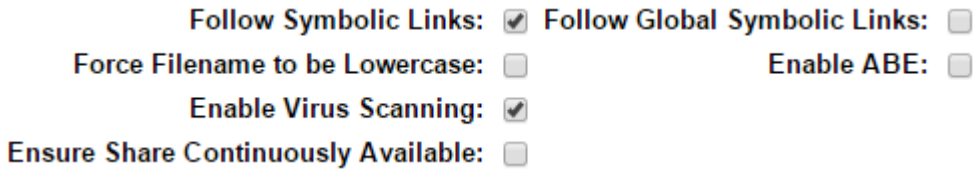

Figure 13

5. Kaspersky Security 10 for Windows Server automatically registers with Hitachi NAS Platform. Once registered, the scan engine is displayed in the **Registered Virus Scan Engines** list.

6. To enable virus scanning for the selected EVS after Kaspersky Security 10 for Windows Server is registered, click **Enable** on the Virus Scanning page.

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

Kaspersky Security 10 for Windows Server Setup Procedure for ICAP

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

1. Kaspersky Security 10 for Windows Server Setup Procedure for Hitachi Virtual Storage Platform Gx00 Models with NAS Module using ICAP

2. Hitachi Virtual Storage Platform Gx00 Models with NAS Module Setup Procedure for Kaspersky Security 10 for Windows Server for ICAP

Kaspersky Security 10 for Windows Server Setup Procedure for Hitachi Virtual Storage Platform Gx00 Models with NAS Module using ICAP

In addition to RPC, Hitachi Virtual Storage Platform Gx00 models with NAS Module can send scan requests using Internet content adaptation protocol (ICAP) to Kaspersky Security 10 for Windows Server. 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 scan operations. If the file is infected, Kaspersky Security 10 for Windows Server sends a response to NAS module of infection, and the NAS module processes the file.

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

Kaspersky Security 10 for Windows Server system requirements include the following:

- One of the following versions of Microsoft Windows Server
  - 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 Security 10 for Windows Server 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 Security 10 for Windows Server configure the antivirus server and EVS clients using the following procedures.

Configure ICAP-Network Storage Protection

Before registering Kaspersky Security 10 for Windows Server with an EVS, configure the properties for ICAP-Network Storage Protection. Do this by setting the protection setting for ICAP-Network storage.

To configure ICAP-Network Storage Protection, do the following.

1. Open **Kaspersky Security Console**.

   (1) From the console, select and expand **Network Attached Storage Protection**.

   (2) Click **ICAP-Network Storage Protection**.

   (3) Figure 14 shows I**CAP-Network Storage Protection**.

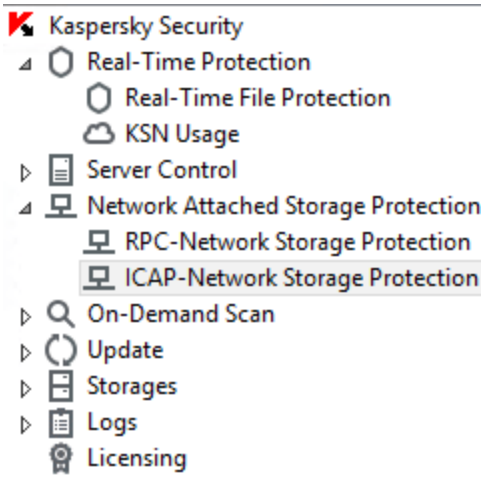

Figure 14

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

   Figure 15 shows the **Properties** area on **ICAP-Network Storage Protection**.

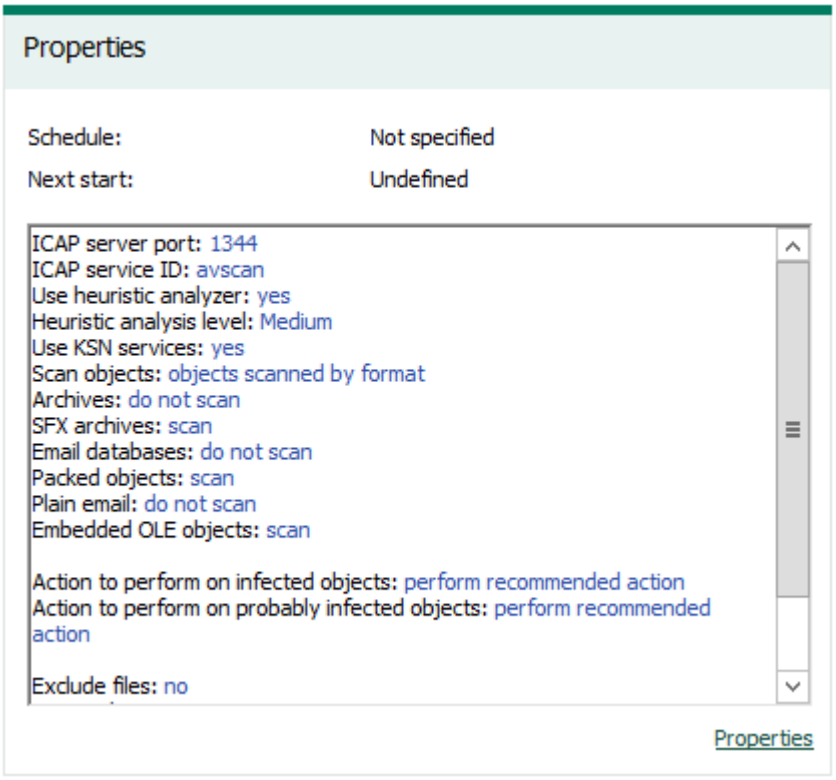

Figure 15

3. The **General** tab shows the current Security level.

   Figure 16 shows the **General** tab with the **Security level** and **Settings** button.

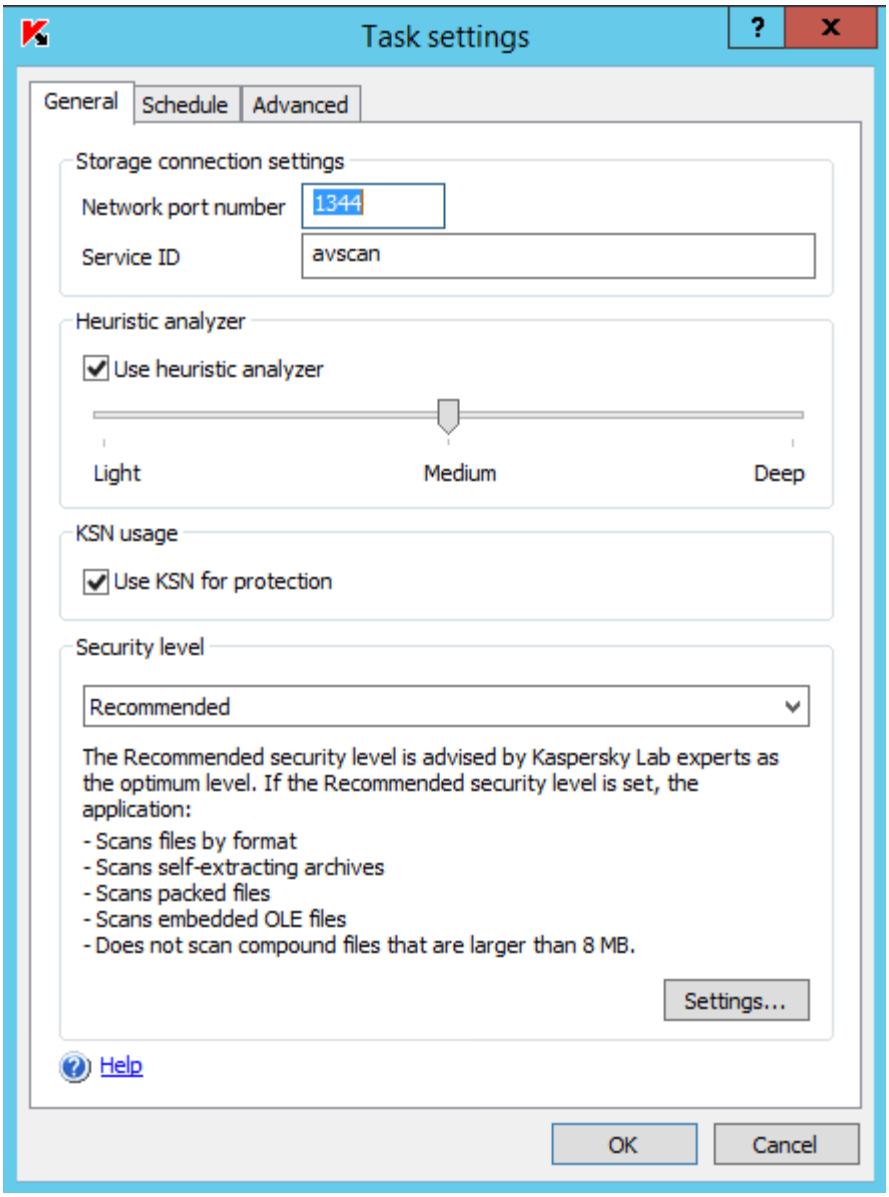

Figure 16

4. On the **General** tab, click on **Settings** under **Security level**, select all of the check boxes.

Note - Selecting **Archives** will impact performance.

Figure 17 shows all compound objects that are marked for protection.

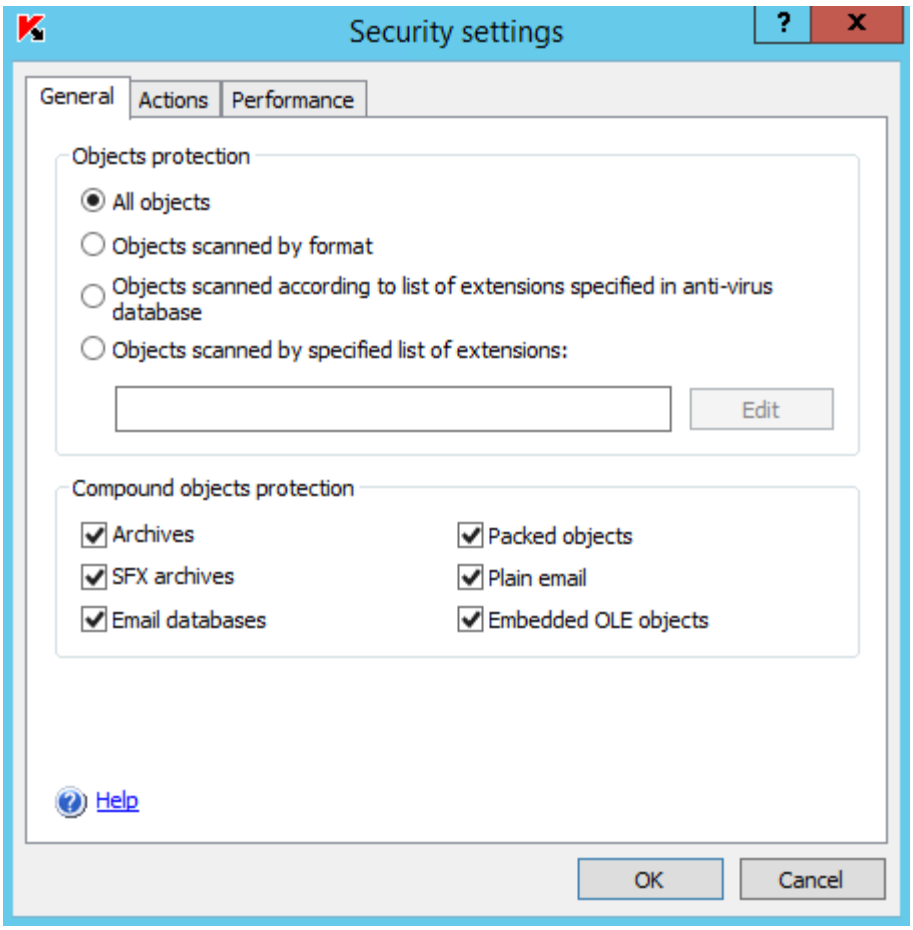

Figure 17

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. Click **OK** to save the settings.
7. To start **ICAP-Network StorageProtection**, click the **Start** link under **Management**.

   Figure 18 shows **ICAP-Network Storage Protect** running.

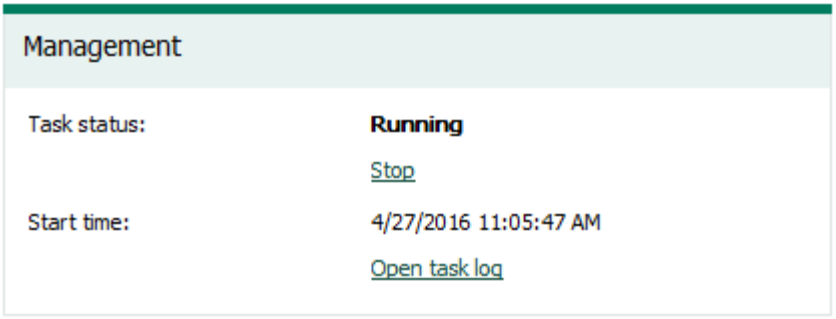
Management
Task status:
Running
Stop
Start time:
4/27/2016 11:05:47 AM
Open task log

Figure 18

Hitachi Virtual Storage Platform Gx00 Models with NAS Module Setup Procedure for Kaspersky Security 10 for Windows Server for ICAP

To setup Hitachi NAS Platform for use with Kaspersky Security 10 for Windows Server, do the following.

1. From the Hitachi Virtual Storage Platform Gx00 models with NAS Module 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.**

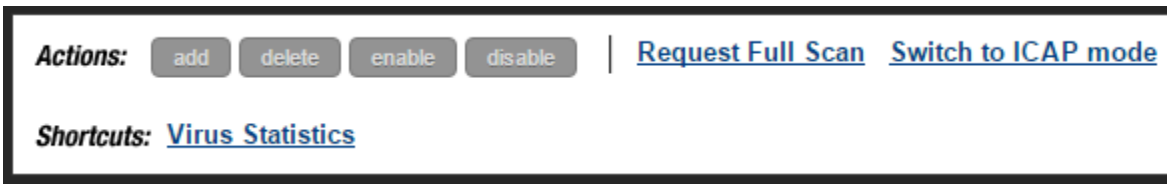

Figure 19

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.

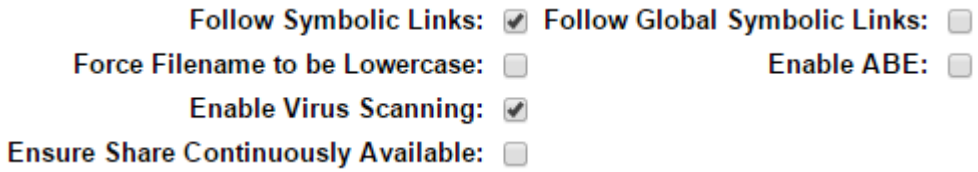

Figure 20

5. To register a new Kaspersky Security 10 for Windows Server using ICAP, click **Add** on the **Virus Scanning** dialog box.

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

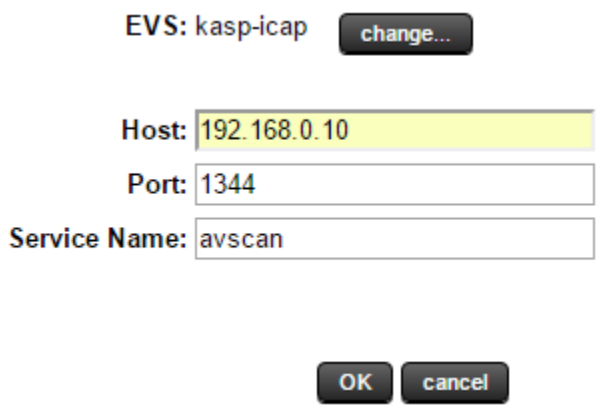

Figure 21

6. To enable virus scanning for the selected EVS after registering Kaspersky Security 10 for Windows Server, click **Enable** on the Virus Scanning page.

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

Administrative Options and Considerations

These are options and considerations that you should take into account when using Kaspersky Security 10 for Windows Server in NAS module.

Availability

When virus scanning is enabled, NAS module 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, then 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 Security 10 for Windows Server servers could be used to service five EVS servers to provide redundancy. When no Kaspersky Security 10 for Windows Server 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 the two following actions.

- **Disable virus scanning**

  This stops all virus scanning until the problem with the Kaspersky Security 10 for Windows Server server or servers is resolved.

  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, NAS module could possibly overload Kaspersky Security 10 for Windows Server with scan requests. When this happens Kaspersky Security 10 for Windows Server 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, NAS module 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 to have antivirus protection installed on them as well.

  Enable or disable best effort scanning at the NAS module command line with the virusscan command.

To ensure an even greater level of availability, use VMware vSphere High Availability in conjunction with Kaspersky Security 10 for Windows Server and Hitachi Virtual Storage Platform Gx00 models with NAS Module. When multiple instances of Kaspersky Security 10 for Windows Server 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 Virtual Storage Platform Gx00 models with NAS Module to load balance across scan engines, you can guarantee a higher level of antivirus protection.

Deregistration

When adding the IP address of Hitachi Virtual Storage Platform Gx00 models with NAS Module to a virus scan engine's list of RPC clients, the virus scan engine automatically registers itself with the Hitachi Virtual Storage Platform Gx00 models with NAS Module.

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 Virtual Storage Platform Gx00 models with NAS Module from the IP address list of the virus scan engine.

Note — When using ICAP, there is no registration or deregistration process. When starting or stopping a virus scan server, Hitachi Virtual Storage Platform Gx00 models with NAS Module reports that the virus scan server is unavailable in the NAS module 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 Virtual Storage Platform Gx00 models with NAS Module home page, click **Data Protection,** and then click **Virus Scanning**.
2. Click **Request Full Scan**.

This flags all of 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 Virtual Storage Platform Gx00 models with NAS Module to run virus scan from the command line interface to issue a full rescan.

Figure 22 shows the creation of a crontab entry that runs the first of every month at 4:42 am.

```
HNAS3090-1:$ crontab add "42 4 1 * *" "virusscan -s"

Added job 1

ID    Date Specification    Mail Recipient(s)         Level      Command(s)
--    ------------------    -----------------    ----------    ------------
 1            42 4 1 * *                         SUPERVISOR    virusscan -s

Local time is now 2014-11-21 15:43:27-08:00
```

Figure 22

You should 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
- CLASS

- CMD
- CNV
- COM
- CPL
- CPT
- CPY
- CSC
- CSH
- CSS
- DAT
- DEV
- DL
- DLL
- DOC
- DOT
- DVB
- DRV
- DWG
- EML
- EXE
- FON
- GMS
- GVB
- HLP
- HTA
- HTM
- HTML
- HTT
- HTW

- HTX
- IM
- INF
- INI
- JS
- JSE
- JTD
- LIB
- LGP
- LNK
- MB
- MDB
- MHT
- MHTM
- MHTML
- MOD
- MPD
- MPP
- MPT
- MRC
- MS
- MSG
- MSO
- MP
- NWS
- OBD
- OBT
- OBJ
- OBZ

- OCX
- OFT
- OLB
- OLE
- OTM
- OV
- PCI
- PDB
- PDF
- PDR
- PHP
- PIF
- PL
- PLG
- PM
- PNF
- PNP
- POT
- PP
- PPA
- PPS
- PPT
- PRC
- PWZ
- QLB
- QPW
- REG
- RTF
- SBF

- SCR
- SCT
- SH
- SHB
- SHS
- SHT
- SHTML
- SHW
- SIS
- SMM
- SWF
- SYS
- TD0
- TLB
- TSK
- TSP
- TT6
- VBA
- VBE
- VBS
- VBX
- VOM
- VS
- VSD
- VSS
- VST
- VWP
- VXD
- VXE

- WBT
- WBK
- WIZ
- WK
- WML
- WPC
- WPD
- WS
- WSC
- WSF
- WSH
- XL
- XML
- XTP
- 386

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 Virtual Storage Platform Gx00 models with NAS Module issues a new request for each file scan to a different Kaspersky Security 10 for Windows 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 needed for your deployments at this time.

Large Files

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

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 Virtual Storage Platform Gx00 models with NAS Module avoids this suboptimal behavior by allowing scans on writes.

Command Line Interface

To configure antivirus scanning on Hitachi Virtual Storage Platform Gx00 models with NAS Module, there is an alternative to the web-based graphical user interface. The alternative is the command line interface. From the command line interface you can enable or disable additional options, such as best effort scanning.

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.

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).

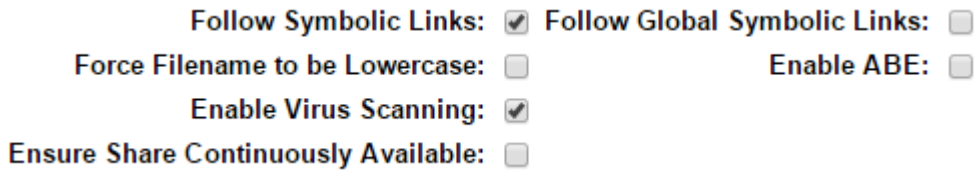

Figure 23

Conclusion

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

Kaspersky Security 10 for Windows Server 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 Virtual Storage Platform Gx00 models with NAS Module, 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.

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 96050-2639 USA
www.HDS.com community.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-526-00 August 2016.