HITACHI
Inspire the Next

Product Security Guide

Hitachi NAS Platform

MK-92HNAS099-00

November 2023

Table of Contents

Preface

About this document

This document provides information about the security related aspects of the server, its administration and, where applicable, acts as a jump off point to specific instructions and procedures in the wider documentation set.

Document conventions

This document uses the following typographic convention:

Convention	Description
Bold	• Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: **Click OK**. • Indicates emphasized words in list items.
Italic	Indicates a document title or emphasized words in text.
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`

Intended audience

This document is intended for operators and administrators of Hitachi Vantara NAS products.

Accessing product downloads

Product software, drivers, and firmware downloads are available on Hitachi Vantara Support Connect: https://support.hitachivantara.com/.

Log in and select Product Downloads to access the most current downloads, including updates that may have been made after the release of the product.

Getting Help

Hitachi Vantara Support Connect is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Chapter 1: Introduction

This guide aims to provide information on the features of Hitachi Vantara NAS systems, with associated guidance on configuration options that an administrator can use to help secure those systems. Much of the detail is common to both Gateway (HNAS 4xx0, HNAS 5x00) and Unified (VSP F/G/Nx00) systems, but where an approach differs this is highlighted in this guide.

If a security vulnerability in a Hitachi Vantara NAS system is discovered, customers are encouraged to report the vulnerability by contacting Hitachi Vantara's Global Support Center. Details of where to find the current Hitachi Vantara Vulnerability Disclosure Policy and Security Advisories, across a range of Hitachi Vantara products, are provided in Appendix A of this document.

Chapter 2: Physical Components

It is assumed and recommended that Hitachi NAS systems are installed in a secure physical environment where access to the hardware is limited to authorized personnel with the responsibility of managing the Hitachi NAS systems.

Physical ports on the Hitachi NAS systems allow for out-of-band management access that, depending on the platform, may include serial, management Ethernet or IPMI connectivity options. Location of physical ports and related configuration settings are described in the individual hardware references for each platform family, highlighted in Appendix B.

Intelligent Platform Management Interface (IPMI)

Hitachi NAS platform Gateway models (HNAS 4xx0, HNAS 5x00) include an Intelligent Platform Management Interface (IPMI) Baseboard Management Controller port that, when cabled and configured, allows remote management and monitoring. IPMI is a specification for providing management and monitoring capability directly to computer hardware without requiring access to the firmware or software.

Detailed guidance on using and managing IPMI for the Hitachi NAS platform Gateway models (HNAS 4xx0, HNAS 5x00) can be found in the “Remote Management using IPMI on HNAS” documentation, referenced in Appendix B. Note that IPMI configuration must be performed on each node in a cluster and not just the system hosting the Admin EVS.

Before using IPMI with an HNAS server, note the following security considerations:

- Ensure that any HNAS server Linux passwords are changed from the default password, especially the root user password.
- Ensure that the ADMIN password on the IPMI installation is changed from the default password.
- Configure IPMI to use a dedicated network port which is connected to a dedicated secure network that cannot be accessed from anywhere except the remote monitoring site.

These steps help to protect your HNAS server from unauthorized access.

Changing the IPMI ADMIN user password on **HNAS 4xx0 Gateway models**

By default, IPMI management is performed as the IPMI “ADMIN” user, and it is recommended that you change this password from the default.

Changing this password should only be attempted from the root user of the underlying Linux operating environment on a node and not the Bali CLI. This can be achieved with the provided tool, “ipmi-adminpasswd”. You will not be required to enter the existing password:

```
# ipmi-adminpasswd password
```

Where *password* is the desired new password.

Changing the IPMI ADMIN user password on **HNAS 5x00 Gateway models**

By default, IPMI management is performed as the IPMI “ADMIN” user, and it is recommended that you change this password from the default.

Changing this password should only be attempted from the root user of the underlying Linux operating environment on a node and not the Bali CLI. This is achieved with the provided “ipmitool” command. This tool requires the ID of the ADMIN user to be passed as an argument, to identify the account being updated. This can be found in the first column of the output from:

```
# ipmitool user list | grep ADMIN
```

You can then pass the ADMIN_ID as an argument to “ipmitool” to change the password by typing:

```
# ipmitool user set password <ADMIN_ID>
```

Configure IPMI to use a dedicated network port on HNAS 4xx0 Gateway models

It is possible to access the IMPI Baseboard Management Controller facilities from the Ethernet management port when IPMI has been configured in “Failover” or “Shared” network mode. It is recommended that functionality be disabled and “dedicated” mode be used, which will limit IPMI access via the configured IPMI network port.

Changing this setting should only be attempted from the root user of the underlying Linux operating environment on a node and not the Bali CLI. This is achieved with the provided “ipmiport” tool.

To check the current settings:

```
# ipmiport
```

To switch to dedicated mode:

```
# ipmiport --dedicated
```

Configure IPMI to use a dedicated network port on HNAS 5x00 Gateway models

It is possible to access the IMPI Baseboard Management Controller facilities from the Ethernet management port when IPMI has been configured in “Failover” or “Shared” network mode. It is recommended that functionality be disabled and “dedicated” mode be used, which will limit IPMI access via the configured IPMI network port.

Changing this setting should only be attempted from the root user of the underlying Linux operating environment on a node and not the Bali CLI. This is achieved with the provided “ipmitool” command:

To check the current settings:

```
# ipmitool raw 0x30 0x70 0x0c 0
```

The value returned can be decoded as follows: 00=dedicated, 01=shared, 02=failover

To switch to dedicated mode:

```
# ipmitool raw 0x30 0x70 0x0c 1 0
```

Statement of Volatility

All Hitachi NAS model types contain a mix of both volatile and non-volatile memory. For Gateway Hitachi NAS (HNAS 4xx0) models and Unified (VSP F/G/Nx00) NAS modules there are no remnants of user data retained in the server memories when the power and battery backup are removed.

Storage devices used to house the servers’ operating environments may contain customer identifiable data. These are field replaceable units and can be overwritten or retained by end customers, where security procedures require it.

Some statistical data, such as performance data and event logs, may remain in non-volatile memories. A statement of volatility detailing individual memory usage, the types of data stored within them and procedures for securely erasing those memories is available on request for these models.

The Gateway Hitachi NAS 5x00 models include super capacitor-backed non-volatile dual inline memory modules (NVDIMM) hardware. A statement of volatility specific to these models, in addition to instructions for the removal of NVDIMM modules is referenced in Appendix B.

Chapter 3: Protocols and Ports

All Hitachi NAS models use a variety of protocols and associated network ports necessary to provide file-serving, management and inter-cluster and communication. As part of good security practice an external firewall or similar security device should be leveraged to filter and limit access to Hitachi NAS resources.

We publish a list of the default ports used by both Hitachi NAS systems and their associated System Management Units in the Hitachi NAS Network Administration Guide, referenced in Appendix B.

Chapter 4: System Administration

Default Management Accounts

This section lists the default system user accounts for Hitachi NAS Platform, NAS module, and embedded or external SMU.

Contact Customer Support to obtain the default passwords for the accounts.

Caution: It is important to change the passwords from the defaults to new, secure passwords.

System component	User account name
Hitachi NAS Platform	
NAS Manager (Embedded SMU)	admin
Storage server CLI	supervisor manager
Linux CLI*	root supervisor manager
NAS module**	
File-serving CLI	maintenance supervisor manager
Linux CLI	maintenance supervisor manager
Linux CLI*	root
NAS Manager (Embedded SMU)	maintenance supervisor manager
External SMU	
NAS Manager	admin
SMU CLI	manager
SMU CLI*	root

Notes:

* The root account provides unlimited access and should only be used with guidance from Customer Support. It is not possible to ssh as this user. The root account must not be deleted but its password can and should be changed.

** To configure NAS module users, use the Maintenance Utility. Only the supervisor user can be created or deleted using the CLI. However, it is possible to log into the CLI and embedded SMU on the NAS module using the credentials of a user defined in the Maintenance Utility with the "Administrator user Group" role. Maintenance Utility users with different permissions cannot log into the NAS module or embedded SMU.

Configuring server management access

The NAS Manager provides the primary management interface for managing the server. In certain circumstances, however, an administrator may wish to use one of the following alternatives:

- The command line interface (CLI), accessible through SSH.
- The SSC utility, available for both Windows and Linux/UNIX.
- Simple Network Management Protocol (SNMP).

To protect the server from unauthorized access, various safeguards have been built in. Statistics are available to monitor access through these various methods. The following sections detail the configuration options that secure the server's management interfaces and ports.

To prevent unauthorized access to the storage system, you should configure the server to respond only to predefined (authorized) management hosts on the network, based on the management access method (Telnet, SSC and SNMP) and defined port number. You can enable or disable access through SSC and SNMP entirely, and you can specify certain configuration settings to control how those protocols can be used.

CLI Session Timeout

The server CLI is typically accessed by first making an SSH connection to the SMU. On an external SMU, this connection is subject to two inactivity or idle session timeouts: one to end idle bash shell sessions after 600 seconds of inactivity, and another to end idle SSH sessions after 300 seconds of inactivity.

Both idle session timeouts are configurable and can also be disabled. However, they must be adjusted as the root user on the SMU using the instructions below, rather than manually editing configuration files in the underlying Linux operating environment.

Adjusting the bash idle session timeout

This example disables the timeout, by setting the timeout value to 0. Alternatively, a desired number of seconds can be used to increase the default timeouts. The use of 'sudo' as the root user is deliberate, to ensure the changed is logged.

```
# echo etc-bashrc-tmout=0 \
| sudo tee --append /var/opt/smu/conf/mgr/axalon.properties

# sudo /opt/smu/mgr-scripts/smu-update-bashrc
```

Adjusting the SSH idle session timeout

This example disables the timeout, by setting the timeout value to 0. Alternatively, a desired number of seconds can be used to increase the default timeouts. The use of 'sudo' as the root user is deliberate, to ensure the changed is logged.

```
# echo "sshd-config-client-alive-interval = 0" \
| sudo tee --append /var/opt/smu/conf/mgr/axalon.properties

# sudo /opt/smu/mgr-scripts/smu-update-sshd
```

Restricting CLI commands

Dynamically managing the access level of some CLI commands can help prevent system users from viewing and/or changing sensitive company data.

Note: This ability is only available on the CLI. It is not possible to restrict command access through the NAS Manager which already has a read-only user.

Restricting CLI commands on the NAS server can prevent exposure of sensitive data, such as:

- File names and contents
- Directory names and contents
- User names
- Client IP addresses

The restriction is cluster wide and affects all EVSs and tenants.

To use the commands which set and unset restricted access, contact your Hitachi Vantara customer support representative. Administrators can list the commands that have been restricted using the Supervisor level **`user-level-override-list`** CLI command. It also lists the restricted command's current access level.

SMU Management Accounts

The SMU manages the storage servers/clusters and controls data migration and replication policies and schedules. For example, you can:

- Secure the SMU, so that only certain predefined hosts can access the SMU for management purposes.
- Configure an external SMU to act as an SMTP relay to the public network.

For an external SMU, basic SMU configuration is usually performed as a part of system initialization. The SMU setup wizard is used to complete the basic configuration of an SMU. Using the SMU Setup Wizard, you can change the administrator's password, set up name services for network operation, specify an SMTP server to relay email from the NAS server, and configure the date and time settings.

SMU Management Accounts: Authentication

When an SMU user administrator attempts to log in, the user ID/password combination is sent to the SMU for authentication. For the SMU, authentication means testing the user ID and password pair, to see if the supplied password matches the stored password for the supplied user ID. Depending on the SMU configuration and the supplied user ID, the SMU may authenticate the user itself (locally), it may authenticate the user through a RADIUS server, or it may authenticate the user through Active Directory. After authorization, the SMU allows the user to perform actions allowed by the user's profile.

Instead of maintaining a separate set of user details, the administrator can use an Active Directory enterprise user database. Active Directory groups can be granted access to the SMU. Then, AD users that belong to these groups, can log into the SMU using their usual name and password.

Groups of Active Directory users can have their access restricted to certain roles. For example, giving an Active Directory group a ‘server’ level access, will restrict all the users that belong to such group to be able to only manage HNAS servers. They will not be able, for example, to make any changes related to SMU administration.

Although the SMU supports RADIUS and Active Directory for external authentication, they are mutually exclusive; it is not possible to have them both configured for external authentication at the same time. When a login attempt is made, the SMU first tries to authenticate the credentials as a local user. If that fails, and Active Directory is configured, they are authenticated as an Active Directory user.
Active Directory authentication requests are sent to servers in the configured sequential order. If a successful connection cannot be made to the first server or a referral error is returned, it attempts to contact the second server and so on. When a connection is made, and an authentication response received (either positive or negative) it is treated as definitive. It does not then contact further servers because all servers are assumed to belong to the same Active Directory Forest.

Detailed steps for adding local or externally authenticated SMU management accounts are provided in the Storage System User Administration Guide, referenced in Appendix B.

SMU Management Accounts: Roles

Management accounts on the SMU are assigned user levels or roles that define the management access available to that account and are referred to as a user profile. These pre-defined roles are:

- **Global Administrators** can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server+Storage Administrators, and other Global Administrators).

  Global Administrators also control what servers and storage devices each administrator can access.

- **Storage Administrators** manage storage devices, as specified in the administrator profile created by the Global Administrator.

  Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users.

- **Server Administrators** manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices.

  Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules.

- **Server+Storage Administrators** manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator.

  Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage file systems, file services, or file system related features and functions, and they can also manage storage devices and their components.

All administrators can connect to the NAS storage system through NAS Manager, the browser-based management utility provided by the system management unit (SMU).

Additionally, Global Administrators on an external or virtual SMU can connect to the SMU command line interface (CLI). SMU CLI access is not available on an embedded SMU or a NAS module SMU.

SMU Management Accounts: Read-only Users

Local users and Active Directory groups can now be given read-only access. A read-only user has permission to view most pages of the NAS Manager; however, they are not generally allowed to perform any actions on the NAS Manager that would trigger a system or configuration change. Based on their defined role, an individual user may or may not perform specific tasks, such as viewing, creating, or modifying files and data. A read-only user may not create, add, or delete files and file systems. Where such actions are not permitted, the corresponding buttons (such as **Add** and **Create**) on the viewed page are disabled. A read-only user retains the scope of their role, such as Global, Storage, Server, or Server plus Storage, and the read-only attribute will not limit which configurations the user may access (except in cases where access to a specific configuration is explicitly defined as limited). All links appropriate to each role are visible on the pages but may be disabled. A global, read-only user can see all configurations. If the system has determined that the logged-on user, either a local user or an Active Directory user, has read-only access, the text "read-only" is appended to the user's name in the top-right corner of the page.

Read-only users can view the **Details** pages and see the objects on those pages, but buttons that submit changes, such as the **OK** button, are disabled. Read-only users may use the **Cancel** button on a **Details** page to navigate away from the page.

Note: Once a user is assigned the read-only attribute, their status as read-only may not be changed. To change a user's status from read-only, it is necessary to delete the user or the Active Directory group and re-add them with new read/write privileges.

Restricting Access to the SMU

It is possible to restrict access to the SMU to a defined set or range of IP addresses in CIDR notation, on the SMU's Security Options screen.

Detailed steps, and the options available for different server models, are provided in the Storage System User Administration Guide, referenced in Appendix B.

SMU Password Controls

On the SMU any logged in user can change their own password. A user with a Global Administrator user profile can also change the password of any user, whether the user is currently logged in or not using SMU GUI or the SMU CLI to change the user password. For systems with NAS modules, use an external SMU or the maintenance utility to change the user password.

This applies to locally defined users on the SMU only. If an account is authenticated through a RADIUS server or via Active Directory, its password must be changed using the tools and utilities available on those systems.

Locally defined SMU users are subject to password complexity and password length controls defined in the underlying Linux operating environment and recorded in /etc/security/pwquality.conf

Login banners

The SMU GUI can be used to create and customize a login security banner, to contain a sample security message to be displayed to all CLI and SMU GUI users, via the SMU's Security Options screen.

The steps and options available on that screen are detailed in the Storage System User Administration Guide, referenced in Appendix B.

Management Auditing

The NAS server supports auditing of administrative and management operations by reporting real-time configuration changes to a local file on the cluster node and, if configured, an external syslog server. Events are described using the Common Event Format (CEF). This enables Administrators to recognize and track any management operations which can impact the security of customer data on the server and take remedial action more quickly.

Note: The audit log data is not replicated across nodes. Each cluster node records audit events for operations which were performed on that cluster node. General administration operations are audited where the admin EVS is located, while service EVS-specific operations are audited on the node where the service EVS is located. If the Administrator configures an external syslog server, all cluster nodes also send their audit events to that server.

The server records the following types of operations:

- **Activity masking** - Commands which disable logging, auditing, or alerts.
- **Vulnerability creation** - Commands which modify security or allow security to be bypassed for Administrators or protocol clients.
- **Data compromising** - Commands which copy or display customer and other data from the server.
- **Retention compliance** - Commands which destroy customer data.
- **Operational** - Operations that impact the availability or performance of the server.

The following commands are available for the configuration of management auditing:

- **audit-mgmt-log** - displays the content of the management audit log on the present cluster node.
- **audit-mgmt-log-server-add** - configures the NAS server to send management audit events to an external syslog server.

- **audit-mgmt-log-server-connections** - displays the connection status (on the present cluster node) for currently configured syslog servers to which the NAS server sends management audit events.
- **audit-mgmt-log-server-delete** - removes a previously configured syslog server from the list of servers to which the NAS server sends management audit events.
- **audit-mgmt-log-server-list** - displays the currently configured syslog servers to which the NAS server sends management audit events.
- **audit-mgmt-log-stats** - displays or resets statistics about entries written to the management audit log on a single cluster node.

For more information, see the Hitachi NAS Command Reference documentation referenced in Appendix B.

A complete list of all Management Audit events is available in the Server and Cluster Administration Guide also referenced in Appendix B.

Chapter 5: File System Security

EVS Security Context

Secure Virtual Servers

A secure virtual server is a file serving EVS that has a specifically defined security configuration (called an individual security context). When no individual security context is specified for an EVS, it uses the global (server or cluster-wide) security configuration settings (the global security context). By defining an individual security context for a particular EVS, you create a secure virtual server (secure EVS)

Note: Secure virtual servers are a licensed feature, identified as EVS Security. Without an EVS Security license, all EVSs use the global security settings (context).

- When no individual security context is defined for an EVS, the global security settings (the global context) are used by default. When an individual security context is added to an EVS, the new individual security context is created using the same settings as are used by the global security context. After adding the individual security context, you can then change settings to make the individual security context settings different than the global settings.

- When using an individual security context, the EVS security context can be configured independently of the global (server or cluster-wide) security settings.

When present, individual security context settings override the global security context settings, allowing a storage server (or cluster) to be shared by multiple groups (departments, customers, or organizations), while maintaining strong security so that no group has access to another group's data.

For example, if a server/cluster has six EVSs, you could define individual security contexts for two of the EVSs, turning them into secure EVSs. Each secure EVS could then be associated with an Active Directory domain that is different than the one used by the cluster, meaning that each of those secure EVSs could be assigned to its own domain. For network clients, access to the file systems in the secure EVSs can then be restricted or allowed as desired using standard network security policies such as username or user group membership.

Secure EVS Considerations

When using secure EVSs, keep the following points in mind:

- **Security context defaults**. Unless an individual security context is specified for an EVS (making it a secure EVS), the EVS security context defaults to the global security context.

- **Inherited global settings**. NDMP username and password settings are not EVS-specific; the same NDMP username and password settings apply to all EVSs and secure EVSs in a server/cluster.

- **Secure EVS-specific security settings**. After an EVS has a defined individual security context, it becomes a secure EVS, and each secure EVS is considered separate from all other EVSs and secure EVSs in the server or cluster.

  A secure EVS is always treated as an individual unit, whether it uses the same security context settings as another secure EVS or uses different security context settings. As a result, different secure EVSs cannot share anything, including an individual EVS name space.

- **Secure EVS migration**. When a secure EVS migrates to a different cluster, it retains all specified security settings in its individual security context. If, however, a secure EVS is configured to use default settings from the global context, then the secure EVS uses the settings in the global context of the cluster to which it migrates.

- **Moving file systems between secure EVSs**. A system administrator with sufficient privileges can move a file system from one secure EVS to another, but a warning is issued if the security contexts of the source and destination secure EVSs are different.

- **External name server access**. Each secure EVS can be configured to connect to several external name servers, and each secure EVS can connect to different name servers.

- **Secure EVSs and name spaces**. Links from the cluster's CNS tree to a secure EVS are supported, according to the following rules:

  - **Accessing the CNS**. Only a secure EVS that uses the global security context can access links in the CNS.

  - **CNS links to a file system hosted by a secure EVS with an individual security context are not allowed**. In the CNS, you cannot add a link to a file system hosted by a secure EVS. Similarly, you cannot configure an individual security context for an EVS (turning an EVS into a secure EVS) if there are CNS links to one or more file systems in that EVS.

  - **Name space usage and the secure EVS**. If you want to use a name space with a secure EVS that does not use the global configuration settings, you must configure an EVS name space for that secure EVS. An EVS name space is required because file systems hosted by the secure EVS cannot be linked to from the CNS, and file systems hosted by the EVS cannot access links in the CNS.

    If you want to use a name space with a secure EVS that does use the global configuration settings, you may configure an EVS name space for that secure EVS, but it is not required. If the secure EVS uses the global security settings, the file systems hosted by the EVS can access links in the CNS.

  - **Links to a secure EVS individual name space**. In a secure EVS with an individual name space, you can add links between file systems hosted by the same secure EVS.

- **Configuring a group of EVSs with the same settings**. To create a group of secure EVSs that use the same individual security context settings (that are different from the global settings), you must configure each secure EVS in the group separately.

- **Reconfiguring a secure EVS security context to use the global context**. If a secure EVS is reconfigured to use the global security context (reverting it to an EVS), and the secure EVS was using a different NT domain than the cluster, CIFS names and CIFS share names become invalid. This occurs because CIFS names (and CIFS share names) are associated with a specific NT domain, and the NT domain name changes.

  If the global security context and the secure EVS and the NT domain are different, after you remove the secure EVS' individual security context (making it an EVS again), you must delete all CIFS names for the EVS and all CIFS shares for the file systems in the EVS. Then, you must recreate the EVS CIFS names and the CIFS shares for the file systems in the EVS.

About security contexts

Because EVSs and secure EVSs inherit many of their settings from the cluster's global context, when configuring name services, you must specify if you want to change the global context or the individual context.

The EVS security context can be any of the following:

- **Global Configuration**, which indicates that the current security context is the global context.
- **Inherits Global Configuration**, indicates that the EVS is a regular EVS (not a secure EVS), and uses the security context settings defined in the global security context.
- **Individual Configuration**, indicates that the current security context is an individual context with individually specified settings.

Security Mode

A HNAS system allows access to the contents of file system from both Unix-like and Windows clients, often simultaneously. The file system Security Mode determines how access controls will be set on a given file system or virtual volume. As the HNAS needs to provide access to files for multiple operating system types, files on a file system need to be able to support both Unix style and Windows style file access controls.

Two Security Modes are available: Unix and Mixed. By default, a file system will inherit its Security Mode from the EVS it is assigned to, and a virtual volume inherits its Security Mode from the file system it is part of. However, Security Modes can be explicitly configured to differ from their defaults.

Regardless of the HNAS Security Mode chosen, every file will have an associated UID, GID and mode, most traditionally seen with Unix-like security models. Choosing a Mixed HNAS Security Mode additionally associates a Security Descriptor with a file. This allows for a richer set of access controls, as seen in a Windows security model. If a file has an associated Security Descriptor, then that will be used to determine access rights and an appropriate UID, GID and mode will be set to reflect that access.

iSCSI Security

Configuring iSCSI security (mutual authentication)

The storage server uses the Challenge Handshake Authentication Protocol (CHAP) to authenticate iSCSI initiators. CHAP requires a “shared secret” known by the initiator and the target. The server also supports mutual authentication where, in addition to the initiator authenticating against the target on the server, the server must also authenticate against the initiator.

To facilitate the mutual authentication process, the server must maintain a list of the initiators with which it can authenticate, and the shared secret for each initiator.

You can configure the storage server for mutual authentication in the NAS Manager GUI.

Logical unit security

As LUs are files, they can be accessed over other protocols, such as SMB and NFS. This renders LUs vulnerable to malicious users who can modify, rename, delete, or otherwise affect them.

Caution: customer support recommends setting sufficient security on either the LU file, the directory in which it resides, or both, to prevent unwanted access.

File System Auditing

File system auditing monitors and records file access and modification operations performed through the SMB and NFSv3 protocols. Records are made using the Windows Event log format and can be stored to the file system's audit log or made available to third-party external tools.

File system audit logging is performed and controlled on a per file system basis.

Currently, file system auditing is only supported for operations using SMB and NFSv3. By default, when file system auditing is enabled, access to the audited file system is only allowed for these two protocols. However, access by clients using other protocols like NFSv2, can optionally be allowed. When such access is allowed, access to file system objects through these protocols is not audited.

Note: Auditing of SMB is based on the open and close operations; because NFSv3 is a stateless protocol and lacks equivalent operations, auditing checks must be performed on each I/O operation, which can be costly in terms of system performance.

After a file has been externally migrated (to an external server, e.g., to a Hitachi Content Platform (HCP) system), subsequent access to the file through the NAS server is audited as if the file were still local.

Controlling file system auditing

File system auditing requires that a file system audit policy be defined for the file system to be monitored, and that auditing is enabled for the specific file system. File system auditing is performed and controlled on a per file system basis.

Creating a file system audit policy

The file system audit policy specifies access restrictions for clients connecting through un-auditable protocols (if access is allowed or denied) and specifies audit log details. The audit log policy specifies naming, location in the file system, size, the log rollover policy, and the backup policy.

You can configure the file system audit policy in the NAS Manager GUI.

Chapter 6: Antivirus

Virus scanning overview

The storage server architecture reduces the effect of a virus because the file system is hardware-based. This prevents viruses from attaching themselves to (or deleting) system files required for server operation. However, viruses can still propagate and infect user data files stored on the server.

The server does not scan the files but provides a connection with configured Virus Scan Engines on the network.

You can configure multiple Virus Scan Engines to enhance both the performance and to maintain high availability of the server. If a Virus Scan Engine fails during a virus scan, the storage server automatically redirects the scan to another Virus Scan Engine.

The server maintains a list of file types, the Inclusion List, that allows the administrator to control which files are scanned (for example, .exe, .dll, .doc, and so forth). The default Inclusion List includes most file types commonly affected by viruses.

You can also set a list of file types on a file system that will be excluded from being sent for scanning by antivirus servers. With an exclusion list you can scan all files except those with certain file extensions, for example, those containing application data. This helps reduce the load on the virus scanning engines and network.

As with the inclusion list, the exclusion list will support wildcarding. The exclusion list is configurable using the command line interface.

Caution: When virus scanning is enabled, the server must receive notification from a Virus Scan Engine that a file is clean before allowing access to the file. As a result, if virus scanning is enabled and there are no Virus Scan Engines available to service the virus scans, CIFS clients may 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.

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

The Hitachi NAS platforms storage systems proactively submit files for scanning to the scan engine on both read (open) and changes and modifications associated with a write (close). If a file has not been verified by a virus scan engine as clean, it will need to be scanned before it can be accessed. However, scanning for viruses when a client is trying to access the file can take time (on read only). To reduce this latency, files are automatically queued to be scanned as soon as they are created or modified, and then closed (on writes).

Queued files are scanned promptly, expediting the detection of viruses in new or modified files, making it unlikely that a virus infected file will remain dormant on the system for a long time.
Virus Scanning statistics for the storage server (in 10-second time slices) are available for activity since the previous reboot or since the point when statistics were last reset.

When a virus is detected, a severe event is placed in the Event Log, identifying the path of the infected file and the IP address of the infected machine. For information on accessing the event log, see the Server and Cluster Administration Guide referenced in Appendix B.

Both DCE/RPC and ICAP protocols are separately supported when communicating with external Virus Scan Engines. For more details, see the Antivirus Administration Guide referenced in Appendix B.

Chapter 7: Backup

In addition to file-based replication and “classic” data migration features, all HNAS models support Network Data Management Protocol (NDMP), an open standard protocol for network-based backup.

Primary NDMP User

All NDMP-functionality is driven by a Data Management Application, for backup purposes this is usually a third-party application, or the Accelerated Data Copy (ADC) command line utility provided with the SMU. To start a backup or restore operation, a Data Management Application must authenticate as an NDMP user, configured on the HNAS system.

It is important to note that any user with knowledge of the configured NDMP password can use a Data Management Application to access data on the HNAS system. It is strongly recommended that the password and/or username be changed from the default. This process can be performed on the SMU by navigating to the NDMP Configuration page. Guidance on performing this action can be found in the Hitachi NAS Backup Administration Guide, referenced in Appendix B.

Restricted NDMP Users

An Administrator can optionally choose to create NDMP users with more restrictive access to files/directories on an EVS and/or backup devices. This can be achieved via the HNAS CLI commands **`ndmp-ruser`** and **`ndmp-ruser-pwd`**. This functionality is normally used in concert with the Accelerated Data Copy (ADC) command line utility provided with the SMU. The details and the options available to those commands are described in the Hitachi NAS Command Reference documentation referenced in Appendix B.

Appendix A: References

Hitachi Vantara Vulnerability Disclosure Policy

Customers are encouraged to report potential security vulnerabilities via the Global Support Centre. Our disclosure policy is available on the Hitachi Vantara Knowledgebase:

https://knowledge.hitachivantara.com/Security/Hitachi_Vantara_Vulnerability_Disclosure_Policy

Hitachi Vantara Security Advisories - Index Page

Whenever a cybersecurity vulnerability is identified and reported, Hitachi Vantara investigates its product lines to determine any impact and presents information on those vulnerabilities on the Hitachi Vantara Knowledgebase:

https://knowledge.hitachivantara.com/Security/CVE_Index_Page#Security_Advisories

Appendix B: Related Documentation

Documentation for the Hitachi NAS family of products can be located online:

- For all Hitachi NAS models: https://knowledge.hitachivantara.com/Documents/Storage/NAS_Platform

Document titles and part numbers referenced in this guide:

Hardware References

Hitachi NAS Platform and Hitachi Unified Storage Series 4000 Hardware Reference	MK-92HNAS030
Hitachi NAS Platform 5000 Series Hardware Reference	MK-92HNAS089
Hitachi Virtual Storage Platform G400, G600 Hardware Reference Guide	MK-94HM8022
Hitachi Virtual Storage Platform G800 Hardware Reference Guide	MK-94HM8026
VSP N400, N600 Hardware Reference Guide	MK-94HM8053
VSP N800 Hardware Reference Guide	MK-94HM8054

Remote Management using IPMI

Remote Management using IPMI on HNAS 4060/4080 and HNAS 4100 User Guide	MK-92HNAS084
Remote Management using IPMI on HNAS 5200 and HNAS 5300	MK-92HNAS092

Statement of Volatility

Hitachi NAS Platform 5000 Series Statement of Volatility	MK-92HNAS093
Hitachi NAS Platform 5000 Series Removing the NVDIMM	FE-92HNAS065

Network Administration Guide

Network Administration Guide: Hitachi Virtual Storage Platform Gx00 and Fx00 with NAS Modules, VSP N series, Hitachi NAS Platform	MK-92HNAS008

Backup Administration Guide

Backup Administration Guide: Hitachi Virtual Storage Platform Gx00 and Fx00 with NAS Modules, VSP N series, Hitachi NAS Platform	MK-92HNAS007

Server and Cluster Administration Guide

Server and Cluster Administration Guide: Hitachi Virtual Storage Platform Gx00 and Fx00 with NAS Modules, VSP N series, Hitachi NAS Platform	MK-92HNAS007

Storage System User Administration Guide

Storage System User Administration Guide: Antivirus Administration Guide: Hitachi Virtual Storage Platform Gx00 and Fx00 with NAS Modules, VSP N series, Hitachi NAS Platform	MK-92HNAS013

Antivirus Administration Guide

Antivirus Administration Guide: Hitachi Virtual Storage Platform Gx00 and Fx00 with NAS Modules, VSP N series, Hitachi NAS Platform	MK-92HNAS004

Command Reference

NAS Module Server Command Reference	MK-92HNAS073
NAS Platform 4000 Series Command Reference	MK-92HNAS062
NAS Platform 5000 Series Command Reference	MK-92HNAS090

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com