HITACHI
Inspire the Next

System Administrator Guide

Hitachi Virtual Storage Platform G200, G400, G600, G800

Hitachi Virtual Storage Platform F400, F600, F800

Hitachi Data Systems

MK-94HM8016-02

November 2015

Hitachi, Ltd., reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Data Systems Corporation at https://support.hds.com/en_us/contact-us.html.

Notice: Hitachi, Ltd., products and services can be ordered only under the terms and conditions of the applicable Hitachi Data Systems Corporation agreements. The use of Hitachi, Ltd., products is governed by the terms of your agreements with Hitachi Data Systems Corporation.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from employees and other individuals to access relevant data; and
2. Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Contents

Preface

This document provides information and instructions to help you use the maintenance utility and some of the functions in Device Manager - Storage NavigatorDevice Manager - Storage Navigator as needed to perform system administration tasks and change settings for Hitachi Virtual Storage Platform G200, G400, G600, G800 or Hitachi Virtual Storage Platform F400, F600, F800 storage systems. It explains the GUI features and provides basic navigation information.

Please read this document carefully to understand how to use the software described in this manual, and keep a copy for reference.

Intended audience

This document is intended for system administrators, Hitachi Data Systems representatives, and authorized service providers who are involved in installing, configuring, and operating Hitachi Virtual Storage Platform G200, G400, G600, G800 or Hitachi Virtual Storage Platform F400, F600, F800 storage systems.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- Hitachi Virtual Storage Platform G200, G400, G600, G800 or Hitachi Virtual Storage Platform F400, F600, F800 storage systems.
- The operating system and web browser software on the SVP hosting the Device Manager - Storage Navigator software.
- The Windows 7 operating system and the management software on the management server.

Product version

This document revision applies to firmware 83-02-0*x* or later for Hitachi Virtual Storage Platform G200, G400, G600, G800 or Hitachi Virtual Storage Platform F400, F600, F800.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document.

Changes in this revision

- Added support for Hitachi Virtual Storage Platform F400, F600, F800 storage systems.
- Clarified how to set up Internet Explorer. For details, see Configuring Internet Explorer for Device Manager - Storage Navigator on page 26.
- Added details about modifying SVP port numbers. For details, see Modifying SVP port numbers on page 42 and Effects of changing SVP port numbers on page 44.
- Added details about managing user accounts. For details, see Workflow for creating and managing user accounts on page 60.
- Added the report PECBInfo.csv on page 182.
- Updated the descriptions of the following reports:
  - Host Groups / iSCSI Targets report on page 132
  - Hosts report on page 133

  - ○ LUNs report on page 135
  - ○ Ports report on page 141
  - ○ Channel Boards report on page 152
  - ○ ChapUserInfo.csv on page 160
  - ○ ChaStatus.csv on page 161
  - ○ DeviceEquipInfo.csv on page 161
  - ○ DkcInfo.csv on page 162
  - ○ ELunInfo.csv on page 163
  - ○ HduInfo.csv on page 167
  - ○ IscsiHostInfo.csv on page 168
  - ○ IscsiPortInfo.csv on page 168
  - ○ IscsiTargetInfo.csv on page 169
  - ○ LdevInfo.csv on page 171
  - ○ LunInfo.csv on page 174
  - ○ LunPortInfo.csv on page 175
  - ○ PcbRevInfo.csv on page 179
  - ○ PdevInfo.csv on page 180
  - ○ PkInfo.csv on page 182
  - ○ SsdDriveInfo.csv on page 184
  - ○ WwnInfo.csv on page 186

Referenced documents

- *Hitachi Command Suite User Guide*, MK-90HC172
- *Hitachi Audit Log User Guide*, MK-94HM8028
- *Performance Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*, MK-94HM8012
- *Encryption License Key User Guide*, MK-94HM8029
- *Hitachi ShadowImage® User Guide*, MK-94HM8021
- *Hitachi SNMP Agent User Guide*, MK-94HM8015
- *Hitachi TrueCopy® User Guide*, MK-94HM8019
- *Hitachi Universal Replicator User Guide*, MK-94HM8023
- *Hitachi Universal Volume Manager User Guide*, MK-94HM8024
- *Storage Subsystem Administration Guide*, MK-92HNAS012
- *Storage Systems User Administration Guide*, MK-92HNAS013
- *File Service Administration Guide*, MK-92HNAS006

Document conventions

This document uses the following terminology conventions:

Convention	Description
• Hitachi Virtual Storage Platform Gx00 models • VSP Gx00 models	All of the following storage systems: • Hitachi Virtual Storage Platform G200 • Hitachi Virtual Storage Platform G400 • Hitachi Virtual Storage Platform G600 • Hitachi Virtual Storage Platform G800
• Hitachi Virtual Storage Platform Fx00 models • VSP Fx00 models	All of the following storage systems: • Hitachi Virtual Storage Platform F400 • Hitachi Virtual Storage Platform F600 • Hitachi Virtual Storage Platform F800

This document uses the following typographic conventions:

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. • Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g` *`group`* (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`
< > angle brackets	Indicates variables in the following scenarios: • Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<`*`report-name`*`><`*`file-version`*`>.csv` • Variables in headings.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
⚠	Note	Calls attention to important or additional information.
💡	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
⚠	Caution	Warns the user of adverse conditions or consequences (for example, disruptive operations).
⚠	WARNING	Warns the user of severe conditions or consequences (for example, destructive operations).

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1{,}000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1{,}000^3$ bytes
1 terabyte (TB)	1,000 GB or $1{,}000^4$ bytes
1 petabyte (PB)	1,000 TB or $1{,}000^5$ bytes
1 exabyte (EB)	1,000 PB or $1{,}000^6$ bytes

Logical storage capacity values (for example, logical device capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: • OPEN-V: 960 KB • Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1{,}024^2$ bytes
1 GB	1,024 MB or $1{,}024^3$ bytes
1 TB	1,024 GB or $1{,}024^4$ bytes
1 PB	1,024 TB or $1{,}024^5$ bytes

Logical capacity unit	Value
1 EB	1,024 PB or $1,024^6$ bytes

Accessing product documentation

Product user documentation is available on Hitachi Data Systems Support Connect: https://support.hds.com/en_us/documents.html. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

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

Hitachi Data Systems Community is a global online community for HDS 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.hds.com, register, and complete your profile.

Comments

Please send us your comments on this document to doc.comments@hds.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Data Systems Corporation.

Thank you!

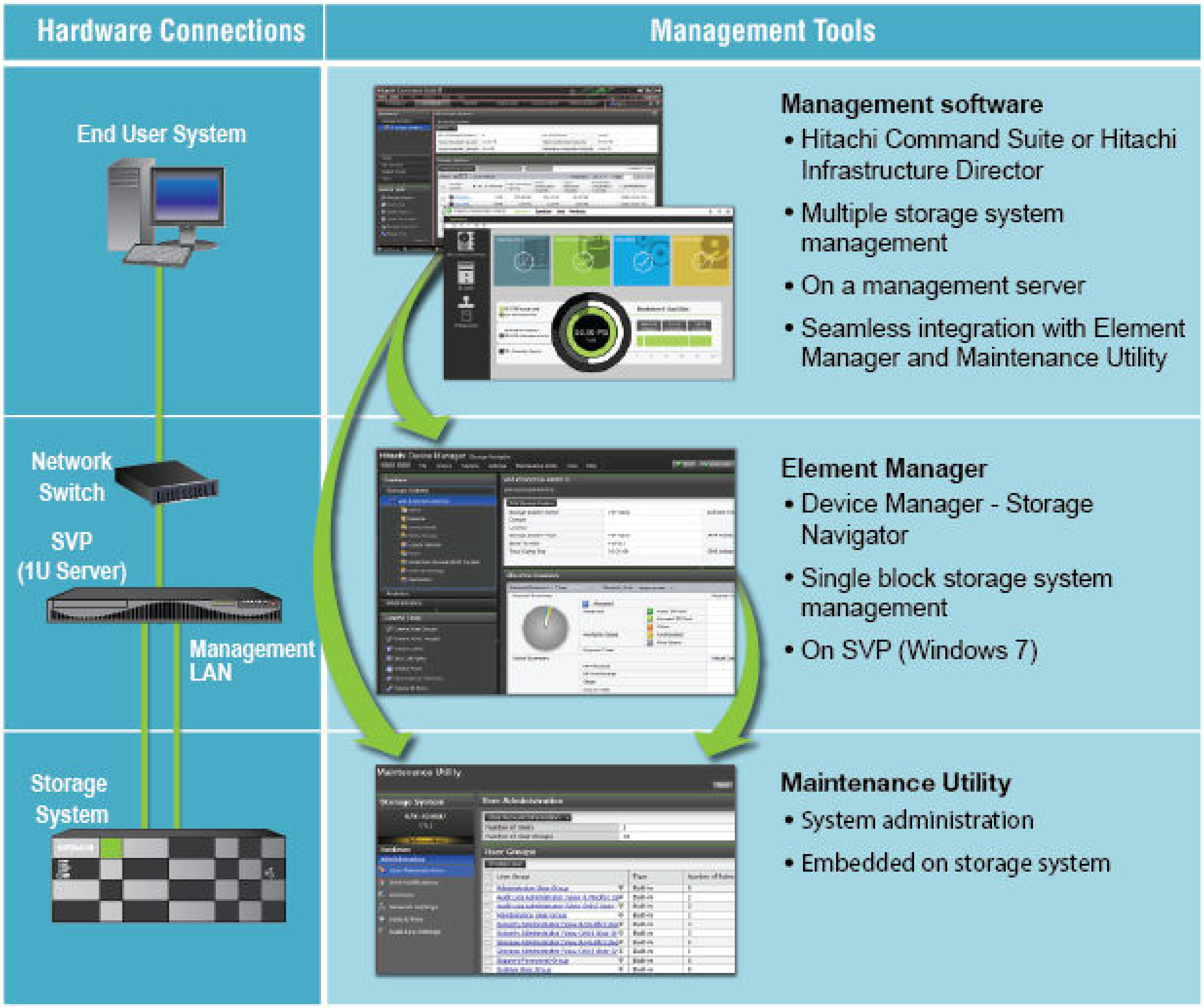
1

System administration overview

This chapter provides a high-level view of Hitachi Virtual Storage Platform G200, G400, G600, G800 or Hitachi Virtual Storage Platform F400, F600, F800 storage systems. It describes the various settings that you can use to configure and manage the SVP and the block element manager (Device Manager - Storage Navigator) running on the service processor.

System management architecture

The following illustration shows a high-level block diagram of the storage management software architecture. It shows the access points that a system administrator can use to configure and manage the system settings.


Hardware Connections
Management Tools
End User System
Network Switch
SVP
(1U Server)
Management LAN
Storage System
Management software
• Hitachi Command Suite or Hitachi Infrastructure Director
• Multiple storage system management
• On a management server
• Seamless integration with Element Manager and Maintenance Utility
Element Manager
• Device Manager - Storage Navigator
• Single block storage system management
• On SVP (Windows 7)
Maintenance Utility
• System administration
• Embedded on storage system

Administration tasks and tools

The system administration tasks described in this guide are for only the block module of a VSP G200, G400, G600, G800 or VSP F400, F600, F800 storage system. To perform administration tasks on the file storage (HNAS) in your environment, access the SMU from your file storage. See the following manuals for information on HNAS administration:

- *Storage Subsystem Administration Guide*

- *Storage Systems User Administration Guide*
- *File Service Administration Guide*

You can manage the system settings from the **Administration** menu in the maintenance utility, which can be accessed from either Device Manager - Storage Navigator or the management software. The following table lists the tasks and the tools needed to accomplish them.

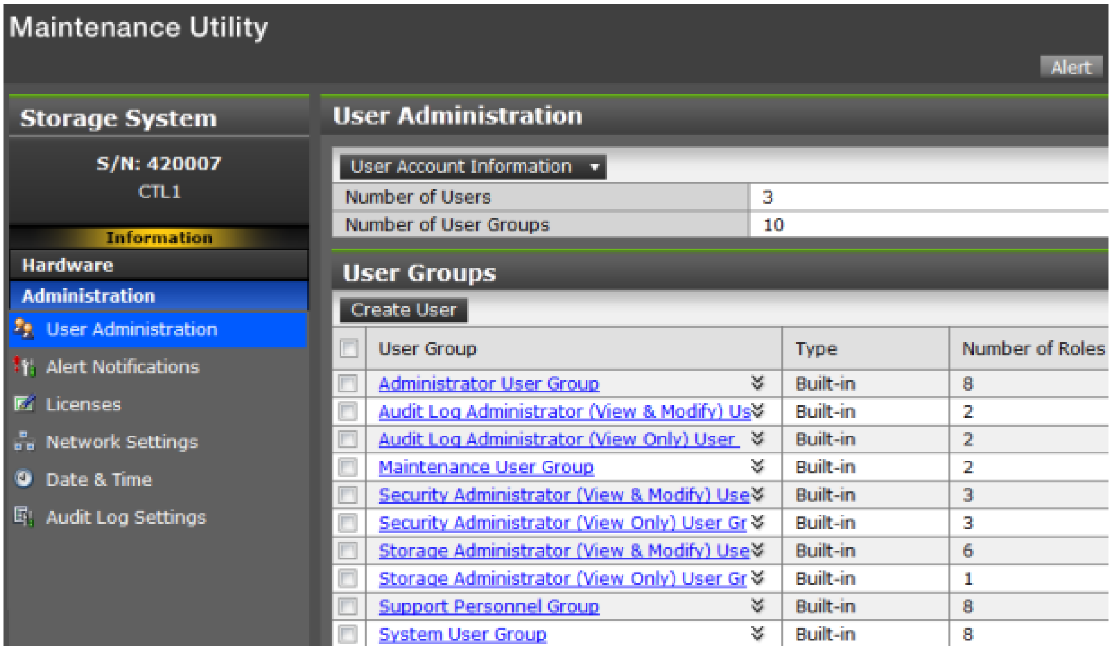
Table 1

Task	Software tools
• Set IPv4 and IPv6 network settings and set HTTP blocking	Device Manager - Storage Navigator > Maintenance utility > Network Settings. See Changing network settings on page 33.
• Set system clock (date and time)	Device Manager - Storage Navigator > Maintenance utility > Date & time. See Changing the date and time on page 32.
• Configure audit log settings	Device Manager - Storage Navigator > Maintenance utility > Audit log settings. See Audit log settings on page 114.
• Configure alert notifications	Device Manager - Storage Navigator > Maintenance utility > Audit log settings. See Alert notifications on page 89.
• Change administrator password • Edit the login message • Select the SSL cipher suite • Update certificate files • Force the system lock to release	Maintenance utility, lower menu. See System configuration on page 21.
• User administration - add, manage, and delete storage system users • Manage user groups	Device Manager - Storage Navigator, accessed from the management software, if available. See User administration on page 59.
• Register the service processor host name. • Change storage system information • Manage SSL certificates: create keypairs, obtain, update, and return certificates, verify and release passphrases • Manage HCS certificates • Manage HDvM - SN configuration files • Manage authorization and authentication servers • Create LDAP, RADIUS, and Kerberos configuration files • Access a storage system when the management software is unavailable	Device Manager - Storage Navigator, accessed from the management software, if available. See Accessing a storage system without the management software on page 98 for instructions to complete each task and the permissions needed to use the tools.

Maintenance utility

The maintenance utility is a tool that you use to perform administration tasks on VSP Gx00 models or VSP Fx00 models. You can access this tool from either HDvM - SN or the management software.

You can use the maintenance utility to configure settings such as licenses, syslog, alerts, and network configuration. As shown in the following figure, these settings are available from the **Administration** navigation tree.



Number of Users	3
Number of User Groups	10

□	User Group	Type	Number of Roles
□	Administrator User Group	Built-in	8
□	Audit Log Administrator (View & Modify) Us	Built-in	2
□	Audit Log Administrator (View Only) User	Built-in	2
□	Maintenance User Group	Built-in	2
□	Security Administrator (View & Modify) Use	Built-in	3
□	Security Administrator (View Only) User Gr	Built-in	3
□	Storage Administrator (View & Modify) Use	Built-in	6
□	Storage Administrator (View Only) User Gr	Built-in	1
□	Support Personnel Group	Built-in	8
□	System User Group	Built-in	8

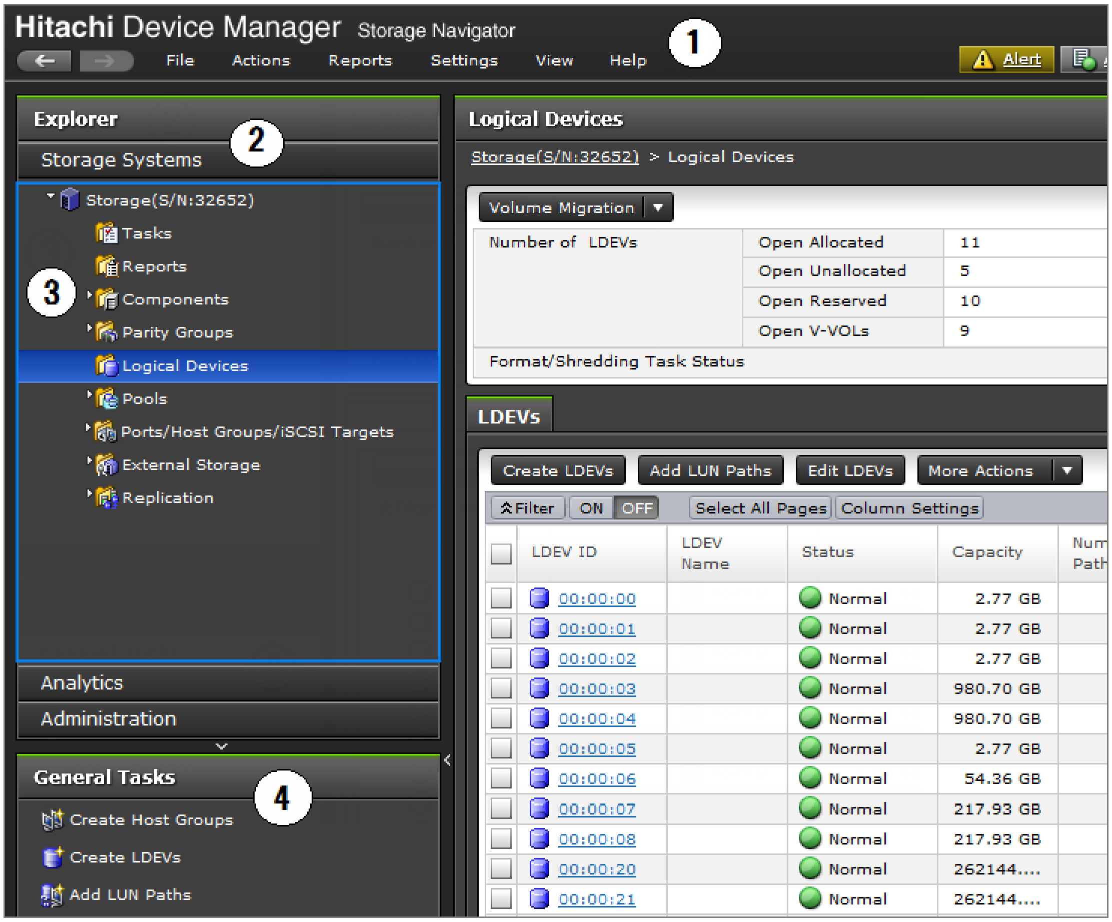
The maintenance utility online help provides procedural information for supported storage system administration tasks. Links to storage system tasks, search functions, and a glossary are included.

Note: Self-service features that are used to install and remove hardware components and to update the firmware are currently available for use only by Hitachi Data Systems customer support personnel or by authorized service providers.

Device Manager - Storage Navigator

Device Manager - Storage Navigator (HDvM - SN) is the element manager for the block module for VSP Gx00 models or VSP Fx00 models. It is a factory-installed application running on the SVP, which is directly connected to the storage system.

You can access Device Manager - Storage Navigator from the management software to perform additional system administration tasks on your storage system besides those available in the maintenance utility. In addition, you can easily access advanced storage configuration options while performing management operations with the management software.



Number of LDEVs	Open Allocated	11
	Open Unallocated	5
	Open Reserved	10
	Open V-VOLs	9
Format/Shredding Task Status		

□	LDEV ID	LDEV Name	Status	Capacity	Num Path
□	00:00:00		Normal	2.77 GB	
□	00:00:01		Normal	2.77 GB	
□	00:00:02		Normal	2.77 GB	
□	00:00:03		Normal	980.70 GB	
□	00:00:04		Normal	980.70 GB	
□	00:00:05		Normal	2.77 GB	
□	00:00:06		Normal	54.36 GB	
□	00:00:07		Normal	217.93 GB	
□	00:00:08		Normal	217.93 GB	
□	00:00:20		Normal	262144....	
□	00:00:21		Normal	262144....	

Device Manager - Storage Navigator allows you to set up and manage more than one storage system. It enables system administrators to have temporary access to the storage system when they cannot access the management software due to server or network issues.

Device Manager - Storage Navigator online help provides procedural information for setting up and managing the storage system. Links to the major storage system tasks, search functions, and glossary are included.

2

System configuration

This section provides instructions to manage the system configuration.

□ Backing up HDvM - SN configuration files

□ Restoring HDvM - SN configuration files

Setting up a management client

The Device Manager - Storage Navigator administrator is responsible for setting up the web client on management clients. This includes the following:

- Ensure that management clients can handle Device Manager - Storage Navigator.
- If you are using a Windows server as a management client, make sure to configure the server.

Requirements for management clients

This topic explains the requirements for management clients on supported versions of Windows and UNIX/Linux operating systems.

General requirements

- An SVP, required for system maintenance, must be installed on the storage system. Device Manager - Storage Navigator connects to the SVP through a TCP/IP network.
- Several storage systems can be managed by one management client. Device Manager - Storage Navigator must be set up for each storage system.
- A maximum of 32 Device Manager - Storage Navigator users can access the same storage system concurrently.

Requirements for Windows-based computers

⚠ **Note:** The combinations of operating system, architecture, browser, Java Runtime Environment, and Adobe Flash Player described below are fixed requirements. Using other combinations or versions might produce unpredictable results such as the inability to operate program windows. Therefore, contact Hitachi Data Systems customer support to use other combinations or versions.

Hardware requirements

Item	Requirement
Processor (CPU)	Pentium 4 640 3.2 GHz or better (Recommended: Core2Duo E6540 2.33 GHz or better)
Memory (RAM)	2 GB or more Recommended: 3 GB
Available storage space	500 MB or more
Monitor	True Color 32-bit or better

Item	Requirement
	Resolution: 1280 x 1024 or better
Keyboard and mouse	You cannot use the mouse wheel feature.
Ethernet LAN card for TCP/IP network	100BASE-T 1000BASE-T

Software requirements

Operating system[1]	Architecture	Browser (Internet Explorer)	Java Runtime Environment (JRE)	Adobe Flash Player[2]
Windows 7 SP1	32 bit	8.0	JRE 6.0 Update 20	10.3
		11.0	JRE 7.0 Update 67	14.0
	64 bit	8.0	JRE 6.0 Update 20	10.3
		11.0	JRE 7.0 Update 67	14.0
Windows 8.1	32 bit or 64 bit	11.0	JRE 7.0 Update 67	14.0
Windows Server 2008 R2 SP1	64 bit	8.0	JRE 6.0 Update 20	10.3
		11.0	JRE 7.0 Update 67	14.0
Windows Server 2012 R2	64 bit	11.0	JRE 7.0 Update 67	14.0

Notes:

1. If the SVP supports Internet Protocol Version 6 (IPv6), you can specify IPv6 addresses.
2. Use Adobe Flash Player with the same architecture (32 bit or 64 bit) as the browser.

Note: To use Device Manager - Storage Navigator secondary windows, first install Java Runtime Environment (JRE).

Requirements for UNIX/Linux-based computers

Note: The combinations of operating system, architecture, browser, Java Runtime Environment, and Adobe Flash Player described below are fixed requirements. Using other combinations or versions might produce unpredictable results such as the inability to operate program windows. Therefore, contact Hitachi Data Systems customer support to use other combinations or versions.

Hardware requirements

Item	Requirement
Processor (CPU)	Pentium 4 640 3.2 GHz or better (Recommended: Core2Duo E6540 2.33 GHz or better)
Memory (RAM)	2 GB or more

Item	Requirement
	Recommended: 3 GB
Available storage space	500 MB or more
Monitor	Resolution: 1280 x 1024 or better
Keyboard and mouse	You cannot use the mouse wheel feature.
Ethernet LAN card for TCP/IP network	100BASE-T 1000BASE-T

Software requirements

Operating system	Architecture	Browser[1]	Java Runtime Environment (JRE)	Adobe Flash Player[2]
Solaris 10	32 bit	Firefox 3.6.28 [3]	JRE 6.0 Update 20	10.3
		Firefox 31	JRE 7.0 Update 67	11.2
Red Hat Enterprise Linux AS version 6.2	64 bit	Firefox 3.6.28 [3]	JRE 6.0 Update 20	10.3
		Firefox 35	JRE 7.0 Update 67	11.2

Notes:

1. IPv6 HTTPS connections from Firefox are not supported.
2. Use Adobe Flash Player with the same architecture (32 bit or 64 bit) as the browser.
3. Device Manager - Storage Navigator supports Firefox 3.6.28, but the maintenance utility does not.

Note: To use Device Manager - Storage Navigator secondary windows, first install Java Runtime Environment (JRE).

Setting up TCP/IP for a firewall

To connect the management client and the SVP through a firewall, configure the firewall so that the TCP/IP port for the protocol you use becomes available.

When attaching Device Manager - Storage Navigator to multiple storage systems, the installer must log in to the SVP of each storage system using separate Device Manager - Storage Navigator sessions and separate web browser instances.

For details about setting up the SVP, see the hardware installation and reference guide for your storage system.

Configuring the web browser

To configure the client web browser, note the following:

- The browser must allow first-party, third-party, and session cookies.
- Pop-up blocker and plug-ins must be disabled.

Consult your browser's documentation for instructions.

⚠ **Caution:** Do not use a modem to connect to the internet because connection speed is too slow.

Configuring Internet Explorer for Device Manager - Storage Navigator

You must set up Internet Explorer on the management client to access Device Manager - Storage Navigator.

Prerequisites

- The management client must be connected to the network via LAN.
- The version of Adobe Flash Player specified in the management client requirements must be installed.

Procedure

1. From the Internet Explorer menu, click **Tools > Internet Options**.
2. Enable cookies.
   a. On the **Privacy** tab, click **Advanced**.
   b. In the **Advanced Privacy Settings** window, specify the following:
      - Select **Override automatic cookie handling**.
      - For **First-party Cookies**, select **Accept**.
      - For **Third-party Cookies**, select **Accept**.
      - Select **Always allow session cookies**.

   c. Click **OK** to close the **Advanced Privacy Settings** window.
3. Allow pop-up windows.

   For Internet Explorer 10:

   a. On the **Privacy** tab, clear the check box for **Turn on Pop-up Blocker**, and then click **Close**.

   For other versions of Internet Explorer:

   a. On the **Privacy** tab, click **Pop-up Blocker Settings**.
   b. In **Address of website to allow**, enter the IP address or host name of the SVP, click **Add**, and then click **Close**.
4. Click **OK** to close the **Internet Options** window.
5. If any third-party add-ons block pop-up windows, configure them to allow pop-ups.

Configuring Firefox for Device Manager - Storage Navigator

You must set up Firefox on the management client to access Device Manager - Storage Navigator.

Prerequisites

- The management client must be connected to the network via LAN.
- The version of Adobe Flash Player specified in the management client requirements must be installed.

Procedure

1. From the menu, click **Tools > Options**.
2. Enable cookies.
   a. On the **Privacy** tab, select **History > Firefox will > Use custom settings for history**.
   b. Specify the following:
      - Select **Accept cookies from sites**.
      - For **Accept third-party cookies**, select **From visited**.
3. Allow pop-up windows.
   a. On the **Privacy** tab, click **Pop-ups > Exceptions**.
   b. Enter the IP address or host name of the SVP, and then click **Allow**.
   c. If any third-party add-ons block pop-up windows, configure them to allow pop-ups.

Installing Adobe Flash Player

Adobe Flash Player must be installed on the management client.

To install the latest Adobe Flash Player, download the installer from http://get.adobe.com/flashplayer/.

To install earlier versions, search for "Archived Flash Player versions" on the Adobe Systems Incorporated website.

Note:
- There are two versions of Windows Flash Player: ActiveX for Internet Explorer and Plugin for other than Internet Explorer. Choose the Flash Player installer that is appropriate for your browser.
- Adobe Flash Player might be installed with Internet Explorer. If so, you can perform Windows Update to install the latest version.
- You can also download an earlier version from Microsoft Security Advisory (2755801).

Procedure

1. Launch the web browser that you normally use and go to the Adobe website http://www.adobe.com.
2. Scroll upward as needed to display the top of the Adobe web page.
3. In the Adobe search box in the upper right corner of the web page (not the browser search box) enter **archived Adobe Flash Player** and click **Search**.
4. In the search results, select **Archived Adobe Flash Player versions.** The Archived Adobe Flash Player version web page on the Adobe website opens.
5. Scroll down to the list of archived Adobe Flash Player versions, select the archived version you want, download the installer, and then run it.

Logging in to Device Manager - Storage Navigator

There are two types of logins to Device Manager - Storage Navigator:

- One-time only initial login by the administrator or super-user who logs in first to create other user accounts
- Normal login allows users to perform only tasks related to initial settings such as account management or software application management. When the initial settings are complete, use Hitachi Command Suite to configure the storage system.

Initial super-user login

This login procedure is for the super-user who logs into Device Manager - Storage Navigator for the first time and sets up the user accounts. The super-user has a built-in ID which includes all permissions, and a default password.

Procedure

1. Call your local service representative to obtain the super-user ID and default password.
2. In your web browser, specify the URL for your SVP:

   `https://`*`IP-address-or-host-name-of-SVP`*`/sanproject/`

   To change the port number of the protocol from the initial value (443), specify the following URL:

   `https://`*`IP-address-or-host-name-of-SVP`*`:`*`port-number-of-the-protocol`*`/`
3. Log in with the superuser ID and password.
4. To prevent unauthorized use of the superuser account, change the password immediately after you log in. Click **Settings > User Management > Change Password** to change your password.

Normal login

Normal login allows you to perform only the following:

- User management
- License management
- Creating a login message
- Editing advanced system settings

When the initial settings are complete, use Hitachi Command Suite to configure the storage system.

Procedure

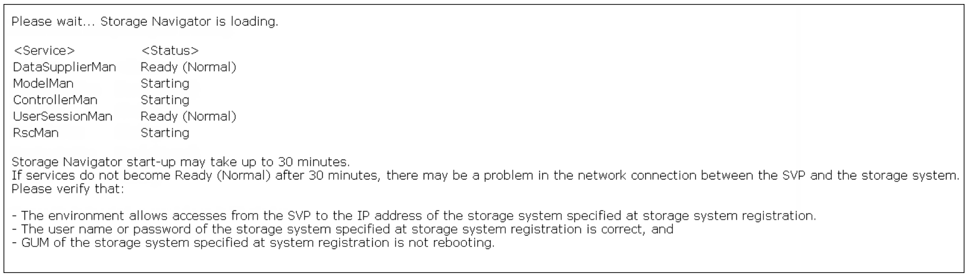
1. In your web browser, specify the following URL:

   `https://`*`IP-address-or-host-name-of-SVP`*

   If you changed the port number of the protocol HTTP from the initial value (443), specify the following URL:

   `https://`*`IP-address-or-host-name-of-SVP`*`:`*`port-number-of-the-protocol-HTTPS`*`/`

   If the loading window displays in Device Manager - Storage Navigator, wait until the service status changes to **Ready (Normal)**. At that time, the login window displays automatically. The following is an example of the loading window.

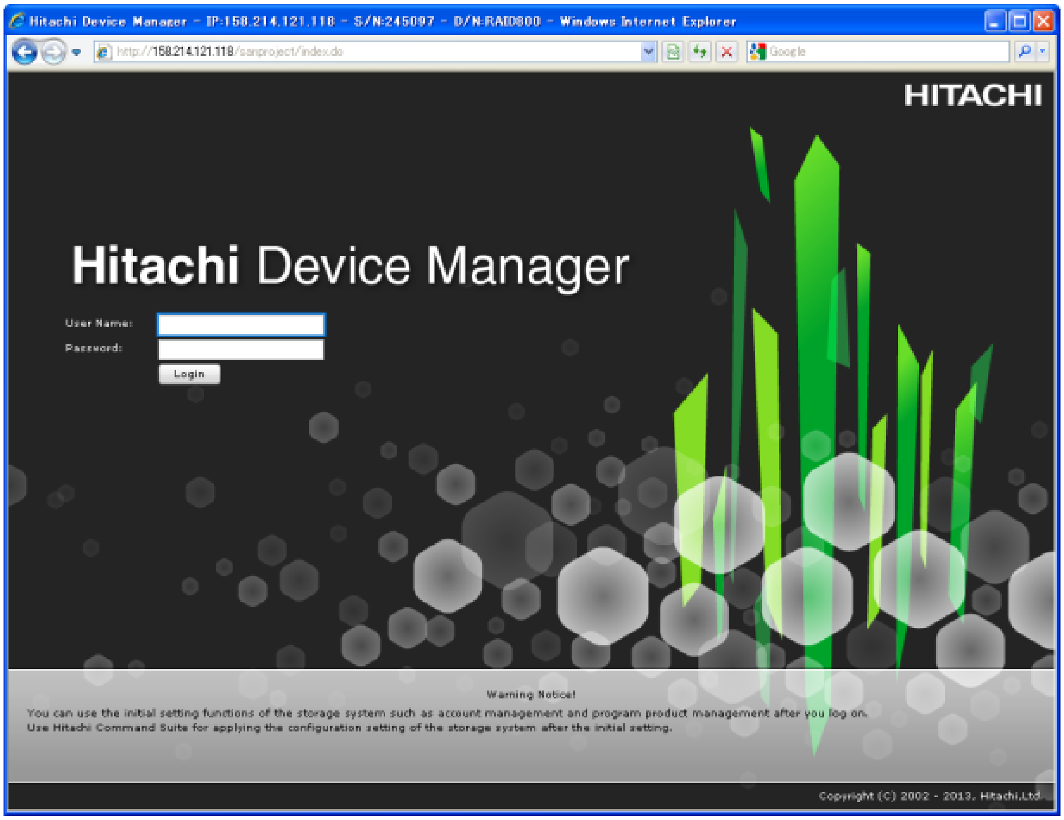


```
Please wait... Storage Navigator is loading.

<Service>          <Status>
DataSupplierMan    Ready (Normal)
ModelMan           Starting
ControllerMan      Starting
UserSessionMan     Ready (Normal)
RscMan             Starting

Storage Navigator start-up may take up to 30 minutes.
If services do not become Ready (Normal) after 30 minutes, there may be a problem in the network connection between the SVP and the storage system.
Please verify that:

- The environment allows accesses from the SVP to the IP address of the storage system specified at storage system registration.
- The user name or password of the storage system specified at storage system registration is correct, and
- GUM of the storage system specified at system registration is not rebooting.
```


Hitachi Device Manager - IP:158.214.121.118 - S/N:245097 - D/N:RAID800 - Windows Internet Explorer
http://158.214.121.118/sanproject/index.do
Google
HITACHI
Hitachi Device Manager
User Name:
Password:
Login

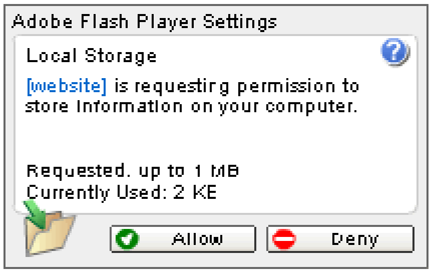
Warning Notice!

You can use the initial setting functions of the storage system such as account management and program product management after you log on.
Use Hitachi Command Suite for applying the configuration setting of the storage system after the initial setting.

Copyright (C) 2002 - 2013, Hitachi,Ltd.

2. The following actions might be required to open the login dialog box, depending on your environment:
   - If a message indicates that the enhanced security configuration is enabled on the management client, select **In the future, do not show this message** and click **OK**.
   - If the SVP is set to support SSL-encrypted communication and security messages appear, make sure the certificate is correct and follow the instructions in the dialog box.
   - If a message indicates that certain web sites are blocked, follow instructions in Adding your SVP to the trusted sites zone for Windows server on page 32.
3. Type the user ID and password.
4. Click **Login**.
5. If the **Security Information** dialog box appears, click **Yes**.

6. If a local storage area pop-up dialog box of Adobe Flash Player Setting appears, click **Allow** to open the Device Manager - Storage Navigator main window. The cache function of Adobe Flash Player optimizes the process of Device Manager - Storage Navigator. Denial of the request might delay the processing speed of Device Manager - Storage Navigator.



Adobe Flash Player Settings

Local Storage

[website] is requesting permission to store information on your computer.

Requested: up to 1 MB
Currently Used: 2 KB

> **Note:** The roles and resource groups for each user are set up ahead of time and will be available to you when you log in to Device Manager - Storage Navigator. If the roles or resource allocations for your username are changed after you log in, the changes will not be effective until you log out and log back in again.

> **Note:** If login fails three times with the same user ID, Device Manager - Storage Navigator stops responding for one minute. This is for security purposes and is not a system failure. Wait, then try again.

Changing your password

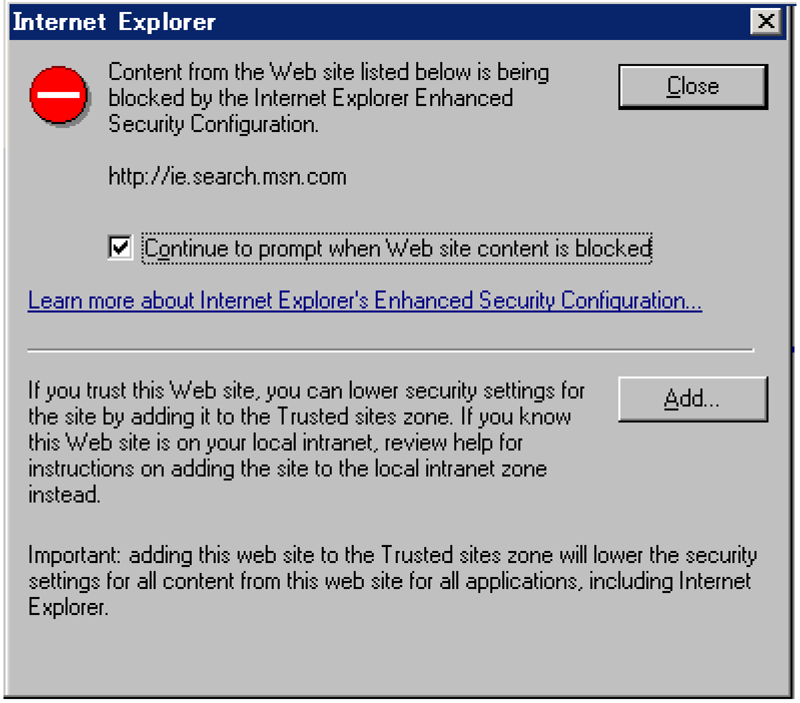
After the administrator gives you a user ID and password, you should change the password.

Procedure

1. Log in to Device Manager - Storage Navigator with the user ID and password given to you by the administrator.
2. Click **Settings > User Management > Change Password** to change your password.

Adding your SVP to the trusted sites zone for Windows server

If you are using Device Manager - Storage Navigator on a Windows Server 2003/2008 computer, the following message may appear during login. If it does, you must add the SVP to the trusted sites zone.



Internet Explorer

Content from the Web site listed below is being blocked by the Internet Explorer Enhanced Security Configuration.

http://ie.search.msn.com

☑ Continue to prompt when Web site content is blocked

Learn more about Internet Explorer's Enhanced Security Configuration...

If you trust this Web site, you can lower security settings for the site by adding it to the Trusted sites zone. If you know this Web site is on your local intranet, review help for instructions on adding the site to the local intranet zone instead.

Important: adding this web site to the Trusted sites zone will lower the security settings for all content from this web site for all applications, including Internet Explorer.

Procedure

1. Click **Add** in the message dialog box. The **Trusted Sites** dialog box opens.
2. In **Add this web site to the zone**, enter the URL of the SVP that you want to log in to. For example, if the host name is `host01`, the URL is `http://host01`. If the IP address is `127.0.0.1`, the URL is `http://127.0.0.1`.
3. Click **Add** to add the URL of the SVP to the **web sites** list.
4. Click **Close** to close the dialog box.

Changing the date and time

To keep the date and time on the storage system controller and the SVP in sync, you must change the date and time settings on both. This section includes procedures to change both settings.

Changing the controller clock settings

Complete the following steps to change the date and time on the storage system controller.

Prerequisites

- You must have the Storage Administrator (View & Modify) role to perform this task.

Procedure

1. In the maintenance utility **Administration** tree, select **Date & Time**.

   The current settings are displayed.
2. Click **Set Up**.
3. Change the settings as needed, and either click **Apply** to save them, or click **Cancel** to close the window without saving the changes.

Changing the SVP clock settings

Complete the following steps to change the Windows 7 date and time on the SVP.

Prerequisites

- The management console is connected to the LAN 2 port on the SVP.
- The console has established a remote desktop connection with the SVP.
- The management utility window is displayed on the console.

On the management console that is connected to the SVP:

Procedure

1. On the Windows 7 desktop, click **Start > Control Panel**.
2. Click **Clock, Language, and Region.**
3. Click **Date and Time.**
4. Click **Change date and time.** The Date and Time Settings window opens.
5. Set the date and time, then click **OK** to save the settings and close the window.

Changing network settings

This section explains how to change the IPv4 and IP6 settings on the SVP to match the settings on the storage system, and how to change network permissions.

Setting up TCP/IP for a firewall

To connect the management client and the SVP through a firewall, configure the firewall so that the TCP/IP port for the protocol you use becomes available.

When attaching Device Manager - Storage Navigator to multiple storage systems, the installer must log in to the SVP of each storage system using separate Device Manager - Storage Navigator sessions and separate web browser instances.

For details about setting up the SVP, see the hardware installation and reference guide for your storage system.

Enabling IPv6 communication

You should assign the SVP the same type of IP addresses (IPv4 or IPv6) that are used on the storage system. You must also configure the client computers with the same IP version that you assign to the SVP. In addition, use the same communication options for both the management client and the SVP.

If you use IPv6 to display the Device Manager - Storage Navigator main window when both IPv4 and IPv6 are available, IPv6 addresses are displayed in the Device Manager - Storage Navigator secondary window but IPv4 communication is actually used.

The following topics provide brief instructions on configuring IPv6 communication.

Changing network communication settings

This procedure explains how to configure a management client to use IPv6 for communication with a service processor.

Procedure

1. In the maintenance utility, click **Administration** to expand the **Administration** navigation pane.
2. Click **Network Settings**.

   The **Network Settings** window displays the current network settings and permissions.
3. In the **Network Settings** window, click **Set Up Network Settings**.

   The **Network Settings** dialog box displays the current settings for the Mac address, IPv4 and IPv6 settings, and the network connection mode for both controllers 1 and 2. It also displays the current settings for the maintenance port and the storage system internal network.
4. Change the settings as needed and click **Apply**.

   The dialog box closes and returns you to the **Network Settings** window.

Changing network permissions

This procedure explains how to block or allow HTTP blocking.

Procedure

1. In the maintenance utility, click **Administration** to expand the **Administration** navigation pane.
2. Click **Network Settings**. The **Network Settings** window displays the current network settings and permissions.
3. In the **Network Settings** window, click **Set Up Network Permissions**.
4. To enable HTTP blocking, click **Enable**. To disable HTTP blocking, click **Disable.**
5. Click **Apply**. The dialog box closes and returns you to the **Network Settings** window.

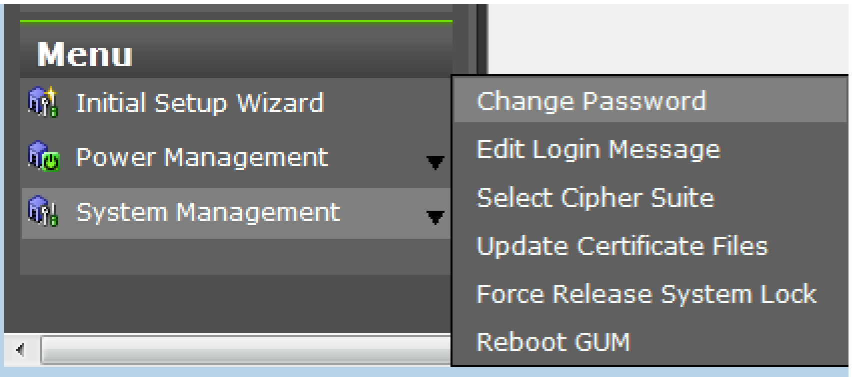
Changing the administrator password

Prerequisites

- You must have the Storage Administrator (View & Modify) role to complete this procedure.

Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Change Password**.
3. Enter your current password and a new password. Enter the password again in the **Re-enter Password** field.
4. Click **Finish**.

Creating a login message

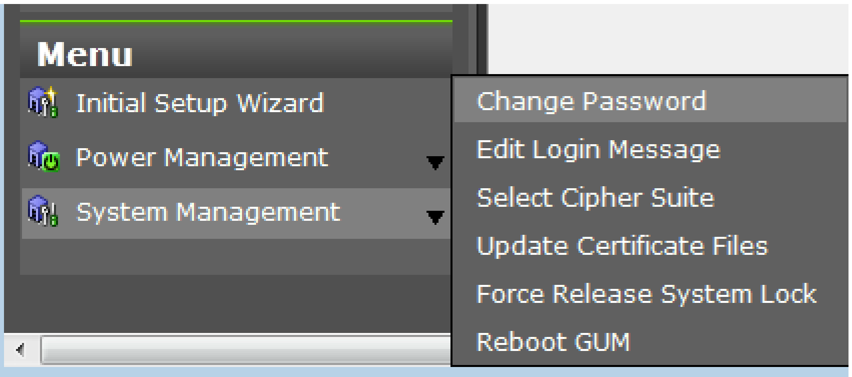
When users log in to the maintenance utility, they will see a login message if one has been written. You can use the login banner message to inform users of specific system conditions, user requirements, or to provide other information that users may need to manage the system.

Prerequisites

You must have the Storage Administrator (View & Modify) role to complete this procedure.

Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Edit Login Message**.
3. Enter a message to be displayed at the time of login. The message can contain up to 2,048 characters. A line break is counted as one character.
4. Click **Apply** to save the message and close the dialog box.

Selecting a cipher suite

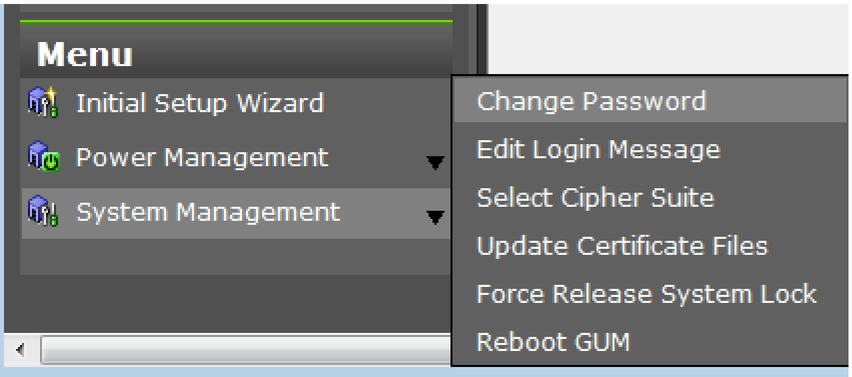
Cipher suites are part of SSL Version 3 and OSI Transport Layer Security Version 1 Cipher Specifications.

Prerequisites

You must have the Storage Administrator (View & Modify) role to complete this procedure.

Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Select Cipher Suite**.
3. Select the type of communication to use between the SVP and the storage system. The selections change the encryption level. Higher encryption provides better security but the communication speed is slower.
   - TLS_RSA_WITH_AES_128_CBC_SHA (Prioritize Transmission Speed). This selection provides higher communication speed and lower security.
   - TLS_RSA_WITH_AES_128_CBC_SHA256 (Prioritize Security). This selection provides higher security and lower communication speed.
4. Click **Apply** to save the setting and close the dialog box.

Updating the certificate files

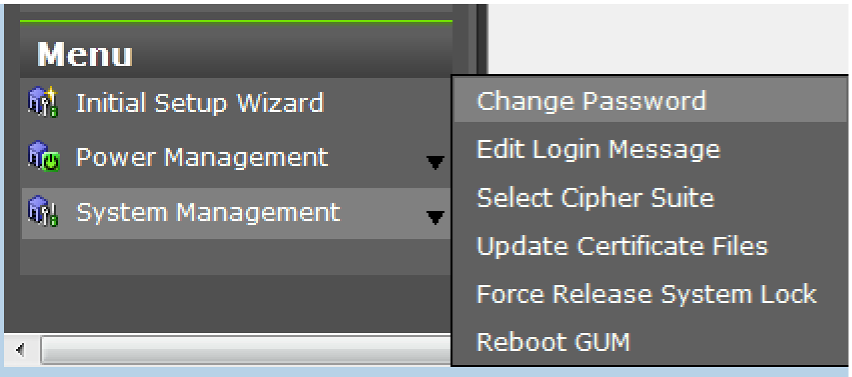
The **Update Certificate Files** window is used to update the certificates that are used for communication between the SVP and the storage system.

Prerequisites

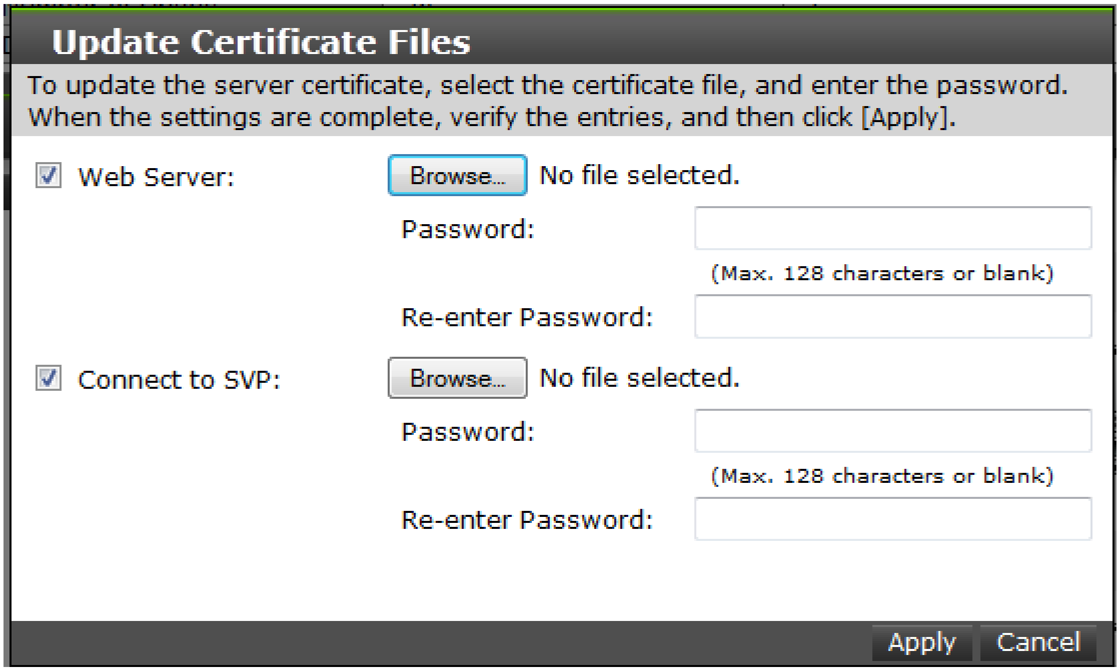
- You must have the Storage Administrator (View & Modify) role to complete this procedure.

Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Update Certificate Files**.
3. Select a Web Server certificate file to update. Click the **Web Server** checkbox, then click **Browse.**



Update Certificate Files

To update the server certificate, select the certificate file, and enter the password. When the settings are complete, verify the entries, and then click [Apply].

☑ Web Server: Browse... No file selected.

Password:

(Max. 128 characters or blank)

Re-enter Password:

☑ Connect to SVP: Browse... No file selected.

Password:

(Max. 128 characters or blank)

Re-enter Password:

4. Browse to the certificate file and click **Open**. The **File Upload** window closes and returns you to the **Update Certificate Files** dialog box.
5. In the Web Server **Password:** field, enter the certificate password.
6. Enter the password again in the Web Server **Re-enter Password:** field.
7. Select a Connect to SVP certificate file to update. Click the **Connect to SVP** checkbox, then click **Browse**.
8. Browse to the certificate file and click **Open**. The **File Upload** window closes and returns you to the **Update Certificate Files** dialog box.
9. In the Connect to SVP **Password:** field, enter the certificate password.
10. Enter the password again in the Connect to SVP **Re-enter Password:** field.

11. Click **Apply** to update the certificates.

Forcing the system lock to release

When a user locks the system, other users cannot log in or access the system. This feature can be used to ensure that no changes to the system can be made while maintenance or upgrade procedures are in process.

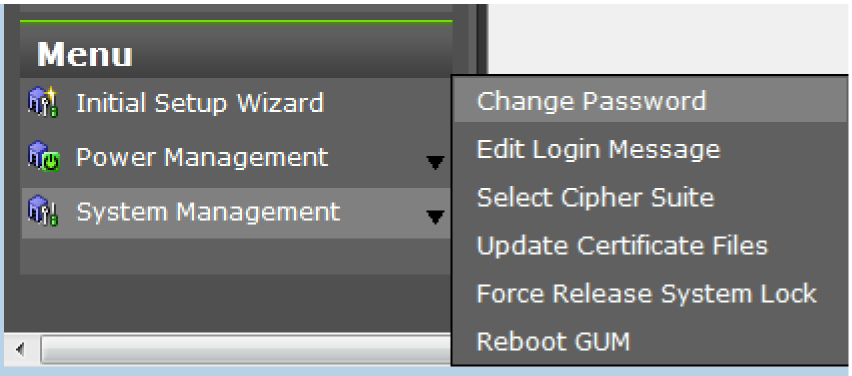
Caution: Before using this feature, ensure that releasing the system lock will not cause system problems due to processes that are currently running. Releasing the system lock can terminate a process before it completes and possibly leave the system in an unknown state. Check with any users that are logged on. Wait until their processes are complete before releasing the system lock.

Prerequisites

You must have the Storage Administrator (View & Modify) role to complete this procedure.

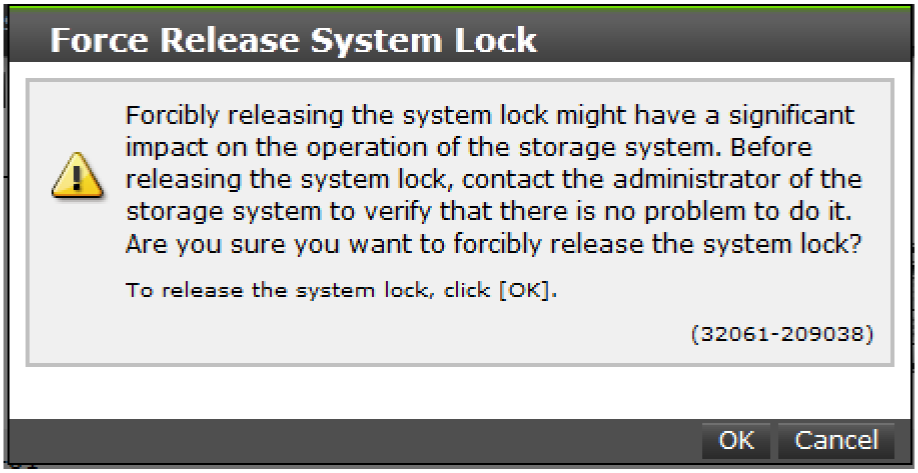
Procedure

1. In the maintenance utility **Menu** navigation tree, click **System Management**.



2. Click **Force Release System Lock**.

3. A warning message is displayed in the dialog box. Verify that releasing the lock will not cause data loss or other problems. To release the system lock, click **OK**. Click **Cancel** to close the dialog box without releasing the system lock.



Force Release System Lock

Forcibly releasing the system lock might have a significant impact on the operation of the storage system. Before releasing the system lock, contact the administrator of the storage system to verify that there is no problem to do it. Are you sure you want to forcibly release the system lock?

To release the system lock, click [OK].

(32061-209038)

Setting storage system information

You can set the name, contact information, and location of the storage system.

Caution: When changing a setting more than once, ensure that the current setting is complete before changing it again. Otherwise, only the new change will be applied, and the result might be different from what you expected.

Procedure

1. In the Device Manager - Storage Navigator **Storage System** tree, select the storage system.
2. From **Settings**, click **Environmental Settings > Edit Storage System**.
3. Enter the items that you want to set.

   You can enter up to 180 alphanumeric characters (ASCII codes) excluding several symbols (\ , / ; : * ? " < > | & % ^). Do not use a space at the beginning or the end.
4. Click **Finish**.
5. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
6. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens to show the status of the task.

Registering the primary SVP host name

You must register the primary SVP host name before completing any of the following tasks.

- Specify a host name instead of an IP address when accessing Device Manager - Storage Navigator.
- Obtain the public key certificate for SSL-encrypted communication from the CA (Certificate Authority). You must register the server name as the host name to the DNS server or the hosts file. The server name is entered in the certificate as a common name.

  Enter the SVP host name and IP address in the DNS server or the hosts file of the management client. You can register any host name to the DNS server or the hosts file, but there are restrictions on the letters you can use for the host name.
- **DNS setting:** You must register the IP address and host name of the SVP to the DNS server that manages the network to which the SVP is connected.
- **Hosts file setting:** You must enter the IP address and host name of the SVP to the hosts file of the management client. The general directory of the hosts file is:
  - **Windows 7:** `C:\Windows\System32\drivers\etc\hosts`
  - **UNIX:** `/etc/hosts`

Report configuration tool

Complete the following instructions to install the report configuration tool.

Prerequisites for the report configuration tool

You need the following items to install the report configuration tool:

- A Windows computer running Windows Server 2000, Windows Server 2003, or Windows Server 2008.

  You can use either an IPv4 address or an IPv6 address to connect the SVP to the Windows computer. You can also connect the management client to the SVP over an IPv4 proxy server. When you use the proxy server, specify a name and a port number of the proxy server as the `HTTP_PROXY` environment variable on the Windows computer. For example:

  ```
  SET HTTP_PROXY=http://proxy.xx.co.jp:8080
  ```
- A user account for exclusive use of the report configuration tool.

  To use the report configuration tool, you must create a user account that is used exclusively for the report configuration tool. Assign the storage administrator role (initial configuration) to this user account.

  For information on user accounts, see Creating user accounts on page 62.

- The report configuration tool installation software
  The Report Configuration Tool is located on the software installation media.

Installing the report configuration tool

Procedure

1. Insert the Report Configuration Tool installation media into a drive.
2. On the media, navigate to the `/program/Config_Report_CLI/Win32` folder and double-click `setup.exe`. Follow the instructions on the screen.
3. When prompted, enter the name of the directory in which to install the report configuration tool. The installer continues until the tool is installed.

Note: The directory where the report configuration tool is installed is not specified as an application path. When necessary, specify the directory as the application path.

Modifying SVP port numbers

You can change SVP port numbers to any arbitrary number. This is optional. You can also initialize the settings to the original status by initializing the port number.

Note: Perform this task only when an SVP port number is duplicated with the number used in another application.

You need to verify the effects before you modify an SVP port number. The table describes the port number key names and the initial value of the port number that you can change.

Port number key name	Protocol	Initial port number	Corresponding SVP software version
MAPPWebServer	HTTP	80	83-01-20-*XX*/00 or later
MAPPWebServerHttps	HTTPS	443	83-01-20-*XX*/00 or later
RMIClassLoader	RMI	51099	83-01-20-*XX*/00 or later
RMIClassLoaderHttps	RMI (SSL)	5443	83-01-20-*XX*/00 or later
RMIIFRegist	RMI	1099	83-01-20-*XX*/00 or later
PreRMIServer	RMI	51100	83-01-20-*XX*/00 or later
DKCManPrivate	RMI	11099	83-01-24-*XX*/00 or later
SLP	SLP	427	83-01-24-*XX*/00 or later
SMIS_CIMOM	SMI-S	5989	83-01-20-*XX*/00 or later
CommonJettyStart	HTTP	8080	83-01-24-*XX*/00 or later
CommonJettyStop	HTTP	8210	83-01-24-*XX*/00 or later

Port number key name	Protocol	Initial port number	Corresponding SVP software version
RestAPIServerStop	HTTP	9210	83-01-24-*XX*/00 or later
DeviceJettyStart	HTTP	8081	83-01-24-*XX*/00 or later
DeviceJettyStop	HTTP	8211	83-01-24-*XX*/00 or later

Changing the SVP port number

You can change the SVP port number to any arbitrary number. After changing the port number, the SVP will be restarted.

Prerequisites

- Remote desktop connection from the management client to SVP has been performed.
- The range of the available port number is from 1 to 65535. Make sure the new port number is not duplicated with the number used in another application.
- You can enter multiple instances of *service-port-number-key-name* and *port-number*. For example:

  ```
  MappSetPortEdit.bat MAPPWebServer 81 MAPPWebServerHttps 444
  ```
- The management file of the SVP port number is stored in the following location:

  ```
  path-to-tool\mpprt\cnf\mappsetportset.properties
  ```

Note:

- Do not change the management file of the port number.
- Close the management file of the port number while executing the command for changing or initializing.
- If the SVP software version of the registered storage system does not support changing the port number, update the SVP software.
- Port numbers 1 to 1023 are reserved for other application programs, so do not use these numbers. If you use these numbers and encounter a problem, change the number to 1024 or higher.
- The following port numbers cannot be used for MAPPWebServer or MAPPWebServerHttps:
  2049, 4045, 6000

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open the Windows command prompt as administrator on the SVP.

3. Move the current directory to the directory where the tool is located (for example, `C:\MAPP\wkSupervisor`). Execute the following command:

   ```
    C:MAPP\wk\Supervisor\MappIniSet\MappSetPortEdit.bat service-
   port-number-key-name port-number
   ```

   ⚠ **Note:**
   - A space is required between `MappSetPortEdit.bat` and *service-port-number-key-name*.
   - A space is required between *service-port-number-key-name* and *port-number*.

4. A service restart message box displays, followed by a completion message box. Press any key to acknowledge the message and close the message box.
5. Close the Windows command prompt.

Initializing the SVP port number

You can initialize the SVP port settings and restore to the original status. After initializing the port number, the SVP will be restarted.

Prerequisites

Remote desktop connection from the management client to SVP has been performed.

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open the Windows command prompt on the SVP.
3. Move the current directory to the directory where the tool is located (for example, `C:\MAPP\wk\Supervisor\MappIniSet`). Execute the following command:

   ```
   C:MAPP\wk\Supervisor\MappIniSet\MappSetPortInit.bat
   ```
4. An initialization confirmation message box displays.

   If you want to continue, enter `Y`, and then press the **Enter** key. If you want to cancel the task, enter `N`, and then press the **Enter** key.
5. A service restart message box displays, followed by a completion message box. Press any key to acknowledge the message and close the message box.
6. Close the Windows command prompt.

Effects of changing SVP port numbers

Set the firewall settings of the management client according to new SVP port numbers.

The following table describes the effects for each port number.

Port number key name	Effects	Referential user guide on changing the SVP port number
MAPPWebServer MAPPWebServerHttps	Changes the method to specify URL for Device Manager - Storage Navigator login	See Logging in to Device Manager - Storage Navigator on page 28.
	In Hitachi Command Suite: You must change the HCS port number to be the same number.	- *Hitachi Command Suite Installation and Configuration Guide*
RMIClassLoader	None	None
RMIClassLoaderHttps	Report Configuration Tool (raidinf command) When you login to Device Manager - Storage Navigator by using raidinf command, you must specify the IP address and new port number of the SVP.	See Report Configuration Tool command reference (raidinf commands) on page 121.
RMIIFRegist	When you execute the Export Tool command, you must specify the IP address and new port number of the SVP for *IP-sub-command*.	*Performance Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models* (Performance Monitor, Server Priority Manager)
	In Hitachi Command Suite: You must change the HCS port number to the same number.	- *Hitachi Command Suite Installation and Configuration Guide*
PreRMIServer	None	None
DKCManPrivate	None	None
SLP	You must change the SMI-S port number to the same number.	*Hardware Reference Guide* for your storage system
SMIS_CIMOM	You must change the SMI-S port number to the same number.	*Hardware Reference Guide* for your storage system
CommonJettyStart	None	None
CommonJettyStop	None	None
RestAPIServerStop	None	None
DeviceJettyStart	None	None
DeviceJettyStop	None	None

Using the report configuration tool

You can use the report configuration tool to create up to 20 configuration reports and then view or download them.

Creating a configuration report on page 119 describes how to create a configuration report. The list of commands for creating reports is located in

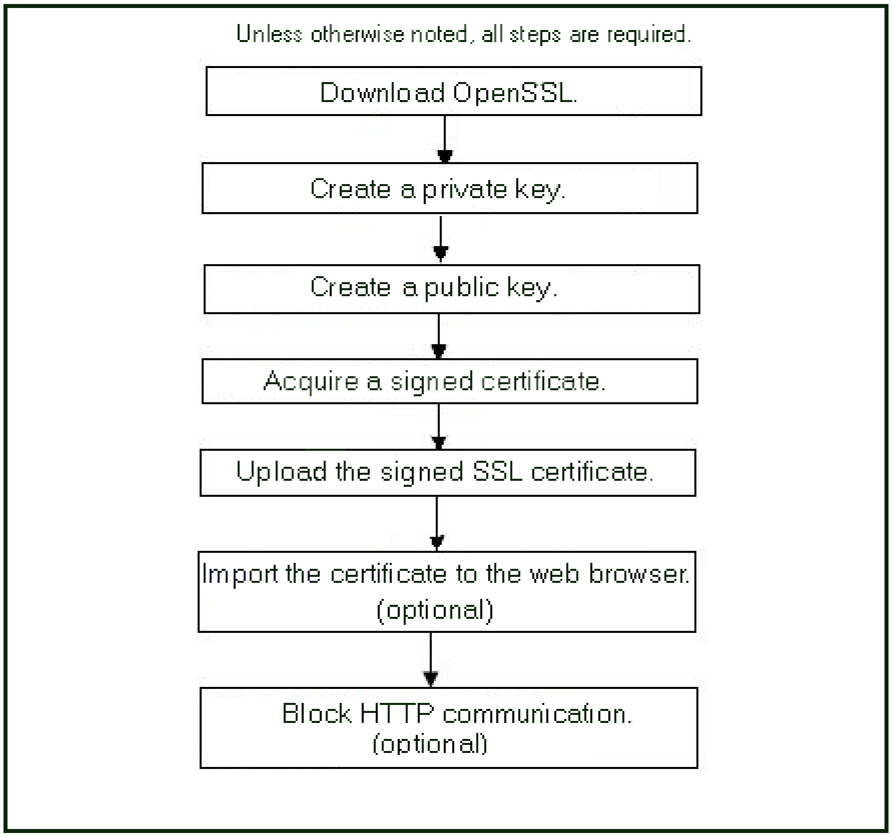
Report Configuration Tool command reference (raidinf commands) on page 121.

Managing SSL certificates

To improve the security of remote operations from a Device Manager - Storage Navigator service processor to a storage system, you can set up Secure Sockets Layer (SSL) encrypted communication. By setting SSL encryption, the Device Manager - Storage Navigator User ID and Password are encrypted.

Flow of SSL communication settings

The following illustration shows the procedure to set up SSL communication. Unless otherwise noted, all steps are required. Note that creation of private and public keys requires a dedicated program. Download one from the OpenSSL website (http://www.openssl.org/).


Unless otherwise noted, all steps are required.
Download OpenSSL.
Create a private key.
Create a public key.
Acquire a signed certificate.
Upload the signed SSL certificate.
Import the certificate to the web browser. (optional)
Block HTTP communication. (optional)

Creating a keypair

To enable SSL, you must create a keypair consisting of a public and a private key. The instructions use Windows 7 as an example.

Creating a private key

A private key is required to create an SSL keypair. The following procedure for Windows 7 creates a private key file called `server.key` in the `c:\key` folder.

Prerequisites

Download `openssl.exe` from the OpenSSL website.

Procedure

1. If the read-only attribute is set, release it from the `c:\openssl` folder.
2. Open a command prompt with administrator permissions.
3. Move the current directory to the folder to which the key file is output (such as `c:\key`), and execute the following command:

   ```
   c:\key > c:\openssl\bin\openssl genrsa -out server.key 1024
   ```

Creating a public key

A public key has the file extension `.csr`. It is required to create an SSL keypair. The following procedure is for the Windows 7 operating system.

Prerequisites

Download `openssl.exe` from the OpenSSL website.

Procedure

1. Open a command prompt with administrator permissions.
2. Move the current directory to the folder to which the key file is output (such as `c:\key`). Execute the following command:

   ```
   c:\key > c:\openssl req -sha256 -new -key server.key -config
   c:\openssl\bin\openssl.cfg -out server.csr
   ```

3. Enter the following information in the prompt:
   - Country Name (two-letter code)
   - State or Province Name
   - Locality Name
   - Organization Name
   - Organization Unit Name
   - Common Name
     To create a self-signed certificate, enter the IP address of the web server (SVP). The name you entered here is used as the server name (host name). To obtain a signed and trusted certificate, ensure that the server name is the same as the host name of the SVP.
   - Email Address
   - Challenge password (optional)

- Company name (optional)

Example

The following example shows the contents of a command window when you create a public key.

```
......++++++
..++++++
is 65537 (0x10001)
C:\key>c:\openssl\bin\openssl req -sha256 -new -key server.key -
config c
You are about to be asked to enter information that will be
incorporated into your certificate request. What you are about
to enter is what is called a Distinguished Name or a DN.
\openssl\bin\openssl.cfg -out server.csr
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Kanagawa
Locality Name (eg, city) []:Odawara
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:Hitachi
Organization Unit Name (eg, section) []:ITPD
Common Name (eg, YOUR name) []:192.168.0.1
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

Obtaining a signed certificate

After creating a private key and public key, obtain a signed public key certificate file. You can use any of these methods to obtain a signed certificate file.

- Create a certificate by self-signing. See Obtaining a self-signed certificate on page 49.
- Obtain a certificate from the certificate authority that is used by your company.
- Request an official certificate from an SSL certificate authority. See Obtaining a signed and trusted certificate on page 49.

Note: When you send a request to a certificate authority, specify the SVP as the host name.

Hitachi recommends that self-signed certificates be used only for testing encrypted communication.

Obtaining a self-signed certificate

To obtain a self-signed certificate, open a command prompt and execute the following command:

```
c:\key>c:\openssl\bin\openssl x509 -req -sha256 -days 10000 -in
server.csr -signkey server.key -out server.crt
```

Note: This command uses SHA-256 as a hash algorithm. MD5 or SHA-1 is not recommended for a hash algorithm due to its low security level.

This command creates a `server.crt` file in the `c:\key` folder, which is valid for 10,000 days. This is the signed private key, which is also referred to as a self-signed certificate.

Obtaining a signed and trusted certificate

To obtain a signed and trusted certificate, you must obtain a certificate signing request (CSR), send that file to a Certificate Authority (CA), and request that the CA issue a signed and trusted certificate. Each certificate authority has its own procedures and requirements. Use of this certificate results in higher reliability in exchange for greater cost and requirements. The signed and trusted certificate is the signed public key.

Verifying and releasing an SSL certificate passphrase

An SSL certificate cannot be applied for the SVP if the passphrase is set. If the passphrase is set, release the passphrase for the SSL certificate before applying the SSL certificate to the SVP. The following procedure explains how to verify and release the passphrase settings.

Prerequisites

- A private key (.key file) has been created.
- OpenSSL must be installed. In this procedure, it is installed in `C:\openssl`.

Procedure

1. Open a command prompt window with administrator permissions.
2. Move the current directory to the folder (for example, `C:\key`) where the key file is stored, and run the following command:

   Caution: Executing this command will overwrite the current key file. To prevent loss of the key file, do one of the following:
   - Back up the key file first.
   - Use a different key file input destination and output destination.

   ```
   C:\key>C:\openssl\bin\openssl rsa -in key-file-input-
   destination -out key-file-output-destination
   ```

If `Enter pass phrase for server.key:` is displayed, the passphrase is set. Enter the passphrase. The passphrase in the SSL private key will be released, and the SSL certificate can be applied to the SVP.

Example (when passphrase is set)

```
C:\key>c:\openssl\bin\openssl rsa -in server.key -out server.key

Enter pass phrase for server.key: "Enter passphrase"

Writing RSA key
```

Example (when passphrase is not set)

```
C:\key>c:\openssl\bin\openssl rsa -in server.key –out server.key

Writing RSA key
```

Converting SSL certificates to PKCS#12 format

If you are uploading a created private key and the SSL certificate to GUM, you need to convert it to PKCS#12 format. If you are not uploading SSL certificate to GUM, conversion is not required.

Prerequisites

- You must store a private key and SSL certificate in the same folder.
- In the following procedure:
  - The private key file name is “client.key”.
  - The SSL certificate file name is “client.crt”.
  - The SSL certificate in PKCS#12 format is output to c:\key.

Procedure

1. Open a command prompt with administrator permissions.
2. Enter the following command: `C:key>c:\openssl\bin\openssl pkcs12 -export -in client.crt –inkey client.key -out client.p12`
3. Enter a password, which is used when uploading the SSL certificate in PKCS#12 format to GUM. You can use up to 128 alphanumeric characters and the following symbols: ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
4. The `client.p12` file is created in the `C:\key` folder. This `client.p12` file is the SSL certificate in PKCS#12 format.
5. Close the command prompt.

Updating a signed certificate

To use SSL-encrypted communication, you must update and upload the private key and the signed server certificate (public key) to the SVP.

Prerequisites

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be logged into the SVP.
- A private key (.key file) has been created. Make sure that the file name is `server.key`.
- The passphrase for the private key (server.key file) is released.
- A signed public key certificate (.crt file) has been acquired. Make sure that the file name is `server.crt`.
- The private key (.key file) must be in PEM format. You cannot use DER format.
- The signed public key certificate (.crt file) must be in X509 PEM format. You cannot use X509 DER format.
- The passphrase for the private key (server.key file) must be released.

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. Enter the following command:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet\MappApacheCrtUpdate.bat
   absolute-path-of-signed-public-key-certification-file
   absolute-path-of-private-key-file
   ```

   ⚠ **Note:** A space is required between the signed public key certification file path and the private key file path.

4. A completion message box displays. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

Notes on updating a signed certificate for the service processor

The following notes provide additional information about updating a signed certificate.

- While the service processor certificate is being updated, tasks that are being run or scheduled to run on Device Manager - Storage Navigator are not executed.
- Certificates for RMI communication are updated asynchronously. The process takes about two minutes.
- If the service processor certificate is updated while Hitachi Command Suite is being set up, the setup operation will fail.
- Update of the SSL certificate gives a great influence to the system and may lead to service processor failure. Therefore take sufficient care about the content of the certificate and private key to be set.

- After the certificate update is complete, depending on the environment, the service processor can take 30 to 60 minutes to restart.

Returning the certificate to default

You can return the certificate that was updated by the procedure in Updating a signed certificate on page 50 back to default.

Prerequisites

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be logged into the SVP.
- A private key (.key file) has been created. Make sure that the file name is `server.key`. See Creating a private key on page 47.
- The passphrase for the private key (server.key file) is released.
- A signed public key certificate (.crt file) has been acquired. Make sure that the file name is `server.crt`. See Creating a public key on page 47.
- The private key (.key file) must be in PEM format. You cannot use DER format.
- The signed public key certificate (.crt file) must be in X509 PEM format. You cannot use X509 DER format. See Obtaining a self-signed certificate on page 49.
- The passphrase for the private key (server.key file) must be released.

Procedure

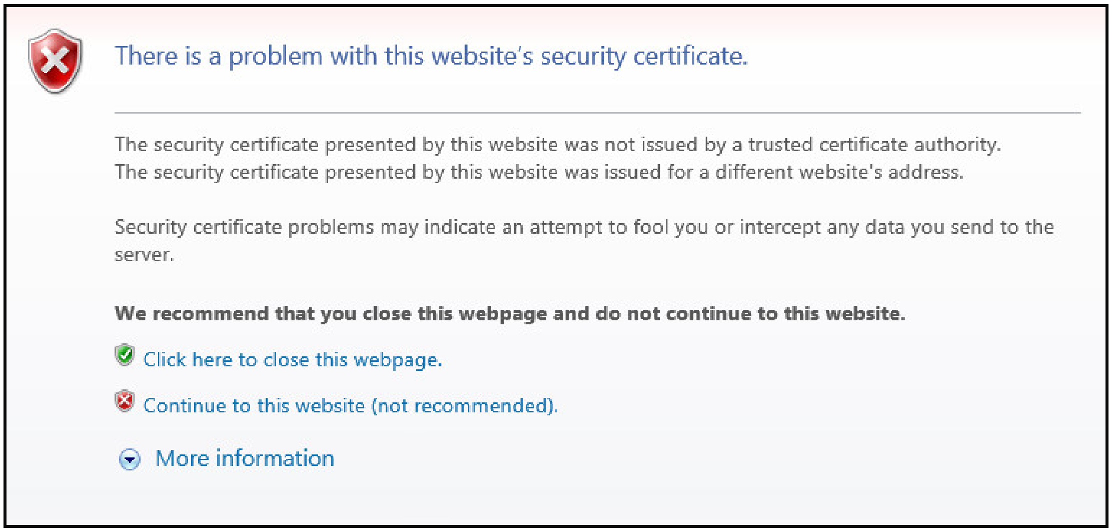
1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. Enter the following command:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet\MappApacheCrtInit.bat
   ```
4. A completion message box displays. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

Problems with website security certificates

When the message "There is a problem with this website's security certificate." is displayed, click **Continue to this website (not recommended)**.

If the security certificate is not issued by a trusted certificate authority, the browser displays a warning message when it connects to an SSL-enabled Device Manager - Storage Navigator.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

Managing HCS certificates

This topic explains how to set or delete certificates for Hitachi Command Suite (HCS) that are used to check the server's reliability when SSL communication for HCS external authentication is performed.

Registering HCS certificates

To check the server reliability during SSL communication for HCS external authentication, upload an HCS public key certificate to the web server to register the certificate. Complete the steps in the following procedure to upload and register a certificate using the certificate update tool.

Note: Ensure that you register or delete the correct certificate. Otherwise, HCS external authentication will not return.

Prerequisites

- You must be logged into the SVP.
- The private key file on the HCS server must be current. Update it if necessary.
- The certificate file must have a .crt extension. Rename the file if necessary.
- The certificate must be in X509 PEM format or X509 DER format.

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. Enter the following command:

```
C:\MAPP\wk\Supervisor\MappIniSet\MappHcsCrtEntry.bat
absolute-path-of-signed-public-key-certificate-file
```

4. A completion message box displays. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

Deleting HCS certificates

You can delete the certificates you registered in the procedure of the "Registering certificates for HCS" section. After you delete a certificate, server reliability for that certificate is not checked by SSL communication for HCS external authentication.

Prerequisites

- You must be logged into the SVP.
- The private HCS server key must be updated.
- The certificate file must have a .crt extension. Rename the file if necessary.
- The certificate must be in X509 PEM format or X509 DER format.

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. Enter the following command:
   ```
   C:\MAPP\wk\Supervisor\MappIniSet\MappHcsCrtDelete.bat
   ```
4. A completion message box opens. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

Blocking HTTP communication to the SVP

If the web server supports SSL (HTTPS), you can use the HTTP setting tool to block or allow access to HTTP communication port, as needed.

Prerequisites

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be logged into the SVP.

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. Enter the following command:
   ```
   C:\MAPP\wk\Supervisor\MappIniSet\MappHttpBlock.bat
   ```
4. A completion message box displays. Press any key to acknowledge the message and close the message box.

5. Close the command prompt window.

Releasing HTTP communication blocking

If the web server supports SSL (HTTPS), you can use the HTTP setting tool to release a block to HTTP communication port, as needed.

Prerequisites

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be logged into the SVP.

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a command prompt window with administrator permissions.
3. Enter the following command:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet\MappHttpRelease.bat
   ```
4. A completion message box displays. Press any key to acknowledge the message and close the message box.
5. Close the command prompt window.

Backing up HDvM - SN configuration files

Before replacing an SVP, you must make a backup copy of the Device Manager - Storage Navigator configuration files on the SVP. You can then use the backup copy to restore the configuration file if it becomes necessary, or to configure a replacement SVP if one fails.

To back up the Device Manager - Storage Navigator configuration files on the SVP, download them to a folder that you specify.

The following configuration items can be backed up and restored. Before you create the backup, ensure that the settings are correct.

- Device Manager - Storage Navigator environment parameters
- Authentication server connection settings
- Key management server connection settings
- Password policy when backing up the management client encryption key
- Display settings (table width) for each Device Manager - Storage Navigator user
- Device Manager - Storage Navigator login warning messages
- Device Manager - Storage Navigator task information
- SMI-S application settings
- SSL certification for HTTPS/SMI-S/RMI

Prerequisites

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be logged into the SVP.

Procedure

1. Close all Device Manager - Storage Navigator sessions.
2. Open a command prompt window with administrator permissions.
3. Enter the following command:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet\MappBackup.bat absolute-path-of-backup-file
   ```

   Note:
   - The backup file must be in .tgz format.
   - A space is required between `MappBackup.bat` and the path to the backup file.

4. A completion message displays. Click any key to continue.
5. Close the command prompt window.

   Tip:
   - If you do not specify a folder in which to save the file, the system automatically creates a default file in the following location:

     ```
     SVP-root\wk\Supervisor\MappIniset
     \LogsyyyyMMddHHmmss.tgz
     ```

     where *yyyyMMddHHmmss* is the year, month, date, and time that the file was created.
   - The backup file is compressed and uses the .tgz format. Use a tool that supports tar and gzip to extract the data from the .tgz file.

6. Save the backup file to another computer or external memory device such as a USB flash memory or hard drive.

Related tasks

- Restoring HDvM - SN configuration files on page 56

Restoring HDvM - SN configuration files

You can use a saved copy of a configuration file to restore the active configuration file if it becomes necessary, or to configure a replacement SVP if one fails.

Prerequisites

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must be logged into the SVP.
- The SVP is configured so that the service does not start automatically when starting the system. See the Hardware Reference Guide for your storage system model for information about the SVP configuration method.

Procedure

1. Close all Device Manager - Storage Navigator sessions.
2. Open a command prompt window with administrator permissions.
3. Enter the following command:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet\MappRestore.bat absolute-path-of-backup-file
   ```

   ⚠ **Note:**
   - The backup file must be in .tgz format.
   - A space is required between `MappRestore.bat` and the path to the backup file.

   ---

4. A completion message displays. Click any key to continue.
5. Close the command prompt window.
6. Set the service to run automatically when starting the SVP. Then reboot the SVP.

Related tasks

- Backing up HDvM - SN configuration files on page 55

3

User administration

This section describes various user roles, permissions and groups available to manage your storage system. You can use the management software to create and manage user accounts on your storage system.

User administration overview

Read and understand the following information before managing users or user groups.

- When a user is assigned to multiple user groups, the user has the permissions of all the roles in each user group that are enabled on the resource groups assigned to each user group.
- If a user has All Resource Groups Assigned set to Yes, the user can access all the resources in the storage system. For example, if a user is a security administrator and a storage administrator and has all resource groups assigned, the user can edit the storage for all the resources.

  If this is an issue, the recommended solution is to register the two user accounts in the storage system and use the two accounts for different purposes.
  - A security administrator user account that has All Resource Groups Assigned set to Yes.
  - A storage administrator user account that has only some of the resource groups assigned.
- For the user groups whose roles are other than the Storage Administrator, All Resource Groups Assigned is automatically set to Yes. If you delete all the roles except the Storage Administrator, reassign resource groups to the user group because All Resource Groups Assigned is automatically set to No.

Related tasks

- Changing assigned resource groups on page 73

Workflow for creating and managing user accounts

Administrators use Device Manager - Storage Navigator to create accounts for all users. The following steps show a basic workflow:

- If an authentication server is used, connect the management clients to it. An authentication server allows users to log in to Device Manager - Storage Navigator with the same password as the one used for other applications in a system.
- If an authentication server is not used, use a password dedicated to Device Manager - Storage Navigator to log in. Whether to use the authentication server can be specified for each user.
- Review Using an authentication server and authorization server on page 74 for information and instructions.

- Review Managing user groups on page 67 to understand the user groups and roles you can assign new or existing users.
- Create user accounts and assign permissions. See Creating user accounts on page 62.
- Change, disable, or delete user passwords and permissions. See Changing user passwords on page 63.

Administrator tasks

To authenticate a user using an authentication server, specify settings for connecting to the server.

Note: When an administrator changes a support person's user account, he or she must notify the user. Otherwise, the user will not be able to log in.

Procedure

1. Log in to Device Manager - Storage Navigator as a built-in user.

   Use `maintenance` as the user name, and `raid-maintenance` as the password. The built-in user has all permissions.
2. Click **Settings > User Management > Change Password** to change the password of the built-in user account.
3. Create a user group. Some user groups, such as built-in groups, are available by default.
4. Create a user.
5. If necessary, change the environment parameter.
6. Save the user account information and environment parameter file.
7. Notify the user of the new user name and the password.

User tasks

Procedure

1. Use the user name and password provided by the administrator to log in to Device Manager - Storage Navigator.
2. Click **Settings > User Management > Change Password** to change the password to your own password.

Managing user accounts

This process describes how to create and manage local administrator accounts in the storage system. You will need to use the local administrator account created during the initial setup step, or create administrator accounts using the procedures described in this chapter as needed to temporarily access the storage system, when the management software is not available.

It is prudent to create more than one user account in case the system administrator is not available when the management software becomes unavailable, and someone else needs to access the system. This is also helpful if multiple users need to access Device Manager - Storage Navigator to use storage features that are not available in the management software.

Related tasks

- Creating user accounts on page 62
- Changing user passwords on page 63
- Changing user permissions on page 64
- Disabling user accounts on page 65
- Deleting user accounts on page 66

Creating user accounts

This section explains how to create a user account and register the account to a user group with appropriate permissions.

Prerequisites

- You must have the Security Administrator (View & Modify) role to perform this task.
- You or an authorized technical support representative can log in to Device Manager - Storage Navigator and CCI with user accounts that are created in Device Manager - Storage Navigator.
- Support representatives must have the Support Personnel (Vendor Only) role to log in.
- The system can support a maximum of 20 user accounts, including the built-in user accounts.

Table 2 User name and password for Device Manager - Storage Navigator

Item	Length in characters	Characters that can be used
User name	1-256	• Alphanumeric characters • The following symbols: # $ % & ' * + - . / = ? @ ^ _ ` { | } ~
Password	6-256	• Alphanumeric characters • All symbols

Table 3 User name and password for logging in to CCI

Item	Length in characters	Characters that can be used
User name	1-63	• Alphanumeric characters • The following symbols:[1]

Item	Length in characters	Characters that can be used
		- . @ _
Password	6-63	• Alphanumeric characters • The following symbols:[1] - . @ _

Note:

1. When you use a Windows computer, you can also specify a backslash (\). When you use a UNIX computer, you can also specify a slash (/).

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, select a user group to which to add a user. This is dependent on which permissions you want to give to the user.
3. On the **Roles** tab, confirm that the displayed permissions are appropriate for the user.
4. On the **Users** tab, click **Create User**.
5. Enter a name.
6. Select **Activate** or **Lock** for the account. If you select **Lock**, the user of this account is disabled and cannot log in to Device Manager - Storage Navigator.
7. To use an authentication server, select **External**. To authenticate users with only Device Manager - Storage Navigator, select **Local**.
8. If you select **Local**, enter the password for this user account in two places.

   For a password, all alphanumeric characters and symbols can be used. The length must be between 6 and 256.
9. Click **Finish**.
10. In the **Confirm** window, check the settings.
11. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens to display the status of the task.

Changing user passwords

This section explains how to change or re-issue passwords for other users on Device Manager - Storage Navigator.

Caution: Do not select any user account used to connect to a storage system that is registered in the **Storage Device List** window. For details, see the Hardware Reference Guide for your storage system.

Prerequisites

- Security administrators with View & Modify roles can change user passwords on Device Manager - Storage Navigator.
- If the target user has a local user account for Device Manager - Storage Navigator, the security administrator can use Device Manager - Storage Navigator to change the target user's password.
- If the target user has a local user account for the authentication server, the security administrator can use the authentication server to change the target user's password. After the password is changed, the target user can use the new password on both the authentication server and Device Manager - Storage Navigator.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, select the user group to which the user belongs.
3. On the **User** tab, select the user whose password you want to change.
4. In the **User** tab, click **Change Password**.
5. In the **Change Password** dialog box, specify a new password for the user in the two password fields.
6. Click **Finish**.
7. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
8. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens to show the status of the task.

Changing user permissions

User permissions are determined by the groups to which the user belongs. You change these permissions by changing membership in the user group. A user can belong to multiple user groups.

For example, if you want to change the role of the user who manages security to the performance management role, add this user to the Storage Administrator (Performance Management) role group and then remove the user from the Security Administrator (View & Modify) role group.

Prerequisites

- You must have the Security Administrator (View & Modify) role to perform this task.
- The user whose permissions you want to change must belong to at least one user group.
- A user account can belong to up to 8 user groups.

- A user group can contain a maximum of 20 user accounts, including the built-in user accounts.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, select the user group that has the role you want the user to have, and then click **Add Users**.
3. In the **Add User** dialog box, select the user and click **Add**.
4. Click **Finish**.
5. In the **Confirm** window, check the settings. If the **Task Name** field is empty, enter a task name.
6. Click **Apply**. The task is registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens. The **Task** window shows the status of the task.
7. In the **Administration** tree, click **User Groups**.
8. Click the **User Groups** tab, then select the user group from which to remove a user.
9. On the **User** tab, select the user group from which to remove a user.
10. Click **More Actions > Remove Users**.
11. In the **Delete Users** window, select the user to be deleted and click **Finish.**
12. In the **Confirm** window, check the settings.
13. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens to show the status of the task.

Disabling user accounts

Security Administrators can disable a user account to temporarily prevent the user from logging in to Device Manager - Storage Navigator.

To allow a user to log in to Device Manager - Storage Navigator, perform this task, but select Enable instead of Disable in the **Edit User** dialog box.

Caution: Do not select any user account used to connect to a storage system that is registered in the **Storage Device List** window. For details, see the Hardware Reference Guide for your storage system.

Prerequisites

- Log into an account that is different from the user whose account that you want to disable.
- You must have the Security Administrator (View & Modify) role to perform this task.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, click **User Groups**.
2. On the **User Group** tab, select the user group.
3. On the **Users** tab, select a user.
4. Click **Edit User**.
5. Click the **Account Status** check box, then click **Disable**.
6. Click **Finish**.
7. In the **Confirm** window, check the settings.
8. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens to show the status of the task.

Deleting user accounts

Security Administrators can delete a user account when the account is no longer in use. Built-in user accounts cannot be deleted.

Caution: Do not select any user account used to connect to a storage system that is registered in the **Storage Device List** window. For details, see the Hardware Reference Guide for your storage system.

Prerequisites

You must have the Security Administrator (View & Modify) role to perform this task.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, click a user group to which a user belongs.
3. On the **Users** tab, select the user whose account you want to delete.
4. Click **More Actions > Delete Users**.
5. In the **Delete Users** window, select the user to be deleted, then click **Finish.**
6. In the Confirm window, check the settings.
7. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens to show the status of the task.

Releasing a user lockout

If a user attempting to log in to Device Manager - Storage Navigator or Command Control Interface enters an incorrect username or password three times, the system sets the login status to locked, preventing further login attempts for 60 seconds. If necessary, you can release the locked status before the lock times out.

Prerequisites

You must have the Security Administrator (View & Modify) role to perform this task.

Procedure

1. In the **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, click a user group to which the locked-out user belongs.
3. On the **User** tab, select the user you want to unlock.
4. On the **User** tab, click **More Actions > Release Lockout**.
   The **Release Lockout** window opens.
5. Specify a task name, and then click **Apply**.

Managing user groups

You can use the Device Manager - Storage Navigator to view existing user groups, and to create, modify, or delete them.

Roles

The following table shows all the roles that are available for use and the permissions that each role provides to the users. You cannot create a custom role.

Role	Capabilities
Security Administrator (View Only)	• Viewing information about user accounts and encryption settings • Viewing information about the encryption key in the key SVP
Security Administrator (View & Modify)	• Configuring user accounts • Creating encryption keys and configuring encryption settings • Viewing and switching where encryption keys are generated • Backing up and restoring encryption keys • Deleting encryption keys backed up in the key SVP • Viewing and changing the password policy for backing up encryption keys on the management client • Connection to the external server • Backing up and restoring connection configuration to the external server • Configuring the certificate used for the SSL communication • Configuring the fibre channel authentication (FC-SP) • Configuring resource groups • Editing virtual management settings • Setting reserved attributes for global-active device
Audit Log Administrator (View Only)	• Viewing audit log information and downloading audit logs

Role	Capabilities
Audit Log Administrator (View & Modify)	• Configuring audit log settings and downloading audit logs
Storage Administrator (View Only)	• Viewing storage system information
Storage Administrator (Initial Configuration)	• Configuring settings for storage systems • Configuring settings for SNMP • Configuring settings for e-mail notification • Configuring settings for license keys • Viewing, deleting, and downloading storage configuration reports • Acquiring all the information about the storage system and updating Device Manager - Storage Navigator window by clicking Refresh All
Storage Administrator (System Resource Management)	• Configuring settings for CLPR • Configuring settings for MP unit • Deleting tasks and releasing exclusive locks of resources • Configuring LUN security • Configuring Server Priority Manager • Configuring tiering policies
Storage Administrator (Provisioning)	• Configuring caches • Configuring volumes, pools, and virtual volumes • Formatting and shredding volumes • Configuring external volumes • Configuring Dynamic Provisioning • Configuring host groups, paths, and WWN • Configuring Volume Migration except splitting Volume Migration pairs when using CCI • Configuring access attributes for volumes • Configuring LUN security • Creating and deleting quorum disk used with global-active device • Creating and deleting global-active device pairs
Storage Administrator (Performance Management)	• Configuring monitoring • Starting and stopping monitoring
Storage Administrator (Local Copy)	• Performing pair operations for local copy • Configuring environmental settings for local copy • Splitting Volume Migration pairs when using CCI
Storage Administrator (Remote Copy)	• Remote copy operations in general • Operating global-active device pairs (except for creation and deletion)
Support Personnel (Vendor Only)	Configuring the SVP • Normally, this role is for Hitachi Data Systems service representatives.
Support Personnel (User)	• Viewing storage system status • Installing OS security patches • Updating operating systems • Performing basic maintenance

Built-in groups, roles, and resource groups

You can assign users to one or more built-in user groups and custom user groups. You cannot change roles or resource groups set to the built-in groups, but you can create custom user groups according to the needs of your storage environment.

For more information about resource groups, see the *Provisioning Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*.

The following table shows all the built-in groups, and their built-in roles and resource groups.

Built-in group	Role	Resource group
Administrator	• Security Administrator (View & Modify) • Audit Log Administrator (View & Modify) • Storage administrator (Initial Configuration) • Storage Administrator (System Resource Management) • Storage Administrator (Provisioning) • Storage Administrator (Performance Management) • Storage Administrator (Local Copy) • Storage Administrator (Remote Copy)	All Resource Groups Assigned
System	• Security Administrator (View & Modify) • Audit Log Administrator (View & Modify) • Storage Administrator (Initial Configuration) • Storage Administrator (System Resource Management) • Storage Administrator (Provisioning) • Storage Administrator (Performance Management) • Storage Administrator (Local Copy) • Storage Administrator (Remote Copy)	All Resource Groups Assigned
Security Administrator (View Only)	• Security Administrator (View Only) • Audit Log Administrator (View Only) • Storage Administrator (View Only)	All Resource Groups Assigned
Security Administrator (View & Modify)	• Security Administrator (View & Modify) • Audit Log Administrator (View & Modify) • Storage Administrator (View Only)	All Resource Groups Assigned
Audit Log Administrator (View Only)	• Audit Log Administrator (View Only) • Storage Administrator (View Only)	All Resource Groups Assigned
Audit Log Administrator (View & Modify)	• Audit Log Administrator (View & Modify) • Storage Administrator (View Only)	All Resource Groups Assigned
Storage Administrator (View Only)	• Storage Administrator (View Only)	meta_resource
Storage Administrator (View & Modify)	• Storage Administrator (Initial Configuration) • Storage Administrator (System Resource Management) • Storage Administrator (Provisioning) • Storage Administrator (Performance Management) • Storage Administrator (Local Copy) • Storage Administrator (Remote Copy)	meta_resource

Built-in group	Role	Resource group
Support Personnel	• Storage Administrator (Initial Configuration) • Storage Administrator (System Resource Management) • Storage Administrator (Provisioning) • Storage Administrator (Performance Management) • Storage Administrator (Local Copy) • Storage Administrator (Remote Copy) • Support Personnel	All Resource Groups Assigned

Related tasks

- Checking if a role is available to a user group on page 70

Verifying the roles available to a user group

You can use Device Manager - Storage Navigator to verify the roles that are available to use with any user group.

Prerequisites

You must have the Security Administrator (View Only) role to perform this task.

Procedure

1. In the Device Manager - Storage Navigator tree, click **User Administration**.
2. On the **User Groups** tab, click the name (not the checkbox) of a user group whose roles you want to check.
3. In the **User Administration** window, click the **Roles** tab.

   The list of roles applied to the selected user group is displayed.
4. To return to the **User Administration** window, click **User Administration**.

Checking if a role is available to a user group

You can use Device Manager - Storage Navigator to verify the roles that are available to use with any user group.

You can assign users to one or more built-in user groups and custom user groups. You cannot change roles or resource groups set to the built-in groups, but you can create custom user groups according to the needs of your storage environment.

Prerequisites

You must have the Security Administrator (View Only) role to perform this task.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, click **User Administration**.
2. On the **User Groups** tab, click the **name** (not the checkbox) of a user group whose roles you want to check.
3. In the **User Administration** window, click the **Roles** tab. The list of roles applied to the selected user group is displayed.
4. To return to the **User Administration** window, click **User Administration**.

Related references

- Built-in groups, roles, and resource groups on page 68

Creating a new user group

This section explains how administrators can create a user group.

A user group name consists of 1 to 64 characters including alphanumeric characters, spaces, and the following symbols:

! # $ % & ' ( ) + - . = @ [ ] ^ _ ` { } ~
The system can support a maximum of 32 user groups, including the nine built-in user groups.

Prerequisites

- You must have the Security Administrator (View & Modify) role to perform this task.

Procedure

1. In the **Administration** tree, select **User Groups**.
2. In the **User Groups** tab, click **Create User Groups** to open the **Create User Group** window.
3. Enter a user group name.
4. If you use an authorization server, click **Check** and verify that the entered user group name is registered in the authorization server.
5. Click **Next** to open the **Assign Roles** window.
6. Select the roles to assign to the user group, and click **Add**.
7. Click **Next** to open the **Assign Resource Groups** window.
8. Select the resource groups to assign to the user group, and click **Add**. If you select a role other than the storage administrator in the **Assign Roles** window, you do not need to select resource groups because all the resource groups are assigned automatically.

9. Click **Finish** to finish and confirm settings.

   Click **Next** to add another user.
10. Check the settings and enter a task name in **Task Name**.
11. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens to show the status of the task.

Changing a user group name

This section explains how to change the name of a user group.

Prerequisites

- You must have the Security Administrator (View & Modify) role to perform this task.
- The names of built-in groups cannot be changed.
- A user group name consists of 1 to 64 characters including alphanumeric characters (ASCII), spaces and the following symbols:
  # $ % & ' ( ) + - . = @ [ ] ^ _ ` { } ~

Procedure

1. In the **Administration** tree, select **User Groups**.
2. In the **User Groups** tab, select the user group.
3. Click **More Actions > Edit User Group**.
4. In the **Edit User Group** window, enter a new user group name.
5. If you use an authorization server, click **Check** and verify that the entered user group name is registered in the authorization server.
6. Click **Finish**.
7. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
8. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens to display the status of the task.

Changing user group permissions

This section explains how to change the permissions that are assigned to user groups.

Prerequisites

- You must have the Security Administrator (View & Modify) role to perform this task.
- The permissions of a built-in group cannot be changed.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. In the **User Groups** tab, select the user group whose permission you want to change.
3. Click the **Roles** tab.
4. Click **Edit Role Assignment**.
5. In the **Edit Role Assignment** window, change roles to be assigned to the user group.
   - Select roles to add, and then click **Add**.
   - Select a role to remove, and then click **Remove**.
6. Click **Finish**.
7. In the **Confirm** window, check the settings and enter a task name in **Task Name**.
8. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens.

Changing assigned resource groups

This section explains how to change the resource groups that are assigned to the user group.

Prerequisites

- You must have the Security Administrator (View & Modify) role to perform this task.
- Create a resource group to be assigned to the user group in advance.
- You cannot change the resource groups of a user group that has All Resource Groups Assigned set to Yes
- You cannot change resource groups of a built-in group.

Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. On the **User Groups** tab, select a user group to change the resource group.
3. Select the **Resource Groups** tab.
4. Click **Edit Resource Group Assignment** to open the **Edit Resource Group Assignment** window.
5. In the **Edit Resource Group Assignment** window, change resource groups to be assigned to the user group.
   - Select the resource group to add, and click **Add**.
   - Select the resource group to remove, and click **Remove**.
6. Click **Finish**.
7. In the **Confirm** window, check the settings and enter a task name in **Task Name**.

8. Click **Apply**. The task is now registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens to display the status of the task.

Deleting a user group

Delete a user group when it is no longer needed.

Prerequisites

- You must have the Security Administrator (View & Modify) role to perform this task.
- You cannot delete a built-in user group.
- You cannot delete a user group if the users in it belong to only the user group to be deleted.

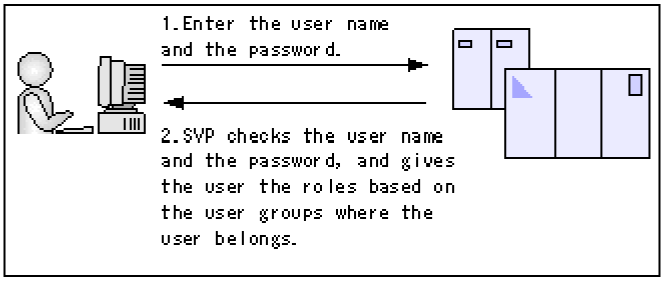
Procedure

1. In the Device Manager - Storage Navigator **Administration** tree, select **User Groups**.
2. In the **User Groups** tab, select the user-created user groups that you want to delete.
3. Click **More Actions > Delete User Groups**.
4. Check the settings, then click **Apply**.

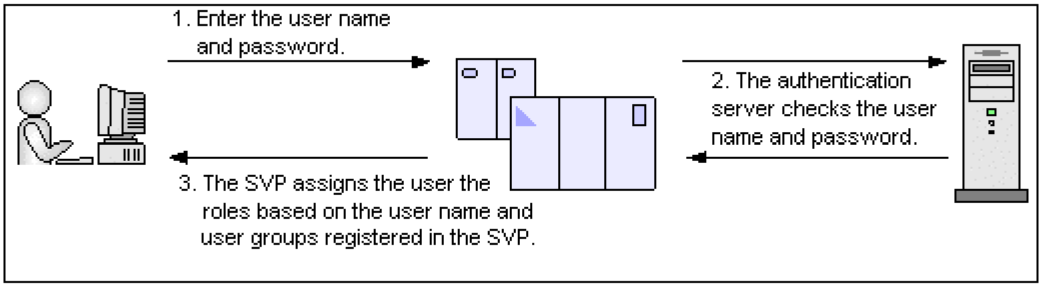
Using an authentication server and authorization server

An authentication server enables users to log in to Device Manager - Storage Navigator with the same password as the password that they use for other applications. The authentication server must be configured for each user.

The following figure shows login workflow without an authentication server:

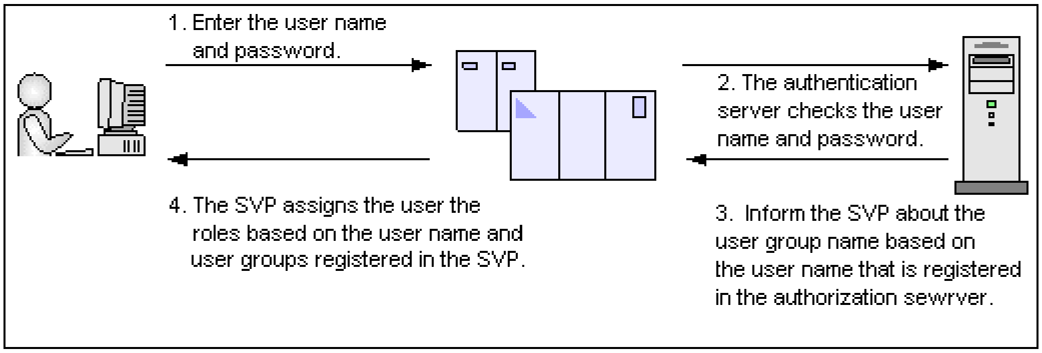

1.Enter the user name and the password.
2.SVP checks the user name and the password, and gives the user the roles based on the user groups where the user belongs.

The following figure shows login workflow with an authentication server:


1. Enter the user name and password.
2. The authentication server checks the user name and password.
3. The SVP assigns the user the roles based on the user name and user groups registered in the SVP.

If an authorization server works together with an authentication server, the user groups that are registered in the authorization server can be assigned to a user for Device Manager - Storage Navigator.

The following figure shows login workflow when an authentication server and an authorization server are used in combination:


1. Enter the user name and password.
2. The authentication server checks the user name and password.
3. Inform the SVP about the user group name based on the user name that is registered in the authorization sewrver.
4. The SVP assigns the user the roles based on the user name and user groups registered in the SVP.

You can use the authentication server without knowing the host names and port numbers, if you register the information of the authentication server as an SRV record in the DNS server. If you register multiple numbers of authentication servers to the SRV record, you can determine the authentication server to be used, based on the priority that has been set in advance.

Authentication server protocols

Authentication servers support the following protocols:

- LDAPv3 simple bind authentication
- RFC 2865-compliant RADIUS with PAP and CHAP authentication
- Kerberos v5

The following certificate file formats are available for LDAP server settings:

- X509 DER format
- X509 PEM format

One of the following encryption types must be used for the Kerberos server:

Windows

- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC
- DES3-CBC-SHA1
- DES-CBC-CRC
- DES-CBC-MD5

Solaris or Linux

- DES-CBC-MD5

Authorization server requirements

The authorization server must satisfy the following requirements if it works together with the authentication server:

Prerequisite OS

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

Prerequisite software

- Active Directory

Authentication protocol for user for searching

- LDAP v3 simple bind

Connecting two authentication servers

Two authentication servers can be connected. When the servers are connected, the server configurations must be the same, except for the IP address and the port.

If you search for a server using information registered in the SRV records in the DNS server, confirm that the following conditions are satisfied:

LDAP server conditions:

- The environmental setting for the DNS server is completed at the LDAP server.
- The host name, the port number, and the domain name of the LDAP server are registered in the DNS server.

Kerberos server conditions:

- The host name, the port number, and the domain name of the Kerberos server are registered in the DNS server.
- You cannot use the SRV records on a RADIUS server.

Because UDP/IP is used to access the RADIUS server, no encrypted communications are available, such as negotiations between processes. To access the RADIUS server in a secure environment, encryption in the packet level is required, such as IPsec.

Connecting authentication and authorization servers

To use an authentication server and an authorization server, you must create configuration files and configure your network. Detailed setting information is required for the authentication server and the authorization server, especially for creating a configuration file. Contact your server administrator for more information about the values to be written in the LDAP, RADIUS, or Kerberos configuration file. Contact your network administrator for more information about the network settings.

Prerequisites

- Contact your server administrator for information about the values to be written in the LDAP, RADIUS, or Kerberos configuration file. If you use LDAP servers, obtain certification for the LDAP server files.
- Contact your network administrator for information about the network settings.

Procedure

1. **1.** Create a configuration file. The items to specify depend on the protocol you use.
2. **2.** Log in to the SVP and store the following files in an easily accessible location.
   - Certificate (for secure communication)
   - Configuration file
3. **3.** Open the Windows command prompt on the SVP.
4. **4.** Move the current directory to the directory where MappSetExAuthConf.bat is located (for example, `C:\MAPP\wk\Supervisor\MappIniSet`).

   Run the following command specifying the configuration file path (for example, `C:\aut\auth.properties`) and the certificate file path (for example, `C:\auth\auth.cer`):

   ```
   C:\MAPP\wk\Supervisor\MappIniSet\MappSetExAuthConf"C:\auth
   \auth.properties" "C:\auth\auth.cer"
   ```
5. **5.** After you complete the settings and verify that you can use the authentication and authorization servers, back up the connection settings for the authentication server.

If the authentication server and the authorization server are unusable even after you make the settings, the network or the configuration file settings might have a problem. Contact the server administrator or the network administrator.

Naming a user group in Device Manager - Storage Navigator

When you create a user group in Device Manager - Storage Navigator, you name the group with the user's `memberOf` attribute value which is found in the Active Directory. Device Manager - Storage Navigator supports Active Directory nested groups.

After entering the user group name, verify that the user group name that you entered is registered in the authorization server.

⚠ **Note:** The domain name (DN) of the user group to be set to Active Directory must be between 1 and 250 characters. The number of user groups that can be registered at one time is 20 at maximum.

⚠ **Caution:** If a user needs to use different user groups for different purposes, create local user accounts on Device Manager - Storage Navigator. Do not use the authorization server.

Creating configuration files

This section includes the procedures to create LDAP, RADIUS, and Kerberos configurations files.

Creating an LDAP configuration file

To use an LDAP server for authentication, create a configuration file in UTF-8 encoding. Include information about the authentication server as shown in the following example. Any file name and extension is allowed.

```
auth.server.type=ldap
auth.server.name=<server_name>
auth.group.mapping=<value>
auth.ldap.<server_name>.<attribute>=<value>
```

A full example is shown here:

```
auth.server.type=ldap
auth.server.name=PrimaryServer
auth.group.mapping=true
auth.ldap.PrimaryServer.protocol=ldaps
auth.ldap.PrimaryServer.host=ldaphost.domain.local
auth.ldap.PrimaryServer.port=636
auth.ldap.PrimaryServer.timeout=3
auth.ldap.PrimaryServer.attr=sAMAccountName
auth.ldap.PrimaryServer.searchdn=CN=sample1,CN=Users,DC=domain,DC
=local
auth.ldap.PrimaryServer.searchpw=passwordauth.ldap.PrimaryServer.
basedn=CN=Users,DC=domain,DC=local
```

```
auth.ldap.PrimaryServer.retry.interval=1
auth.ldap.PrimaryServer.retry.times=3
auth.ldap.PrimaryServer.domain.name=EXAMPLE.COM
```

The LDAP attributes are defined in the following table.

Attribute	Description	Required / Optional	Default value
auth.server.type	Type of an authentication server. Specify `ldap`.	Required	None
auth.server.name	The name of an authentication server. When registering a primary and a secondary server, use a comma to separate the names. The name of the server, including the primary name, secondary name, and the comma (1 byte) must be 64 bytes or less. The names can use all ASCII code characters except for the following: \ / : , ; * ? " < > | $ % & ' ~ In this manual, the value specified here is called <server_ name> hereafter.	Required	None
auth.group.mapping	Information about whether to work together with an authorization server: • true: Works together • false: Does not work together	Optional	False
auth.ldap.<server_name>.protocol	LDAP protocol to use. • ldaps: Uses LDAP over SSL/TLS. • starttls: Uses StartTLS. When you specify "true" to auth.ldap.<server_name>.dns_lookup, specify ldaps.	Rquired	None
auth.ldap.<server_name>.host	A host name, an IPv4 address or an IPv6 address of the LDAP server. An IPv6 address must be enclosed in square brackets. To use StartTLS as a protocol, specify a host name. If this value is specified, auth.ldap.<server_name>.dns_lookup will be ignored	Optional[1]	None
auth.ldap.<server_name>.port	A port number of the LDAP server. Must be between 1 and 65,535.[2]	Optional	389
auth.ldap.<server_name>.timeout	The number of seconds before the connection to the LDAP server	Required	10

Attribute	Description	Required / Optional	Default value
	times out. It must be between 1 and 30.[2]		
auth.ldap.<server_name>.attr	Attribute name to identify a user (such as a user ID). • Hierarchical model: An attribute name where the value that can identify a user is stored • Flat model: An attribute name for a user entry's RDN sAMAccountName is used for Active Directory.	Required	None
auth.ldap.<server_name>.searchdn	DN of the user for searching. If omitted, [value_of_attr]=[Login_ID],[value_of _basedn] is used for bind authentication.[3]	Otional	None
auth.ldap.<server_name>.searchpw	User password that is used for searching. Specify the same password that is registered in the LDAP server.	Required	None
auth.ldap.<server_name>.basedn	BaseDN for searching for users to authenticate.[3] • Hierarchical model: DN of hierarchy that includes all the targeted users for searching • Flat model: DN of hierarchy that is one level up from the targeted user for searching	Required	None
auth.ldap.<server_name>.retry.interval	Retry interval in seconds when the connection to the LDAP server fails. Must be between 1 and 5.[2]	Optional	1
auth.ldap.<server_name>.retry.times	Retry times when the connection to the LDAP server fails. Must be between 0 and 3. Zero means no retry.[2]	Optional	3
auth.ldap.<server_name>.domain.name	A domain name that the LDAP server manages.	Required	None
auth.ldap.<server_name>.dns_lookup	Information about whether to search the LDAP server with the information registered in the SRV records in the DNS server. • true: Searches with the information registered in the SRV records in the DNS server • false: Searches with the host name and port number When "host" and "port" are specified, the LDAP server is not	Optional	False

Attribute	Description	Required / Optional	Default value
	searched with the information registered in the SRV records by specifying "true".		
Notes: **1.** The item can be omitted if true is specified for "auth.ldap.<server_name>.dns_lookup". **2.** If the specified value is not valid, the default value will be used. **3.** To use symbols such as + ; , < = and >, enter a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash before it. For example, to enter abc++ in the searchdn field, use \+ instead of + as shown here: abc\+\+ To enter \ , /, or ", enter a backslash and then enter the ASCII code in hex for the following symbols: • Enter \5c for \ • Enter \2f for / • Enter \22 for " For example, to enter abc\ in the searchdn field, enter abc\5c.			

Creating a RADIUS configuration file

To use a RADIUS server for authentication, create a configuration file in UTF-8 encoding. Include information about the authentication server as shown in the following example. Any file name and extension is allowed. If an authorization server is not used, you do not need to define the items for it.

```
auth.server.type=radius
auth.server.name=server-name
auth.group.mapping=value
auth.radius.server-name.attribute=value
auth.group.domain-name.attribute=value
```

A full example is shown below:

```
auth.server.type=radius
auth.server.name=PrimaryServer
auth.group.mapping=true
auth.radius.PrimaryServer.protocol=pap
auth.radius.PrimaryServer.host=xxx.xxx.xxx.xxx
auth.radius.PrimaryServer.port=1812
auth.radius.PrimaryServer.timeout=3
auth.radius.PrimaryServer.secret=secretword
auth.radius.PrimaryServer.retry.times=3
auth.radius.PrimaryServer.attr.NAS-Identifier=xxxxxxxx
auth.group.auth.radius.PrimaryServer.domain.name=radius.example.c
om
auth.group.auth.radius.PrimaryServer.domain.name.protocol=ldap
auth.group.auth.radius.PrimaryServer.domain.name.host=xxx.xxx.xxx
.xxx
auth.group.auth.radius.PrimaryServer.domain.name.port=386
auth.group.auth.radius.PrimaryServer.domain.name.searchdn=CN=samp
le1,CN=Users,DC=domain,DC=local
auth.group.auth.radius.PrimaryServer.domain.name.searchpw=passwor
d
auth.ldap.PrimaryServer.basedn=CN=Users,DC=domain,DC=local
```

The attributes are defined in the following tables.

Table 4 RADIUS definition (for authentication server)

Attribute	Description	Required / Optional	Default value
auth.server.type	Type of an authentication server. Specify `radius`.	Required	None
auth.server.name	The name of an authentication server. When registering a primary and secondary server, use a comma to separate the names. The name of the server, including the primary name, secondary name, and the comma (1 byte) must be 64 bytes or less. The names can use all ASCII code characters except for the following: \ / : , ; * ? " < > | $ % & ' ˜ In this manual, the value specified here is called *server-name* hereafter.	Required	None
auth.group.mapping	Information about whether to work together with an authorization server • true: Works together • false: Does not work together	Optional	False
auth.radius.*server-name*.protocol	RADIUS protocol to use. • PAP: Password authentication protocol that transmits plaintext user ID and password • CHAP: Challenge-handshake authentication protocol that transmits encrypted password	Required	None
auth.radius.*server-name*.host	A host name, an IPv4 address or an IPv6 address of the RADIUS server. An IPv6 address must be enclosed in square brackets.	Required	None
auth.radius.*server-name*.port	A port number of the RADIUS server. Must be between 1 and 65,535.[1]	Optional	1,812
auth.radius.*server-name*.timeout	The number of seconds before the connection to the RADIUS server times out. Must be between 1 and 30.[2]	Optional	10
auth.radius.*server-name*.secret	RADIUS secret key used for PAP or CHAP authentication	Required	None
auth.radius.*server-name*.retry.times	Retry times when the connection to the RADIUS server fails. Must be between 0 and 3. 0 means no retry.[1]	Optional	3
auth.radius.*server-name*.attr.NASIdentifier	Identifier for the RADIUS server to find SVP. Specify this value if the attr.NAS-	Optional[2]	None

Attribute	Description	Required / Optional	Default value
	Identifier attribute is used in your RADIUS environment. ASCII codes up to 253 bytes long are accepted.		
auth.radius.*server-name*.attr.NAS-IPv4-Address	IPv4 address of the SVP. Specify the value of the NAS-IP-Address attribute. This value is transmitted to the RADIUS server when the authentication is requested.	Optional[2]	None
auth.radius.*server-name*.attr.NAS-IPv6-Address	IPv6 address of the SVP. Specify the value of the NAS-IPv6-Address attribute. This value is transmitted to the RADIUS server when the authentication is requested.	Optional[2]	None
Notes: **1.** If the specified value is not applicable, the default value will be used. **2.** Set either `NAS-Identifier`, `NAS-IP-Address`, or `NAS-IPv6-Address`.			

Table 5 RADIUS definition (for authorization server)

Attribute	Description	Required / Optional	Default value
auth.radius.*server-name*.domain.name	A domain name that the LDAP server manages. In this manual, the value specified here is called *domain-name* hereafter.	Required	None
auth.radius.*server-name*.dns_lookup	Information about whether to search the LDAP server with the information registered in the SRV records in the DNS server. • true: Searches with the information registered in the SRV records in the DNS server • false: Searches with the host name and port number. When "host" and "port" are specified, the LDAP server is not searched with the information registered in the SRV records by specifying "true".	Optional	false
auth.radius.*domain-name*.protocol	LDAP protocol to use. • ldaps: Uses LDAP over SSL/TLS. • starttls: Uses StartTLS. When you choose ldap, specify "true" to "auth.radius.*domain-name*.dns_lookup"	Required	None
auth.radius.*domain-name*.host	A host name, an IPv4 address or an IPv6 address of the LDAP server. An IPv6	Optional[1]	None

Attribute	Description	Required / Optional	Default value
	address must be enclosed in square brackets ([ ]).		
auth.radius.*domain-name*.port	A port number of the LDAP server. Must be between 1 and 65535.[2]	Optional	389
auth.radius.*domain-name*.searchdn	DN of the user for searching.	Required	None
auth.radius.*domain-name*.searchpw	User password for searching. Specify the same password that is registered in the LDAP server.	Required	None
auth.radius.*domain-name*.basedn	Base DN for searching for users to authenticate. Specify DN of the hierarchy, including all the users for searching because the targeted users for searching are in lower hierarchy than the specified DN.[3]	Optional	abbr
auth.radius.*domain-name*.timeout	The number of seconds before the connection to the LDAP server times out. Must be between 1 and 302.	Optional	10
auth.radius.*domain-name*.retry.interval	Retry interval in seconds when the connection to the LDAP server fails. Must be between 1 and 5.[2]	Optional	1
auth.radius.*domain-name*.retry.times	Retry times when the connection to the LDAP server fails. Must be between 0 and 3. 0 means no retry.[2]	Optional	3

Notes:

1. The item can be omitted if true is specified for "auth.ldap.*server-name*.dns_lookup".
2. If the specified value is not valid, the default value will be used.
3. To use symbols such as + ; , < = and >, enter a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash before it. For example, to enter abc++ in the searchdn field, use \+ instead of + as shown here: abc\+\+
   To enter \ , /, or ", enter a backslash and then the ASCII code in hex for these symbols.
   - Enter \5c for \.
   - Enter \2f for /.
   - Enter \22 for "

   For example, to enter abc\ in the searchdn field, enter abc\5c.

Creating a Kerberos configuration file

To use an Kerberos server for authentication, create a configuration file in UTF-8 encoding. Include information about the authentication server as shown in the following example. Any file name and extension are allowed. If an authorization server is not used, you do not need to define the items for it.

```
auth.server.type=kerberos
auth.group.mapping=<value>
auth.kerberos.<attribute>=<value>
auth.group.<realm name>.<attribute>=<value>
```

A full example is shown below:

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=example.com
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockshow=300
auth.kerberos.timeout=10
auth.group.example.com.searchdn=CN=sample1,CN=Users,DC=domain,DC=
localauth.group.example.com.searchpw=passwordauth.ldap.PrimarySer
ver.basedn=CN=Users,DC=domain,DC=local
```

The Kerberos attributes are defined in the following table.

Table 6 Kerberos definition (for authentication server)

Attribute	Description	Required / Optional	Default value
auth.server.type	Type of an authentication server. Specify `kerberos`.	Required	None
auth.group.mapping	Information about whether to work together with an authorization server • true: Works together • false: Does not work together	Optional	false
auth.kerberos.default_realm	Default realm name	Required	None
auth.kerberos.dns_lookup.kdc	This is a switch that determines which information registered in the SRV records in the DNS server to use when searching the Kerberos server. • true: Searches with the information registered in the SRV records in the DNS server • false: Searches with the host name and port number When "realm name" and "<value specified to the realm name>.kdc" are specified, the Kerberos server is not searched with the information registered in the SRV records by specifying "true".	Optional	false
auth.kerberos.clockskew	The acceptable range of the difference in time between the SVP and the Kerberos server where the SVP is operating. Must be between 0 and 300 seconds.[1]	Optional	300

Attribute	Description	Required / Optional	Default value
auth.kerberos.timeout	The number of seconds before the connection to the RADIUS server times out. Must be between 1 and 30. When 0 is specified, the connection does not time out until a communication error occurs.[1]	Optonal	10
auth.kerberos.realm_name	Realm identifier name Any name to distinguish the information of Kerberos server in each realm. Duplicate names cannot be used. If you register multiple names, use a comma to separate the names. The value specified here is called <realm_name> hereafter.	Optional[2]	None
auth.kerberos.<realm_name>.realm	The realm name set to the Kerberos server.	Optional[2]	None
auth.kerberos.<realm_name>.kdc	The host name, the IPv4 address, and the port number of the Kerberos server. Specify these in the format of "<Host name or IP address>[:Port number]".	Optional[2]	None

Notes:

1. The item can be omitted if true is specified for "auth.ldap.<server_name>.dns_lookup".
2. If the specified value is not valid, the default value will be used.
3. To use symbols such as + ; , < = and >, enter a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash before it. For example, to enter abc++ in the searchdn field, use \+ instead of + as shown here: abc\+\+
   To enter \ , /, or ", enter a backslash and then the ASCII code in hex for these symbols.
   - Enter \5c for \.
   - Enter \2f for /.
   - Enter \22 for ".

   For example, to enter abc\ in the searchdn field, enter abc\5c.

Table 7 Kerberos definition (for authorization server)

Attribute	Description	Required / Optional	Default value
auth.group.<realm_name>.protocol	LDAP protocol to use. • ldaps: Uses LDAP over SSL/TLS. • starttls: Uses StartTLS.	Required	None
auth.group.<realm_name>.port	A port number of the LDAP server. Must be between 1 and 65535. [1]	Optoinal	389
auth.group.<realm_name>.searchdn	DN of the user for searching.[2]	Required	None

Attribute	Description	Required / Optional	Default value
auth.group.<realm_name>.searchpw	Password of the user for searching. Specify the same password that is registered in the LDAP server.	Required	None
auth.group.<realm_name>.basedn	BaseDN when the search for users begins. When searching, specify the hierarchy DN, including all the users, because the targeted user for the search is in a lower hierarchy than the specified DN.[2]	Optional	abbr
auth.group.<realm_name>.timeout	Number of seconds before the connection to the LDAP server times out. Must be between 1 and 30 seconds. When 0 is specified, the connection does not time out until a communication error occurs.[1]	Optional	10
auth.group.<realm_name>.retry.interval	Retry interval in seconds when the connection to the LDAP server fails. Must be between 1 and 5.[1]	Optional	1
auth.group.<realm_name>.retry.times	Retry times when the connection to the LDAP server fails. Must be between 0 and 3. 0 means no retry.[1]	Optional	3

Notes:

1. If the specified value is not valid, the default value will be used.
2. To use symbols such as + ; , < = and >, enter a backslash (\) before each symbol. When using multiple symbols, each symbol must have a backslash before it. For example, to enter abc++ in the searchdn field, use \+ instead of + as shown here: abc\+\+
   To enter \ , /, or ", enter a backslash and then the ASCII code in hex for these symbols.
   - Enter \5c for \
   - Enter \2f for /
   - Enter \22 for "

   For example, to enter abc\ in the searchdn field, enter abc\5c.

Related concepts

- Using an authentication server and authorization server on page 74

Related tasks

- Connecting authentication and authorization servers on page 77

4

Alert notifications

This section provides requirements and procedures to view and manage system event and alert notifications.

Viewing alert notifications

You can view alert email messages, alert Syslog messages, and alert SNMP trap messages in the Device Manager - Storage Navigator Alerts tab and the **Alert Detail** window.

Prerequisites

You must have the Storage Administrator (View Only) or Storage Administrator (Initial Configuration) role to perform this task.

- Email: Check your email to view alerts sent by email. Alerts that are reported through email are the same as the SIM information that is displayed in the Alert window or reported through an SNMP trap.
- Syslog: Check the messages on the Syslog server to view alert information sent there.
- SNMP traps: To view SNMP trap information, use the SNMP Manager in Device Manager - Storage Navigator. See the *Hitachi SNMP Agent User Guide* for information about using SNMP traps.

Configuring alert notifications

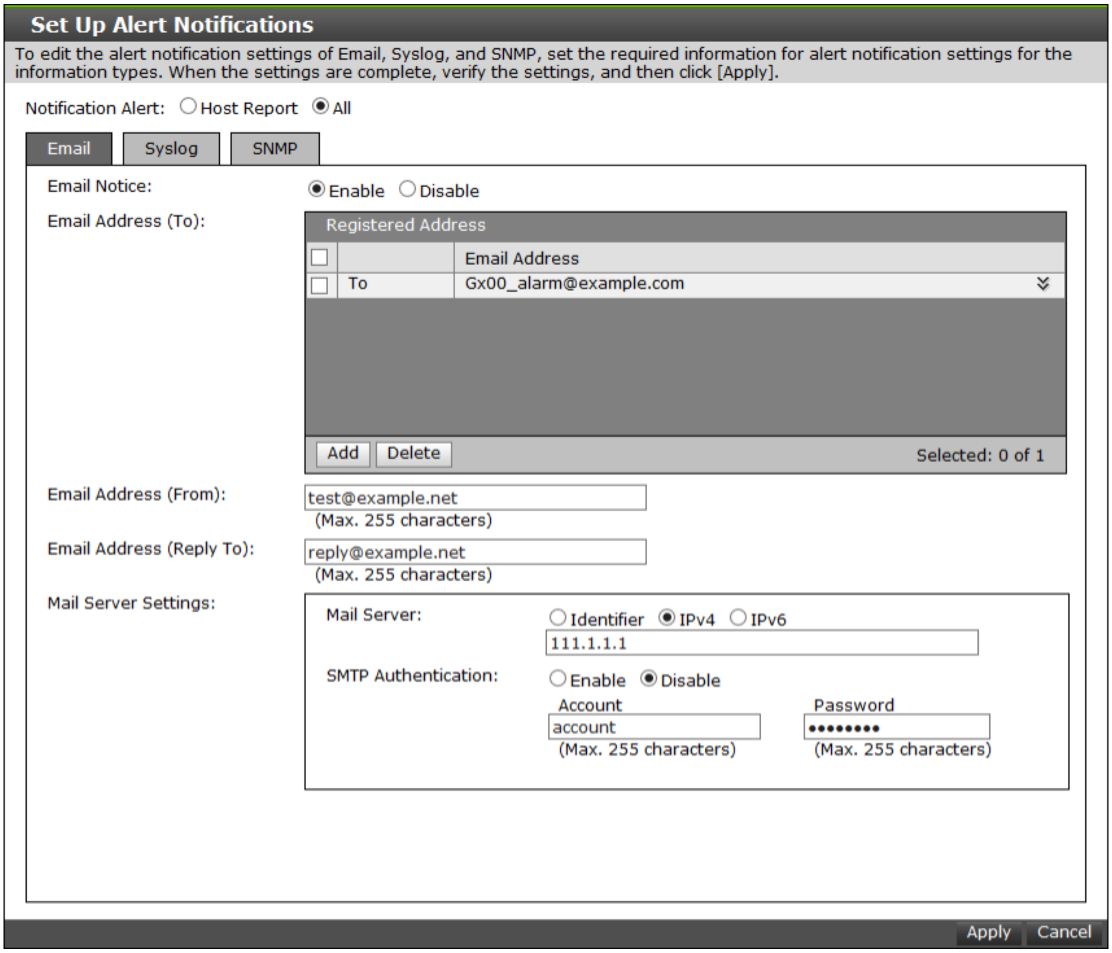
Procedure

1. In the maintenance utility, click the **SNMP** tab to display it.
2. In **SNMP Agent**, click **Enable** to use the agent or **Disable** not to use it.
3. Select the **Email** tab. The **Email** window displays the current settings for the Mail Server, SMTP Authentication, an Email Address.
4. To send a test email message, click **Send Test Email**. A completion notice displays.
5. Click OK to acknowledge the notice and close the message.
6. Click the **Syslog** tab. The **Syslog** window displays the current settings for the Primary Server, IP address, and port number, and for the secondary server IP address and port number.
7. To send a test message to the Syslog server, click **Send Test message to the Syslog Server**. A completion notice displays.
8. Click **OK** to acknowledge the notice and close the message.
9. Click the **SNMP** tab. The **SNMP** window displays the current settings for the Storage System Name, Contact, Location, SNMP Trap and SNMP Manager.
10. To send a test SNMP trap, click **Send Test SNMP Trap**. A completion notice displays.
11. Click **OK** to acknowledge the notice and close the message.

General settings

Procedure

1. In the maintenance utility **Administration** pane, select **Alert Notifications**.
2. In the **Alert Notifications** window, click **Set Up**. The **Set Up Alert Notifications** window displays the **Email** tab by default.



Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: ○ Host Report ● All

Email Notice: ● Enable ○ Disable

Email Address (To):

Registered Address

□		Email Address
□	To	Gx00_alarm@example.com

Selected: 0 of 1

Email Address (From): test@example.net (Max. 255 characters)

Email Address (Reply To): reply@example.net (Max. 255 characters)

Mail Server Settings:

Mail Server: ○ Identifier ● IPv4 ○ IPv6
111.1.1.1

SMTP Authentication: ○ Enable ● Disable

Account: account (Max. 255 characters)

Password: •••••••• (Max. 255 characters)

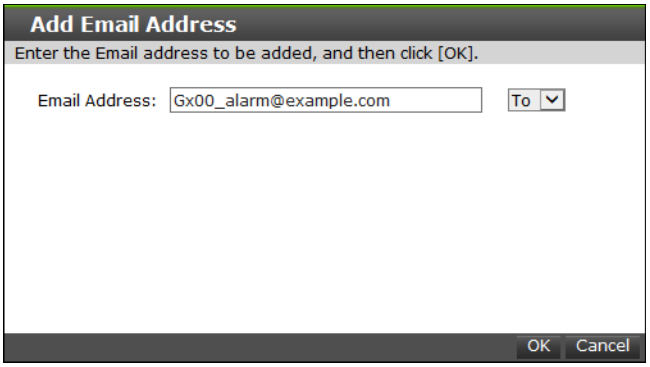
3. Select the type of report to send.
   - **Host Report**: Sends alerts only to the hosts for which a SIM report setting is made.
   - **All**: Sends alerts to all hosts.

   The alert notification destination is common to Syslog, SNMP, and email.

Email settings

Procedure

1. To send email notices click **Enable** next to **Email Notice**. Click **Disable** to not send email notices.
2. Click **Add** to add an email address to the list of registered addresses.



Add Email Address

Enter the Email address to be added, and then click [OK].

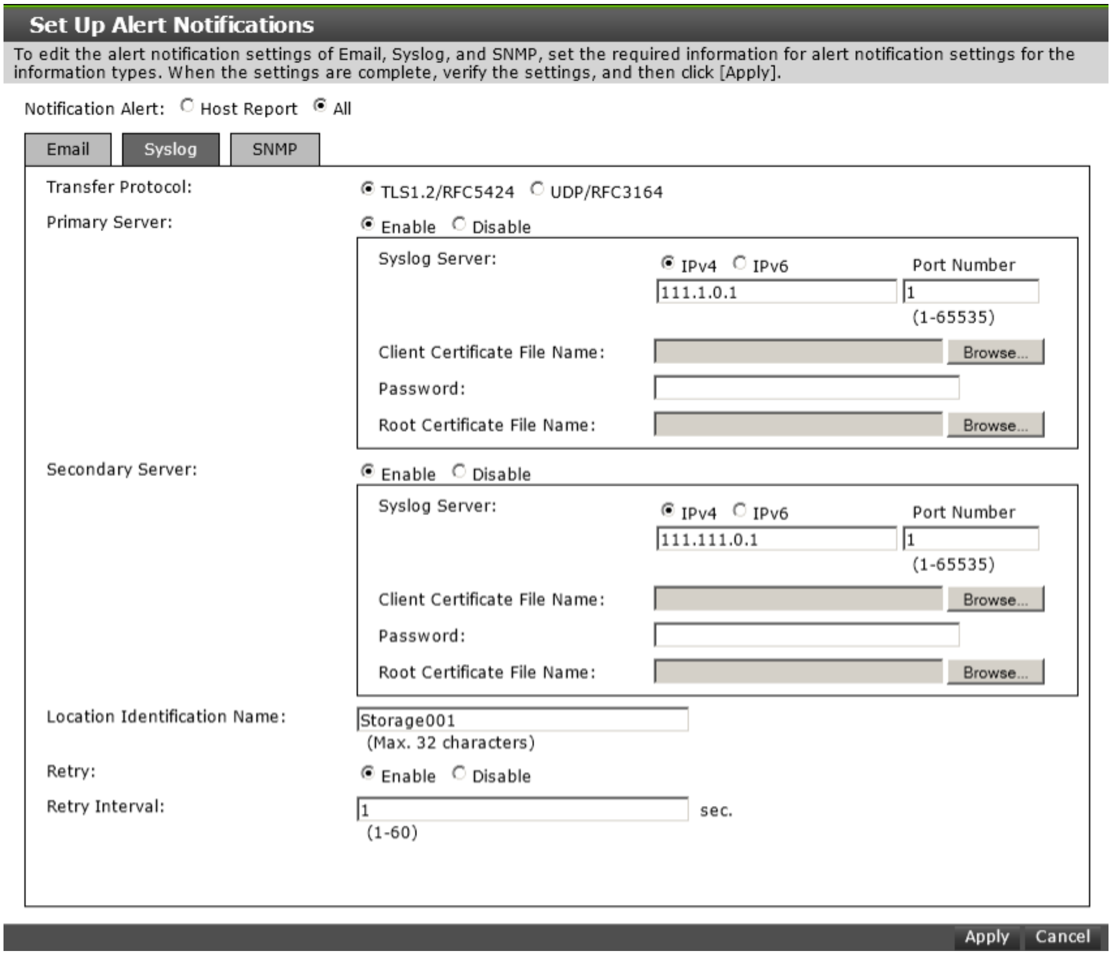
Email Address: Gx00_alarm@example.com To

3. Enter the email address and then use the pull-down menu to select the type of address: **To**, **Cc**, or **Bcc.**
4. Click **OK** to save the email address and close the dialog box.
5. Enter an email address in **Email Address (From)**.
6. Enter an email address in **Email Address (Reply To:)**.
7. In **Mail Server Settings**, select the mail server type: **Identifier**, **IPv4**, or **IPv6.**
8. To use SMTP authentication, click **Enable**.
9. In **Account**, enter an SMTP account name.
10. In **Password**, enter the SMTP account password.
11. Click **Apply** to save the changes and close the **Set Up Alert Notifications** window.

Syslog settings

Procedure

1. Click the **Syslog** tab.



Set Up Alert Notifications

To edit the alert notification settings of Email, Syslog, and SNMP, set the required information for alert notification settings for the information types. When the settings are complete, verify the settings, and then click [Apply].

Notification Alert: ○ Host Report ● All

Transfer Protocol: ● TLS1.2/RFC5424 ○ UDP/RFC3164

Primary Server: ● Enable ○ Disable

Syslog Server: ● IPv4 ○ IPv6 111.1.0.1 Port Number 1 (1-65535)

Client Certificate File Name: Browse...

Password:

Root Certificate File Name: Browse...

Secondary Server: ● Enable ○ Disable

Syslog Server: ● IPv4 ○ IPv6 111.111.0.1 Port Number 1 (1-65535)

Client Certificate File Name: Browse...

Password:

Root Certificate File Name: Browse...

Location Identification Name: Storage001 (Max. 32 characters)

Retry: ● Enable ○ Disable

Retry Interval: 1 sec. (1-60)

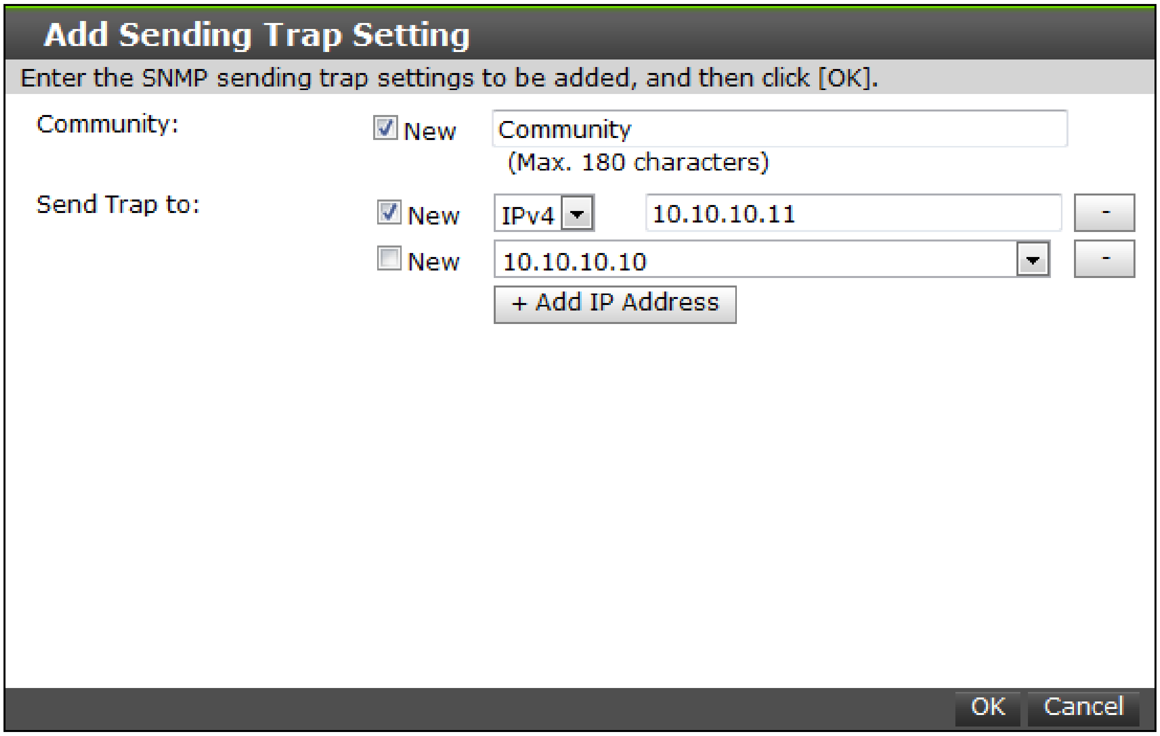
2. Select the type of transfer protocol to use.
3. In **Primary Server**:
   a. Click **Enable** to use the server or **Disable** not to use it.
   b. Select the type of IP address to use for the server: **IPv4** or **IPv6**.
   c. In **Client Certificate File Name**, click **Browse** to select a client certificate file.
4. In **Secondary Server**:
   a. Click **Enable** to use the server or **Disable** not to use it.
   b. Select the type of IP address to use for the server: **IPv4** or **IPv6**.
   c. In **Client Certificate File Name**, click **Browse** to select a client certificate file.

5. In **Location Identification Name** enter a name to use to identify the server.
6. To set up an automatic attempt to reconnect to the server in case of communication failure, in **Retry** click **Enable**. Click **Disable** to not use this feature.
7. If you enabled retry, in **Retry Interval** enter the number of seconds that the system will wait between retry attempts.

SNMP settings

Procedure

1. Click the **SNMP** tab.
2. In **SNMP Agent**, click **Enable** to use the agent or **Disable** not to use it.
3. In **Trap Destination**, click the type of address to send the SNMP trap information: **Community** or **Public.**
4. Click **Add** to add an SNMP trap address.



Add Sending Trap Setting

Enter the SNMP sending trap settings to be added, and then click [OK].

Community: ☑ New Community
(Max. 180 characters)

Send Trap to: ☑ New IPv4 10.10.10.11

☐ New 10.10.10.10

5. In **Community**, create a new community name or select an existing one.
6. In **Send Trap to**, enter a new IP address or select an existing one.
7. Click **OK** to save the information and close the dialog box.

Sending test messages

The lower section of the **Alert Notifications** window contains three tabs: Email, Syslog, and SNMP. Select the desired tab to send a test message of the type specified in the tab name.

Sending a test email message

Procedure

1. Click the **Email** tab.

   The **Email** tab displays the current settings for the mail server, SMTP authentications, and email addresses.
2. Click **Send Test Email**.

   A completion notice displays.
3. Click **OK** to acknowledge the notice and close the message.

Example of a test email message

```
Subject: VSP Gx00 Report
DATE : 24/10/2014
TIME : 10:09:30
Machine : Hitachi Virtual Storage Platform Gx00 (Serial# 64019)
RefCode : 7fffff
Detail: This is Test Report.
```

The field definitions in the test email message are listed in the following table.

Item	Description
Subject	Email title (name of the storage system) + (report)
DATE	Date when a system failure occurred.
TIME	Time when a system failure occurred.
Machine	Name and serial number of the storage system.
RefCode	Reference code. The same code as the one reported by SNMP traps.
Detail	Failure details. The same information as the one reported by SNMP traps.

See the *Hitachi SNMP Agent User Guide* for reference codes and failure details.

Sending a test Syslog message

Procedure

1. Click the **Syslog** tab.

The **Syslog** tab displays the current settings for the primary and secondary servers.

2. Click **Send Test message to the Syslog Server**.

   A completion notice displays.
3. Click **OK** to acknowledge the notice and close the message.

Sending a test SNMP trap

Procedure

1. Click the **SNMP** tab.

   The **SNMP** tab displays the current settings for the storage system name, contact, location, SNMP trap, and SNMP manager.
2. Click **Send Test SNMP Trap**.

   A completion notice displays.
3. Click **OK** to acknowledge the notice and close the message.

5

Accessing a storage system

This section provides requirements and procedures to use Device Manager - Storage Navigator when the management software is not available to manage the storage system.

Accessing a storage system without the management software

You can use the administrator account created during the initial setup to temporarily use Device Manager - Storage Navigator to access the storage system. You can then perform critical storage management operations during a planned maintenance activity or an unexpected downtime on the management server.

Prerequisites

- You must have an administrator login account with the Storage Administrator (initial configuration) role. For information about creating user accounts, see User administration on page 59 in this manual, and the *Hardware Reference Guide* for your system model.
- Flash player must be configured on the client to use Device Manager - Storage Navigator.

Note: To obtain the administrator login information, contact Hitachi Data Systems customer support.

Procedure

1. Start a web browser and enter the following URL:

   `https://`*`IP-address-or-host-name-of-the-SVP`*`/sanproject/emergency.do`
2. The following actions might be required to open the login dialog box, depending on your environment:
   - If a message indicates that the enhanced security configuration is enabled on the computer, select **In the future, do not show this message** and click **OK**.
   - If the SVP is set to support SSL-encrypted communication and security messages appear, make sure the certificate is correct and follow the instructions in the dialog box.
   - If a messages indicates that certain web sites are blocked, make sure you have added the SVP to the trusted sites zone.
3. Enter a user ID and password for the account.
4. Click **Log In**.
5. If the Security Information dialog box appears, click **Yes**.
6. If an Adobe Flash Player local storage area pop-up dialog box appears, click **Allow** to open the Device Manager - Storage Navigator main window.

   The cache function of Flash Player optimizes the process of Device Manager - Storage Navigator. Denial of the request might reduce processing speed.

⚠ **Note:** If the login process fails three times with the same user ID, Device Manager - Storage Navigator will stop responding for one minute. This is for security purposes and is not a system failure. Wait, and then try again.

6

License keys

This storage system includes base and optional software features for Hitachi Virtual Storage Platform G200, G400, G600, G800 or Hitachi Virtual Storage Platform F400, F600, F800 storage systems that must be enabled by installing license keys. This section describes the types of available licenses, license capacity calculation, and instructions for installing, enabling, disabling, and uninstalling license keys.

Overview

When you install a license key, it is automatically enabled and the timer on the license starts at that time. To preserve time on a term key license, you can disable it without uninstalling it. When you need the software, enable the license again.

License key types

To use software, you must install the license key provided when you purchase that software.

You can use software with licensed capacity for a term key by installing a term key and overwriting a permanent key as long as the term key is valid. If the term key expires when the system is being used, and the capacity needed for the operation is insufficient, operations that you can perform are limited. In this case, a SIM that indicates the term key expiration (reference code 7ff7*xx*) is output on the Alerts tab in the Storage Systems window.

The following table describes the four types of license keys.

Type	Description	Effective term[1]	Estimating licensed capacity
Permanent	For purchase	No limit	Required
Term	For purchase	365 days	Required
Temporary	For trial use before purchase (try and buy)	120 days	Not required
Emergency	For emergency use	30 days	Not required

Notes:

1. When you log in to Device Manager - Storage Navigator, a warning message appears if 45 days or less remain before the expiration.

Using the permanent key

You can purchase the permanent key to use a software application indefinitely. You must estimate a licensed capacity required for using the software application and purchase a license key for the amount of the required capacity.

- If insufficient license capacity is installed, Not Enough License displays in the status field of the **License Keys** window, and the software application is not enabled.
- If the capacity of the usable volume exceeds the licensed capacity while the storage system is running, for example, an LDEV was additionally installed, Grace Period displays in the status field of the **License Keys** window. You can continue to perform the same operations, but the deficient amount of license must be purchased within 30 days.

Using the term key

You can purchase the term key to use the software application for a specific number of days. You must estimate a licensed capacity required for using the software application and purchase a license key for the amount of the required capacity.

- If insufficient license capacity is installed, Not Enough License or Grace Period displays in the status field of the **License Keys** window.
- You can enable or disable the term key for each software application. Unlike the temporary key and the emergency key, the number of days the term key is enabled is counted as the number of effective days of the term key rather than the number of elapsed days from the installation date.
- The number of effective days is decremented by one day when the date changes.
  For example, if the term key is set to be enabled for 150 days during installation and the term key is disabled for 100 days and a total of 250 days have elapsed since the installation, the number of remaining effective days of the term key is 215 days. This is determined by subtracting 150 days from 365 days. By disabling the term key on the days when the software application is not used, you can prevent the unnecessary shortening of the period in which the term key can be used.
- If the term key is expired, Not Installed displays in the status field of the **License Keys** window, and the software application is disabled.

Using the temporary key

You can use the temporary key for trial purposes. The effective term is 120 days from the time of installation of the temporary key. The effective term is not increased even if the temporary key is reinstalled during the effective term.

If you uninstall the temporary key, even though the effective term remains, Temporary is displayed in the status field, Not Installed is displayed in the Key Type field, and the remaining days of the effective term are displayed in the Term (Days) field of the **License Keys** window.

If the temporary key expires, you cannot reinstall the temporary key for 180 days. Expired displays in the status field of the **License Keys** window, and the software application is disabled.

Using the emergency key

You can use the emergency key if the license key cannot be purchased, or if an emergency occurs, such as a system failure or a communication error.

You can also use the emergency key if the configuration of the software application that is installed by the temporary key remains in the changed status and cannot be restored to the original status. For example, if you do not plan to purchase the software application after using the temporary key for trial purposes, you can restore the changed configuration to the original status by temporarily enabling the software application with the emergency key.

Caution:
- If an emergency key is installed for a software application for which a permanent or term key is installed, the effective term of the license key is 30 days. However, because the emergency key can be reinstalled during the effective term, the effective term can be restored to 30 days.
- In other scenarios, the emergency key can be installed only once.

Software packaging

The following table shows the software included for each software bundle:

Software bundle	Software
Hitachi Storage Virtualization Operating System (SVOS)	• Open Volume Management • LUN Manager[1] • Performance Monitor • Server Priority Manager[2] • HDvM/Device Manager - Storage Navigator • SNMP Agent • Data Retention Utility • Volume Shredder • JAVA API • Dynamic Provisioning[3] • Universal Volume Manager • Virtual Partition Manager • Resource Partition Manager
Hitachi Remote Replication	• TrueCopy[4] • Universal Replicator[5]
Hitachi Local Replication	• ShadowImage[4] • Thin Image[6]
Hitachi Command Suite Data Mobility	• Dynamic Tiering[7] • Volume Migration V2 • Active flash[9]
Hitachi Encryption Key[8]	• Encryption License Key
Hitachi Disaster Recovery Extended	Disaster Recovery Extended[10]
Global-active device	Global-active device[4]

Notes:
1. Includes LUN security function.
2. To use Server Priority Manager, you must install the Performance Monitor.
3. For VSP G400, G600, G800 or VSP F400, F600, F800, you must estimate the total pool capacity.
4. For VSP G800 or VSP F800, you must estimate the normal volume. If you are using a Dynamic Provisioning, active flash, or Dynamic Tiering V-VOL as a P-VOL or S-VOL, license

Software bundle	Software
capacity is calculated by using the capacity of pages allocated to the V-VOL (capacity which the pool uses). **5.** To use Universal Replicator, you must install TrueCopy. For VSP G800 or VSP F800, you must estimate the normal volume. For the normal volume, if you are using a Dynamic Provisioning, active flash, or Dynamic Tiering V-VOL as a P-VOL or S-VOL, license capacity is calculated by using the capacity of pages allocated to the V-VOL (capacity which the pool uses). **6.** To use Thin Image, you must install Dynamic Provisioning. For VSP G800 or VSP F800, you must estimate the combined capacity of normal volume and total pool capacity. For the normal volume, if you are using a Dynamic Provisioning, active flash, or Dynamic Tiering V-VOL as a P-VOL or S-VOL, license capacity is calculated by using the capacity of pages allocated to the V-VOL (capacity which the pool uses). **7.** To use Dynamic Tiering, you must install Dynamic Provisioning. For VSP G800 or VSP F800, you must estimate the total pool capacity. **8.** Supported for VSP G400, G600, G800 or VSP F400, F600, F800. **9.** To use active flash, you must install Dynamic Provisioning and Dynamic Tiering. For VSP G800, you must estimate the total pool capacity. **10.** To use Disaster Recovery Extended, you must install Universal Replicator.	

Note:
- Before using Volume Migration, contact Hitachi Data Systems customer support.
- A model upgrade license is required when upgrading from VSP G400 or VSP F400 to VSP G600 or VSP F600.

Estimating licensed capacity

The licensed capacity is volume capacity that you are licensed to use with the software application. You must estimate the amount of capacity that you want to use with the software application before you purchase the permanent key or the term key.

Software and licensed capacity

Three licensed capacity types are available. The one you choose depends on the software application. The following table describes the licensed capacity types:

Caution: If you use Dynamic Provisioning, the licensed capacity might become insufficient because the used capacity of Dynamic Provisioning pools could increase, even if you do not add any volumes. If this happens, you must purchase an additional license within 30 days to increase the capacity to match the new volume size. For instructions to calculate pool capacity, see the *Provisioning Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*.

Table 8 Licensed capacity types

Type	Description
Used capacity	The licensed capacity is calculated by using one of the following capacities: • Normal volumes (volumes) • External volumes mapped to the storage system • Pools
Mounted capacity/ usable capacity	The licensed capacity is estimated by using the capacity of all the volumes in the storage system.
Unlimited capacity	You can use the software regardless of the volume capacity.

Table 9 Software bundle licensed capacity

Software bundle	VSP G200	VSP G400, G600 or VSP F400, F600	VSP G800 or VSP F800
Hitachi Storage Virtualization Operating System (SVOS)	Unlimited	Mounted capacity	Mounted capacity
Hitachi Remote Replication	Unlimited	Mounted capacity	Used capacity
Hitachi Local Replication	Unlimited	Mounted capacity	Used capacity
Hitachi Command Suite Data Mobility	Unlimited	Mounted capacity	Used capacity
Hitachi Encryption Key	N/A	Unlimited	Unlimited
Hitachi Disaster Recovery Extended	Unlimited	Unlimited	Unlimited
Global-active device	Unlimited	Mounted capacity	Used capacity

Calculating licensed capacity for a normal volume

A normal volume is a volume that is not blocked or protected. The volume can be written to. The calculation of the normal volume capacity depends on the volume emulation type. Use the formula in the following table to estimate capacity for purchase. When you calculate the volume capacity, round the value up to the second decimal place.

Table 10 Formulas for calculating capacity of a normal volume

Volume emulation type	Formula for calculating capacity of a normal volume
3390-*x*[1]	870 KB × *number-of-user-cylinders*
OPEN-*x*[1]	Same as the capacity specified when creating the volume
Notes:	

Volume emulation type	Formula for calculating capacity of a normal volume
1. *x* indicates a number or a letter. For example, OPEN-*x* refers to emulation types such as OPEN-3 and OPEN-V.	

An example is shown in the following table.

Table 11 Example of calculating license capacity

Item	Value
Volume emulation type	3390-3
Number of user cylinders	3,339
Number of volumes	2,048
Total capacity of all the volumes	870 KB × 3,339 × 2,048 = 5,949,296,640 KB 5,949,296,640 KB / 1,024 = 5,809,860 MB 5,809,860 MB / 1,024 ≒ 5,673.70 GB 5,673.70 GB / 1,024 ≒ 5.55 TB
Estimated required capacity	At least 6 TB

Calculating licensed capacity for an external volume

Use the following equation to calculate the licensed capacity for an external volume:

```
External Volume Capacity (KB) = Volume Capacity (number of
blocks) X 512 (bytes) / 1,024
```

Calculating pool capacity

The license capacity of Dynamic Provisioning is calculated using the total capacity of the Dynamic Provisioning pool. If you use Dynamic Provisioning V-VOLs as P-VOLs or S-VOLs of ShadowImage, TrueCopy, Universal Replicator, or global-active device, the license capacity of ShadowImage, TrueCopy, Universal Replicator, or global-active device is calculated by using the page capacity allocated to the Dynamic Provisioning V-VOLs (that is, used pool capacity).

For more information on calculating pool capacity, see the *Provisioning Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*.

Cautions on license capacities in license-related windows

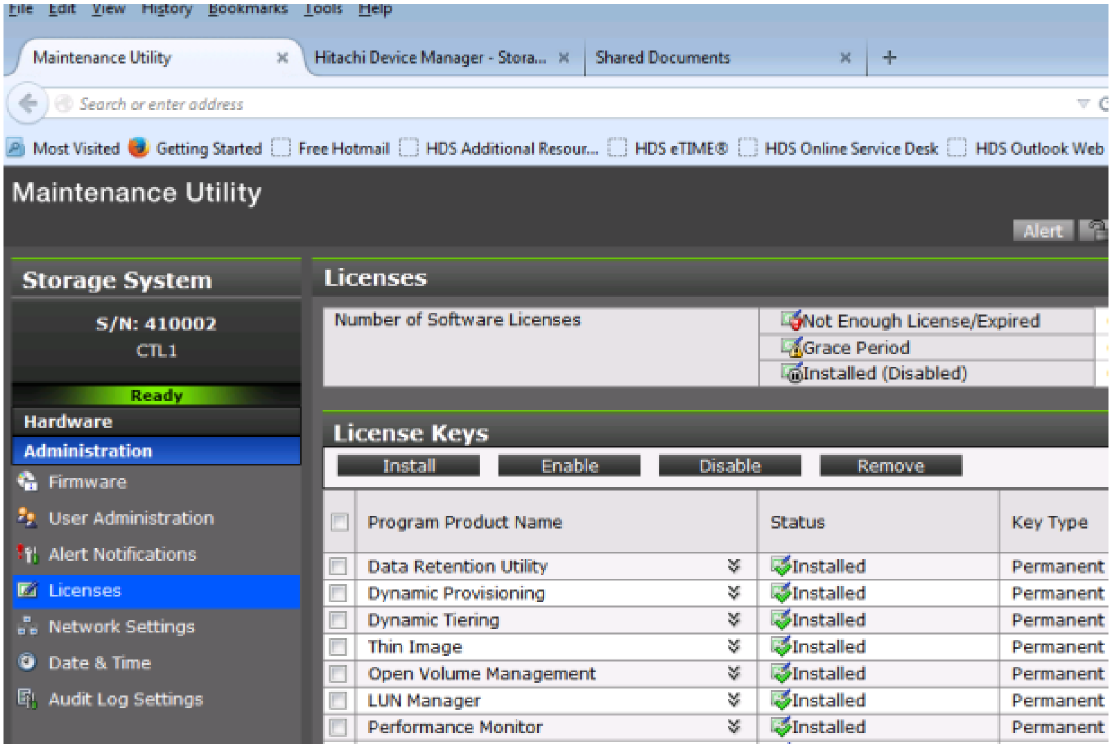
License capacities are displayed not only in license-related windows but also in the **Pools** window and the **Replication** window.

When you install or overwrite a temporary key or an emergency key for an installed software application, the license capacity before the overwrite installation is displayed as Permitted (TB) in license-related windows. However, Unlimited (license capacity for the temporary key or emergency key) is displayed as Licensed Capacity in the **Pools** window and the **Replication** window.

For example: You install a term key that has a license capacity of 5 TB for Compatible FlashCopy®, and when the term expires, you use an emergency key. In license-related windows, 5 TB is displayed in the Permitted (TB) field. However, in the **Licensed Capacity** field in a **Replication** window, Unlimited (capacity of the emergency key) is displayed.

Managing licenses

Use the Licenses window to install and uninstall license keys.



Number of Software Licenses	
	Not Enough License/Expired
	Grace Period
	Installed (Disabled)

□	Program Product Name	Status	Key Type
□	Data Retention Utility	Installed	Permanent
□	Dynamic Provisioning	Installed	Permanent
□	Dynamic Tiering	Installed	Permanent
□	Thin Image	Installed	Permanent
□	Open Volume Management	Installed	Permanent
□	LUN Manager	Installed	Permanent
□	Performance Monitor	Installed	Permanent

Related concepts

- When the status is Installed (Disabled) on page 109

Related tasks

- Installing licenses on page 109
- Enabling a license on page 109
- Disabling a license on page 110
- Removing a software license on page 111

Related references

- Examples of license information on page 110

Installing licenses

Prerequisites
You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. In the maintenance utility **Administration** tree, select **Licenses.**
2. Select whether to enter a key code or specify a license key file.
   - **Key Code**: Enter a key code to install the software. In **Key Code**, enter the license key code for the software.
   - **File**: Specify a license key file to install the software. Click **Browse** and specify the license key file. You can use a file name of up to 200 alphanumeric characters excluding these symbols: (" \ : ; , * ? < > | /). Include the .plk file extension.
3. Click **Apply.**

Related concepts

- When the status is Installed (Disabled) on page 109

Enabling a license

You can enable a license that is in disabled status.

Prerequisites
You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. From the **Maintenance Utility** menu, click **License Keys** to open the **License Keys** window.
2. Select the license to enable. You can select from one to all of the licenses listed in the window at the same time.
3. Click **Enable** to display the **License Keys** window.
4. Check the settings and click **Apply.**

When the status is Installed (Disabled)

If you do not install the prerequisite software before you install the license key software, the software will install correctly but will be disabled. To enable a license key, install the prerequisite software, and then enable the key.

Related tasks

- Installing licenses on page 109

Examples of license information

The following table provides examples of license information displayed in the **License Keys** table of the maintenance utility.

License key status (example)	Status	Key type	Licensed capacity	Term (Days)
Not installed	Not installed	blank	Blank	Blank
Installed with the permanent key	Installed	permanent	Permitted	-
Installed with the term key and set to Enabled	Installed	term	Permitted	Number of remaining days before expiration
Installed with the term key and set to Disabled	Installed (Disabled)	term	Permitted	-
Installed with the temporary key.	Installed	temporary	-	Number of remaining days before expiration
Installed with the emergency key.	Installed	emergency	-	Number of remaining days before expiration
A temporary key was installed, but has expired.	Expired	temporary	-	Number of remaining days before expiration
A term key or an emergency key was installed, but has expired.	Not installed	blank	Blank	Blank
Installed with the permanent key or the term key, but the licensed capacity was insufficient.	Not Enough License	permanent or term	Permitted and Used	-
Installed with the permanent or term key, and then LDEVs are added, but the license capacity was insufficient.	Grace Period	permanent or term	Permitted and Used	Number of remaining days before expiration
Installed with the temporary key, and then reinstalled with the permanent key, but the license capacity was insufficient.	Installed	temporary	Permitted and Used	Number of remaining days before expiration
Installed with the permanent or term key, then reinstalled with the emergency key.	Installed	emergency	Permitted and Used	Number of remaining days before expiration

Disabling a license

You can disable a license that is in enabled status.

Prerequisites

You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. From the **Maintenance Utility** menu, click **License Keys** to open the **License Keys** window.
2. Select the license to disable. You can select from one to all of the licenses listed in window the at the same time.
3. Click **Disable** to display the **License Keys** window.
4. Click **Finish**.
5. Check the settings and click **Apply**.

Removing a software license

You can remove a software license that is in disabled status.

Prerequisites

You must have the Storage Administrator (Initial Configuration) role to perform this task.

Procedure

1. In the maintenance utility **Administration** tree, click **License Keys**.
2. In the **License Keys** window, select the license to uninstall. You can select from one to all of the licenses listed in the window at the same time.
3. In the **License Keys** window, click **Uninstall Licenses**.
4. Check the settings and click **Apply**.

   On rare occasions, a software option that is listed as Not Installed but still has available licensed capacity (shown as XX TB) might remain in the list. In this case, select that option and uninstall the software.

   Note: To reinstall a license key after uninstalling it, contact Hitachi Data Systems customer support to reissue the license key file.

Related tasks

- Removing a Data Retention Utility license on page 111

Removing a Data Retention Utility license

Caution: When you remove a Data Retention Utility license, an error might occur, even if the Permitted Volumes column of the **License Keys** window indicates that the licensed capacity is 0 TB.

Procedure

1. Click **Actions > Other Function > Data Retention** to open the **Data Retention** window.
2. In the **Data Retention** window, find logical volumes that are unusable as S-VOLs.
3. Change the settings so that the logical volumes are usable as S-VOLs.
4. Uninstall the Data Retention Utility.

License key expiration

If the license key for software-A expires, the license key for software-B is also disabled if software-B requires an enabled software-A. In this scenario, Installed (Disabled) is shown for software-B in the Status column of the **License Keys** table. After that, when you re-enable software-A, software-B is also re-enabled. If the Status column for software-B continues to display Installed (Disabled), go to the **License Keys** table and manually change the status of software-B back to Installed.

After your license key expires, no new configuration settings can be made, and no monitoring functions can be used with Performance Monitor. Configuration settings made before the expiration of the license key remain in effect. You can cancel configuration changes for some software.

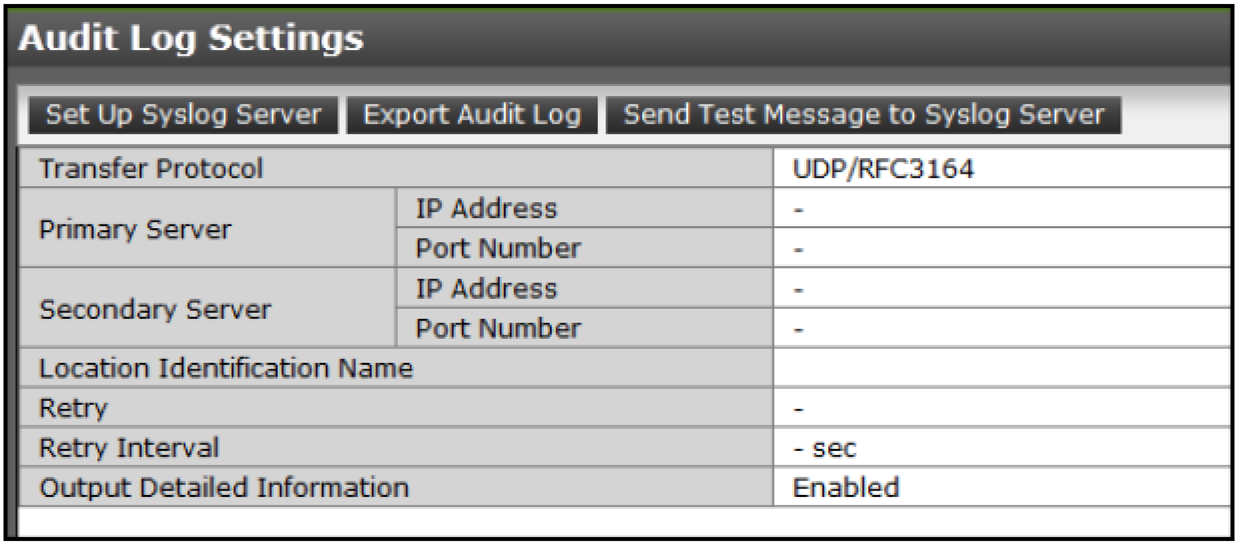
7

Configuring audit logs

This section provides procedures to change the audit log settings in the maintenance utility.

Audit log settings

This section provides the procedures to configure the audit log settings.



Transfer Protocol		UDP/RFC3164
Primary Server	IP Address	-
	Port Number	-
Secondary Server	IP Address	-
	Port Number	-
Location Identification Name		
Retry		-
Retry Interval		- sec
Output Detailed Information		Enabled

The **Audit Log Settings** window shows the current audit log settings. Select one of more of the three tabs to change the settings.

Related tasks

- Setting up a syslog server on page 114
- Exporting an audit log on page 115
- Sending a test Syslog message on page 95

Setting up a syslog server

Prerequisites

You must have the Audit Log Administrator (View & Modify) role to perform this task.

Procedure

1. In the maintenance utility **Administration** tree, select **Audit Log Settings**.
2. Click **Set Up Syslog Server**.
3. Select the desired **Transfer Protocol**.
4. Enable or disable the **Primary Server**.
5. Enable or disable the **Secondary Server**.
6. Enable or disable the **Output Detailed Information**.
7. Click **Apply** to save the settings or **Cancel** to close the window without saving the settings.

Exporting an audit log

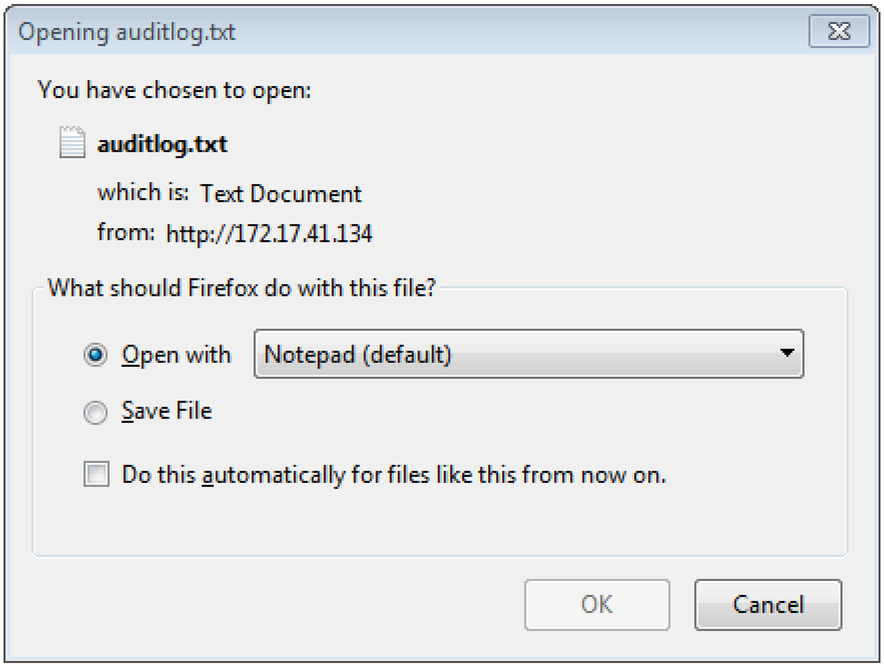
Use the following procedure to send a display an audit log file on the screen or to save it to a file on the SVP or your laptop.

Prerequisites

You must have the Audit Log Administrator (View Only) role to perform this task.

Procedure

1. In the maintenance utility **Administration** tree, select **Audit Log Settings**.
2. Click **Export Audit Log**.



Opening auditlog.txt

You have chosen to open:

auditlog.txt

which is: Text Document

from: http://172.17.41.134

What should Firefox do with this file?

● Open with Notepad (default)

○ Save File

□ Do this automatically for files like this from now on.

3. To open the file without saving, click **Open with** and then use the pull-down menu to select the software application to use to open the file.
4. Click **OK**. The auditlog.txt file is displayed.
5. To save the file, click **Save File**.
6. To use one of the two settings in steps 3 through 5 when you export an another auditlog.txt file, click **Do this automatically for files like this from now on**.
7. Click **OK**.
8. Browse to the directory where you want to save the file. Use the default file name auditlog.txt or change the file name as desired.

   Click **Save**. The file is saved and the dialog box closes.

9. Browse to the directory where you want the file. Use the default file name auditlog.txt or change the file name as desired.
10. Click **Save**. The file auditlog.txt file is saved.

Send test message to syslog server

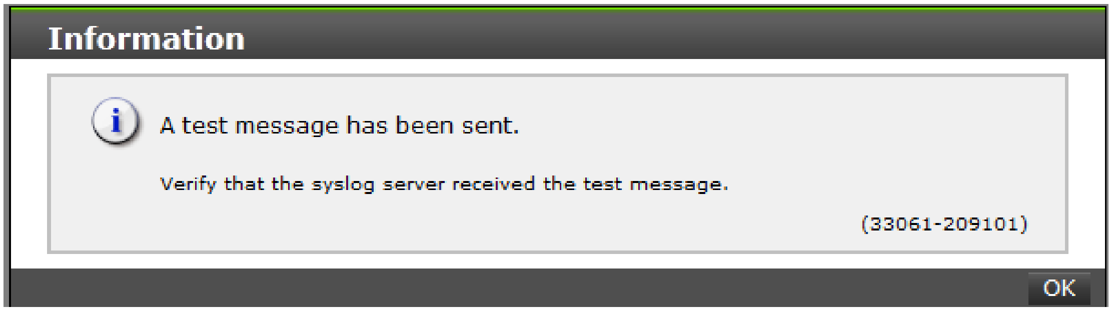
Use the following procedure to send a test audit log message to the syslog server.

Prerequisites

You must have the Audit Log Administrator (View Only) role to perform this task.

Procedure

1. In the maintenance usage **Administration** tree, select **Audit Log Settings**.
2. Click **Send Test Message to Syslog Server**. The following message box opens:



Information

A test message has been sent.

Verify that the syslog server received the test message.

(33061-209101)

3. Click **OK** to close the message box. Check the syslog server messages and verify that the test message was received and is on the server.

8

Managing storage system reports

This section describes the procedures to create storage configuration reports and view them. It includes examples of the three types of reports.

About storage system reports

Device Manager - Storage Navigator can generate a standard set of reports that provide views of various aspects of the storage system. In addition to these views, you can generate custom reports for specific areas of the system. These include a summary of the system data and configuration, ports, channel adapters, and disk adapters. You can save reports in CSV files or HTML files. Tables in the HTML version of the configuration reports are sortable.

Before making changes to a storage system, create reports of your storage system's physical configurations and logical settings. Make a similar report after the changes, and then compare the reports to verify that new settings were made as intended.

Viewing a Device Manager - Storage Navigator report

Prerequisites

- Adobe Flash Player must be installed.
- Users can view the reports that they created.
- Users that have the Storage Administrator (Initial Configuration) role can view all reports.

Procedure

1. Expand the **Storage Systems** tree, and then click **Reports**.
2. Specify the report to download.
3. Click **Download Reports**.
4. Specify a folder in which to save a `.tgz` file.
5. Extract the downloaded `.tgz` file.
6. Display the report.

   For HTML reports:

   Open the file *extracted-folder*`\html\index.html`.

   For CSV reports:

   Open a CSV file in the folder *extracted-folder*`\csv`.

Viewing a report in the Reports window

You can view only HTML format reports in the **Reports** window. You can view CSV format reports in the previous procedure.

Procedure

1. Expand the **Storage Systems** tree, and then click **Reports**.

2. Click the name of the report to display.

   The report is displayed in the **Reports** window.
3. In the **Reports** window, click the name of the report in the list at the left, and then view the report at the right.

Creating a configuration report

You can use the report configuration tool to create up to 20 configuration reports and then view or download them.

Prerequisites

You must have Storage View permission to perform this task.

Procedure

1. From **General Tasks**, click **Create Configuration Report**.
2. Specify a task name and click **Apply**. This task name is used as the report name in the **Reports** window. This process takes approximately 10 minutes to complete.
3. Click **Refresh** to update the **Reports** window. The created report appears in the list.

Deleting a configuration report

You can delete a report when you no longer need it, or to make room in the **Reports** window when the number of reports is near the limit.

Prerequisites

Users that create the report or users with Storage Administrator (Initial Configuration) role can delete a configuration report.

Procedure

1. Expand the **Storage Systems** tree, and then click **Reports**.
2. Select the report to delete.
3. Click **Delete Reports**.
4. Click **Apply**.

Collecting dump files using the Dump tool

Use the Dump tool to download dump files onto a Device Manager - Storage Navigator computer. The downloaded dump files can be used to:

- Troubleshoot the system. Use the Dump tool to download dump files from the SVP and give it to the HDS support personnel.

- Check system configuration. First click File > Refresh All to update the configuration information, and then use the Dump tool to download the dump files.

There are two types of dump files:

- Normal Dump includes all information about the SVP and the minimum information about the storage system. Select this when you have a less serious problem such as incorrect display.
- Detail Dump includes all information about the SVP and the storage system. Select this when Device Manager - Storage Navigator has a serious problem (for example, Device Manager - Storage Navigator does not start) or when you need to determine if the storage system has a problem.

Prerequisites

- You must be logged into the SVP.
- All other users (including the SVP user) must stop using the Dump tool.
- Stop all maintenance operations.

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Open a Windows command prompt with administrator permissions.
3. Move the current directory to the folder where the tool is available. (For example: `<`*`SVP-root-directory`*`>\DKC200\mp\pc)`.
4. Specify the output destination of the dump file and execute `Dump_Detail.bat` or `Dump_Normal.bat`.

   For example, if you are storing the result of `Dump_Detail.bat` to `C:\Result`, enter the following:

   ```
   Dump_Detail.bat C:\Result
   ```
5. A completion message box displays. Press any key to acknowledge the message and close the message box.
6. Close the Windows command prompt.

A

Report Configuration Tool command reference (raidinf commands)

This section describes the `raidinf` commands, symbols, and reports used in Device Manager - Storage Navigator.

raidinf command list and command description

The following table lists the `raidinf` commands and symbols.

Table 12 raidinf command list

Command	Description
`raidinf -login`	Log in to Device Manager - Storage Navigator.
`raidinf add report`	Creates a report.
`raidinf delete report`	Deletes a report.
`raidinf download report`	Downloads a report.
`raidinf get reportinfo`	Displays a list of reports.
`raidinf -logout`	Log out of Device Manager - Storage Navigator.
`raidinf -h`	Displays the raidinf command syntax.

Table 13 Conventions of the command format

Symbol	Description
< >	The item enclosed in this symbol is variable.
| Vertical bar	Symbol is placed between multiple items to indicate "or". For example: `-A	-B` Specifies -A or -B.
[ ] Square brackets	The enclosed item can be omitted. If some items are delimited by the vertical bar, specify one item or omit all items. For example: `[ -A ]` Specifies nothing or specifies -A. `[-a	-b]` Specifies nothing or specifies -a or -b.
{ } Curly brackets	The meaning differs, depending on the enclosed item. • If items in curly brackets are delimited by vertical bars, one of the items must be specified. For example: `{-A	-B |-C }` Specifies -A, -B, or -C. • If curly brackets enclose items enclosed by square brackets, at least one of the items must be specified. For example: `{[-A][-B][-C]}` Specifies one or more items from -A, -B, or -C.

raidinf -login

Syntax

```
raidinf -login <user_name> <password> -servername <hostname/
ipaddress> [-port <port>]
```

Options and parameters

Option	Description
`-login [<user_name> <password>]`	Executes a user authentication for Device Manager - Storage Navigator. Specifies a user name and a password. The user is logged out automatically three minutes (180 seconds) after the last command is entered.
`-servername <hostname/ ipaddress>`	Specifies the host name or IP address of the SVP.
`[-port <port>]`	If you have changed the TCP port number for raidinf, specify the new TCP port number. If omitted, TCP port number will perform by specifying the initial value (5443). For operations after login (such as report creation), the port number used for login will be used. Therefore, specifying the port number will not be necessary for the operations after login.

Examples

This example authenticates `user01` using the password `xxxxxx`:

```
# raidinf -login user01 xxxxxx -servername svp.xxx.co.jp
```

This example authenticates `user01` using the password `xxxxxx` with TCP port number 6443:

```
# raidinf -login user01 xxxxxx -servername svp.xxx.co.jp -port
6443
```

raidinf add report

The `raidinf add report` command creates a report.

If other users have created 20 reports, the logged in user cannot create a report and will receive an error.

Syntax

```
raidinf add report -servername <hostname/ipaddress> [-report
<report_name>]
```

Options and parameters

Option	Description
-servername <*hostname*/ *ipaddress*>	Specifies the host name or IP address of the SVP.
[-report <*report_name*>]	Specifies a report name, up to 32 characters. All characters exceeding 32 are ignored. If the report name is omitted, the default report name *YYMMDD*-CreateConfigurationReport is specified. A hyphen cannot be specified at the beginning of the report name.

Examples

The following example creates a report with the default report name:

```
# raidinf add report -servername 10.213.74.121

ReportName                        UserName   CreateTime
101009-CreateConfigurationReport user01     2010/10/09-12:43:10
```

The following example creates a report named 101009-CreateConfigurationReport:

```
# raidinf add report -servername 10.213.74.121 -report 101009-
CreateConfigurationReport

ReportName                        UserName   CreateTime
101009-CreateConfigurationReport user01     2010/10/09-12:43:10
```

The following items are output:

- ReportName

  The report name is displayed (up to 32 characters).
- UserName

  The user name is displayed (up to 16 characters). If the user name exceeds 16 characters, an ellipsis (...) is displayed.
- CreateTime

  The time of creating a report is displayed (up to 19 characters).

raidinf delete report

The raidinf delete report command deletes a report.

If multiple reports of the same name exist, the command deletes the oldest report. If the specified report does not exist, the command does nothing, and terminates normally.

Reports created using Device Manager - Storage Navigator can also be deleted.

Syntax

```
raidinf delete report -servername <hostname/ipaddress>
{-report<report_name> | -report_id
 <report_id>} [-fill]
```

Options and parameters

Option	Description
-servername <*hostname/ ipaddress*>	Specifies the host name or the IP address of the SVP.
{-report <*report_name*> | -report_id <*report_id*>}	Specifies either -report or -report_id. • -report specifies a report name, up to 32 characters. All characters exceeding 32 are ignored. • -report_id specifies a report ID in the report list. Because each report has a unique ID, you can identify a specific report, even if the report list contains multiple reports with the same name.
[-fill]	Deletes a report only if there are already 20 reports in the queue. If there are fewer than 20 reports, the specified report is not deleted.

Examples

The following example deletes the report named 101009-CreateConfigurationReport:

```
# raidinf delete report -servername 10.213.74.121 -report 101009-
CreateConfigurationReport
```

101009-CreateConfigurationReport is deleted from the SVP.

raidinf download report

The raidinf download report command downloads a report.

Reports created by Device Manager - Storage Navigator can also be downloaded. The report in process of creation cannot be downloaded.

The name of the downloaded file is Report_*report name*.tgz. The files are overwritten if reports of the same name has already existed.

Example: the name of the downloaded file when the report name is 110309-CreateConfigurationReport

Report_110309-CreateConfigurationReport.tgz

Syntax

```
raidinf download report -servername <hostname/ipaddress>
  {-report <report_name> | -report_id <report_id>}
 -targetfolder <folder>
```

Options and parameters

Option	Description
`-servername <hostname/ ipaddress>`	Specifies the host name or the IP address of the Web server (SVP).
`{-report <report_name> | -report_id <report_id>}`	Specifies either `-report` or `-report_id`. • `-report` specifies a report name, up to 32 characters. All characters exceeding 32 are ignored. If the special name `LatestReport` is specified as a report name, the most recently created report is downloaded. To download another report that has the same name as `LatestReport`, specify the report ID for this report in `-report_id`. If multiple reports have the same name, the most recent report is replaced when a new report is downloaded. • `-report_id` specifies a report ID in the report list. Because each report has a unique ID, you can identify a specific report, even if the report list contains multiple reports with the same name.
`-targetfolder <folder>`	Specifies a folder name to which a report is downloaded. The folder whose name you specify must already exist, and you must have write permissions to the folder.

Examples

The following example shows how to download the most recent report:

```
# raidinf download report -servername 10.213.74.121
 -report LatestReport -targetfolder C:\tmp
```

`Report_101009-CreateConfigurationReport.tgz` is downloaded to `C:\tmp`.

The following example shows how to download the report named `101009-CreateConfigurationReport`:

```
# raidinf download report -servername 10.213.74.121
 -report 101009-CreateConfigurationReport -targetfolder C:\tmp
```

`Report_101009-CreateConfigurationReport.tgz` is downloaded to `C:\tmp`.

raidinf get reportinfo

The `raidinf get reportinfo` command displays a list of reports.

Reports created using Device Manager - Storage Navigator are also displayed. A report currently being created cannot be downloaded.

Syntax

```
raidinf get reportinfo -servername <hostname/ipaddress>
```

Options and parameters

Option	Description
-servername <*hostname/ ipaddress*>	Specifies the host name or IP address of the web server.

Examples

The following example displays a list of reports:

```
# raidinf get reportinfo -servername 10.213.74.121

ReportName                          UserName   CreateTime   ReportID
101009-CreateConfigurationReport user01     2010/10/09-12:43:10
33S3
101008-CreateConfigurationReport user01     2010/10/08-11:22:31
33J3
101007-CreateConfigurationReport user01     2010/10/07-11:17:20
2344
101006-CreateConfigurationReport configuration...
2010/10/06-15:30:42 4n1j
```

The following items are output:

- `ReportName`

  The report name is displayed. It can contain up to 32 characters.
- `UserName`

  A user name is displayed. It can contain up to 16 characters. If the user name exceeds 16 characters, an ellipsis (...) is displayed.
- `CreateTime`

  The time of creating the report is displayed. It can contain up to 19 characters.
- `ReportID`

  The report ID is displayed.

raidinf -logout

The `raidinf -logout` command is used for logging out from Device Manager - Storage Navigator.

Syntax

`raidinf -logout -servername <`*`hostname/ipaddress`*`>`

Options and parameters

Option	Description
-logout	Log out from Device Manager - Storage Navigator.

Option	Description
`-servername <`*`hostname/ ipaddress`*`>`	Specifies the host name or the IP address of the SVP.

Example

```
# raidinf -logout -servername mapp.xxx.co.jp
```

raidinf -h

The `raidinf -h` command is used to display the syntax..

Syntax

```
raidinf -h
```

Options and parameters

Option	Description
`-h`	Displays the raidinf help.

B

Storage configuration reports

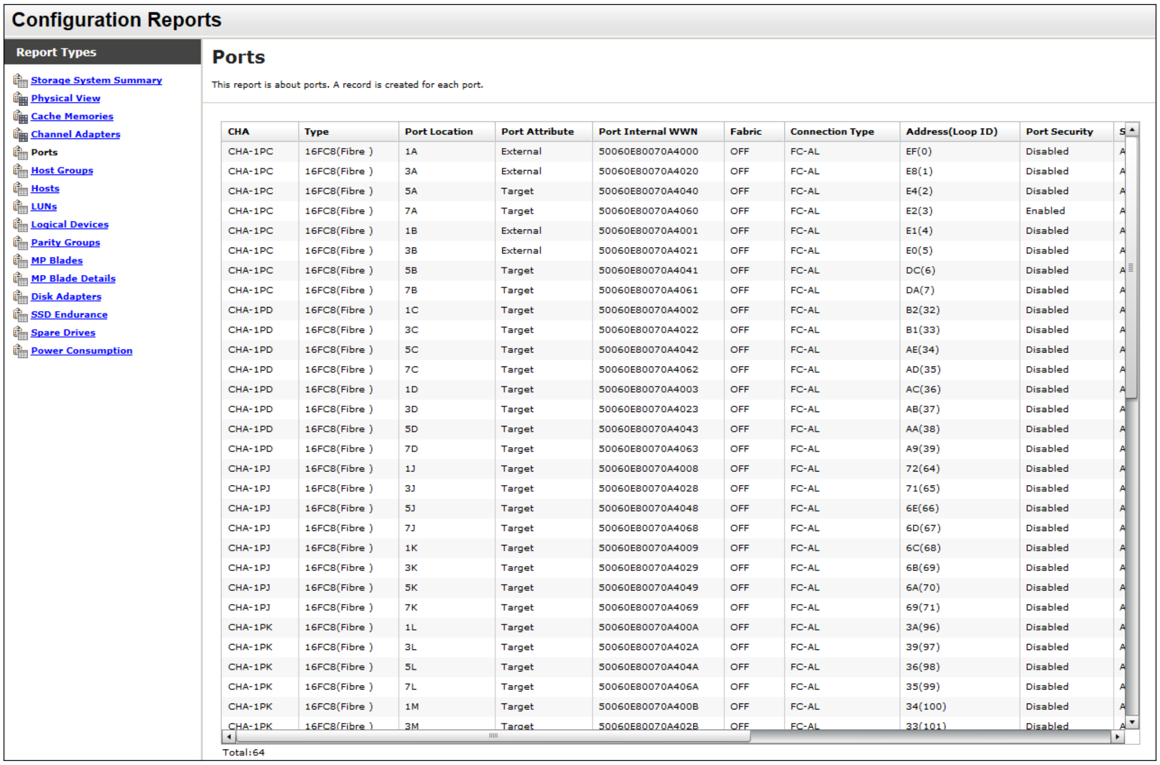
This section describes the configuration reports you can generate in Device Manager - Storage Navigator. They are grouped in this appendix according to the way they display: in tables, graphs, or CSV files.

To create, download, and delete reports, see Viewing a Device Manager - Storage Navigator report on page 118.

Reports in table view

Some Device Manager - Storage Navigator reports appear in table format.

The following figure provides examples of reports in table format. The 🗐 icons are displayed before the names of the reports in table view. If the icons are not displayed correctly, update the window.



Configuration Reports

Report Types

- Storage System Summary
- Physical View
- Cache Memories
- Channel Adapters
- Ports
- Host Groups
- Hosts
- LUNs
- Logical Devices
- Parity Groups
- MP Blades
- MP Blade Details
- Disk Adapters
- SSD Endurance
- Spare Drives
- Power Consumption

Ports

This report is about ports. A record is created for each port.

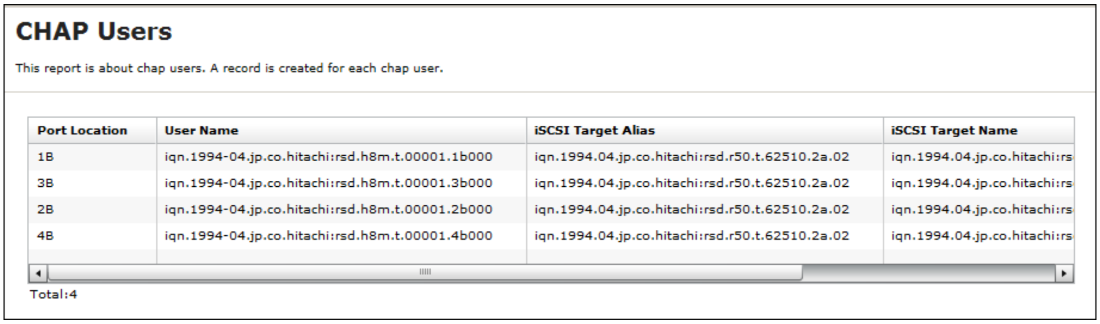
CHA	Type	Port Location	Port Attribute	Port Internal WWN	Fabric	Connection Type	Address(Loop ID)	Port Security	S
CHA-1PC	16FC8(Fibre)	1A	External	50060E80070A4000	OFF	FC-AL	EF(0)	Disabled	A
CHA-1PC	16FC8(Fibre)	3A	External	50060E80070A4020	OFF	FC-AL	E8(1)	Disabled	A
CHA-1PC	16FC8(Fibre)	5A	Target	50060E80070A4040	OFF	FC-AL	E4(2)	Disabled	A
CHA-1PC	16FC8(Fibre)	7A	Target	50060E80070A4060	OFF	FC-AL	E2(3)	Enabled	A
CHA-1PC	16FC8(Fibre)	1B	External	50060E80070A4001	OFF	FC-AL	E1(4)	Disabled	A
CHA-1PC	16FC8(Fibre)	3B	External	50060E80070A4021	OFF	FC-AL	E0(5)	Disabled	A
CHA-1PC	16FC8(Fibre)	5B	Target	50060E80070A4041	OFF	FC-AL	DC(6)	Disabled	A
CHA-1PC	16FC8(Fibre)	7B	Target	50060E80070A4061	OFF	FC-AL	DA(7)	Disabled	A
CHA-1PD	16FC8(Fibre)	1C	Target	50060E80070A4002	OFF	FC-AL	B2(32)	Disabled	A
CHA-1PD	16FC8(Fibre)	3C	Target	50060E80070A4022	OFF	FC-AL	B1(33)	Disabled	A
CHA-1PD	16FC8(Fibre)	5C	Target	50060E80070A4042	OFF	FC-AL	AE(34)	Disabled	A
CHA-1PD	16FC8(Fibre)	7C	Target	50060E80070A4062	OFF	FC-AL	AD(35)	Disabled	A
CHA-1PD	16FC8(Fibre)	1D	Target	50060E80070A4003	OFF	FC-AL	AC(36)	Disabled	A
CHA-1PD	16FC8(Fibre)	3D	Target	50060E80070A4023	OFF	FC-AL	AB(37)	Disabled	A
CHA-1PD	16FC8(Fibre)	5D	Target	50060E80070A4043	OFF	FC-AL	AA(38)	Disabled	A
CHA-1PD	16FC8(Fibre)	7D	Target	50060E80070A4063	OFF	FC-AL	A9(39)	Disabled	A
CHA-1PJ	16FC8(Fibre)	1J	Target	50060E80070A4008	OFF	FC-AL	72(64)	Disabled	A
CHA-1PJ	16FC8(Fibre)	3J	Target	50060E80070A4028	OFF	FC-AL	71(65)	Disabled	A
CHA-1PJ	16FC8(Fibre)	5J	Target	50060E80070A4048	OFF	FC-AL	6E(66)	Disabled	A
CHA-1PJ	16FC8(Fibre)	7J	Target	50060E80070A4068	OFF	FC-AL	6D(67)	Disabled	A
CHA-1PJ	16FC8(Fibre)	1K	Target	50060E80070A4009	OFF	FC-AL	6C(68)	Disabled	A
CHA-1PJ	16FC8(Fibre)	3K	Target	50060E80070A4029	OFF	FC-AL	6B(69)	Disabled	A
CHA-1PJ	16FC8(Fibre)	5K	Target	50060E80070A4049	OFF	FC-AL	6A(70)	Disabled	A
CHA-1PJ	16FC8(Fibre)	7K	Target	50060E80070A4069	OFF	FC-AL	69(71)	Disabled	A
CHA-1PK	16FC8(Fibre)	1L	Target	50060E80070A400A	OFF	FC-AL	3A(96)	Disabled	A
CHA-1PK	16FC8(Fibre)	3L	Target	50060E80070A402A	OFF	FC-AL	39(97)	Disabled	A
CHA-1PK	16FC8(Fibre)	5L	Target	50060E80070A404A	OFF	FC-AL	36(98)	Disabled	A
CHA-1PK	16FC8(Fibre)	7L	Target	50060E80070A406A	OFF	FC-AL	35(99)	Disabled	A
CHA-1PK	16FC8(Fibre)	1M	Target	50060E80070A400B	OFF	FC-AL	34(100)	Disabled	A
CHA-1PK	16FC8(Fibre)	3M	Target	50060E80070A402B	OFF	FC-AL	33(101)	Disabled	A

Total:64

- To sort data in table reports, click any column header.
- While a table is reading a large amount of data, the table columns cannot be manipulated, sorted, or resized. However, you can view previously displayed items, select rows, and scroll.

CHAP Users report

The following illustration shows an example of a CHAP Users report. The table following the illustration describes the items in the report.



CHAP Users

This report is about chap users. A record is created for each chap user.

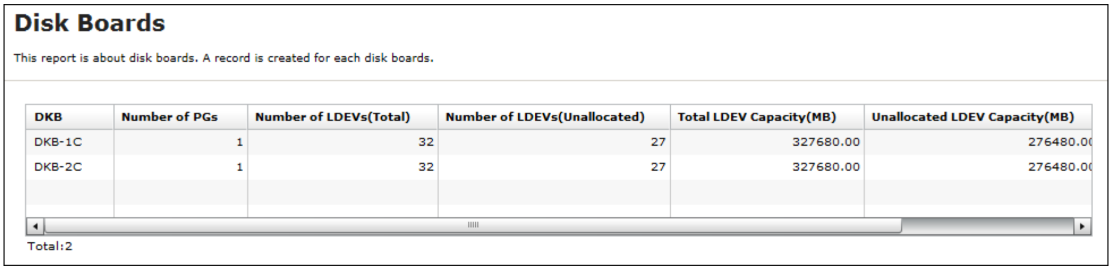
Port Location	User Name	iSCSI Target Alias	iSCSI Target Name
1B	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000	iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02	iqn.1994.04.jp.co.hitachi:rs
3B	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.3b000	iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02	iqn.1994.04.jp.co.hitachi:rs
2B	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.2b000	iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02	iqn.1994.04.jp.co.hitachi:rs
4B	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.4b000	iqn.1994.04.jp.co.hitachi:rsd.r50.t.62510.2a.02	iqn.1994.04.jp.co.hitachi:rs

Total:4

Item	Description
Port Location	Name of the port
User Name	Name of the CHAP user for authentication
iSCSI Target Alias	Alias of the iSCSI target
iSCSI Target Name	Name of the iSCSI target

Disk Boards report

The following illustration shows an example of a Disk Boards report. The table following the illustration describes the items in the report.



Disk Boards

This report is about disk boards. A record is created for each disk boards.

DKB	Number of PGs	Number of LDEVs(Total)	Number of LDEVs(Unallocated)	Total LDEV Capacity(MB)	Unallocated LDEV Capacity(MB)
DKB-1C	1	32	27	327680.00	276480.0(
DKB-2C	1	32	27	327680.00	276480.0(

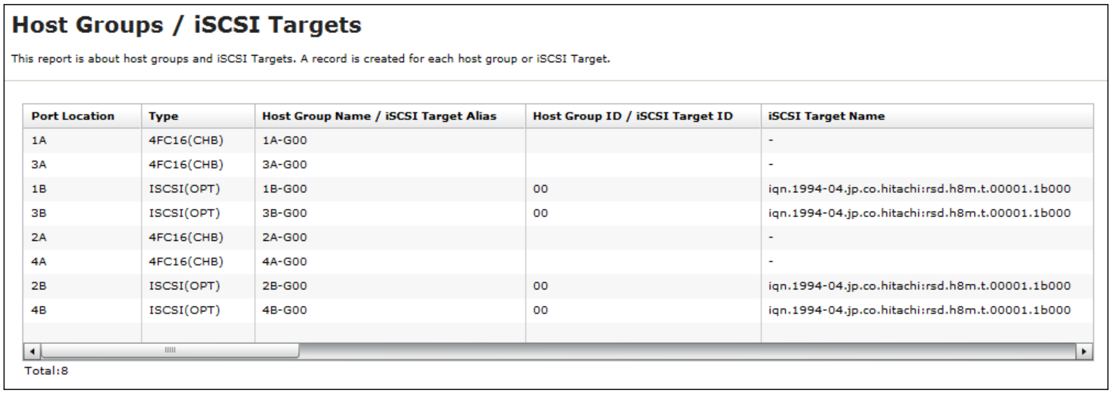
Total:2

Item	Description
DKB	Location of the disk board. • "External" is displayed when the storage system has an external storage system. • "External (FICON DM)" is displayed when the storage system has volumes for FICON DM.
Number of PGs	The number of the parity groups that the disk board controls. • If "DKB" is "External", this item indicates the number of parity groups mapped to external volumes. • If "DKB" is "External (FICON DM)", this item indicates the number of parity groups mapped to volumes for FICON DM.
Number of LDEVs (Total)	The number of the logical volumes belonging to the parity groups that the disk board controls.

Item	Description
Number of LDEVs (Unallocated)	The number of the logical volumes that are inaccessible from the host and belong to the parity groups controlled by the disk board.
Total LDEV Capacity (MB)	Total capacity of the logical volumes belonging to the parity groups that the disk board controls.
Unallocated LDEV Capacity (MB)	Total capacity of the logical volumes that are inaccessible from the host and belong to the parity groups controlled by the disk board.

Host Groups / iSCSI Targets report

The following illustration shows an example of a Host Groups / iSCSI Targets report. The table following the illustration describes the items in the report.



Host Groups / iSCSI Targets

This report is about host groups and iSCSI Targets. A record is created for each host group or iSCSI Target.

Port Location	Type	Host Group Name / iSCSI Target Alias	Host Group ID / iSCSI Target ID	iSCSI Target Name
1A	4FC16(CHB)	1A-G00		-
3A	4FC16(CHB)	3A-G00		-
1B	ISCSI(OPT)	1B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
3B	ISCSI(OPT)	3B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
2A	4FC16(CHB)	2A-G00		-
4A	4FC16(CHB)	4A-G00		-
2B	ISCSI(OPT)	2B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
4B	ISCSI(OPT)	4B-G00	00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000

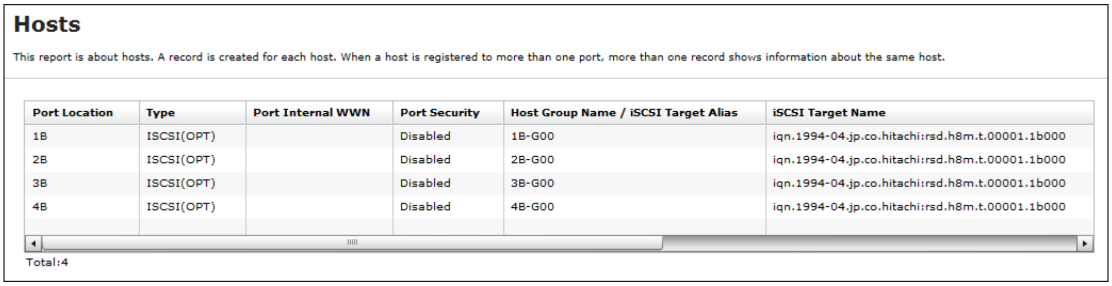
Total:8

Item	Description
Port Location	Name of the port
Type	Type of the host group
Host Group Name / iSCSI Target Alias	Name of the host group / alias of the iSCSI target
Host Group ID / iSCSI Target ID	Number of the host group / ID of the iSCSI target
iSCSI Target Name	Name of the iSCSI target
Resource Group Name	Resource Group Name where the host group belongs
Resource Group ID	Resource Group ID where the host group belongs
Number of LUNs	The number of LU paths defined to the host group
Number of LDEVs	The number of logical volumes that are accessible from the hosts in the host group
Number of PGs	The number of parity groups with logical volumes that are accessible from the hosts in the host group
Number of DKBs	The number of disk boards controlling the parity groups where the logical volumes that are accessible from the hosts in the host group belong

Item	Description
Total LDEV Capacity (MB)	Total capacity of the logical volumes accessible from the hosts in the host group. This is the total capacity of LDEVs referred to in "Number of LDEVs".
Port Security	Security of the port
Authentication : Method	iSCSI target method authentication settings • CHAP • None • Comply with Host Setting
Authentication : Mutual CHAP	Enable or disable the iSCSI target mutual CHAP • Enabled • Disabled
Authentication : User Name	Authenticated iSCSI target user name
Authentication : Number of Users	The number of authenticated users registered in the iSCSI target
Host Mode	Host mode of the host group
Host Mode Option	Host mode option of the host group. Host mode options are separated by semicolons (;) when more than one option is specified.
Number of Hosts	The number of the hosts in the host group.

Hosts report

The following illustration shows an example of a hosts report. The table following the illustration describes the items in the report. When a host is registered to more than one port, more than one record shows information about the same host.



Hosts

This report is about hosts. A record is created for each host. When a host is registered to more than one port, more than one record shows information about the same host.

Port Location	Type	Port Internal WWN	Port Security	Host Group Name / iSCSI Target Alias	iSCSI Target Name
1B	ISCSI(OPT)		Disabled	1B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
2B	ISCSI(OPT)		Disabled	2B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
3B	ISCSI(OPT)		Disabled	3B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000
4B	ISCSI(OPT)		Disabled	4B-G00	iqn.1994-04.jp.co.hitachi:rsd.h8m.t.00001.1b000

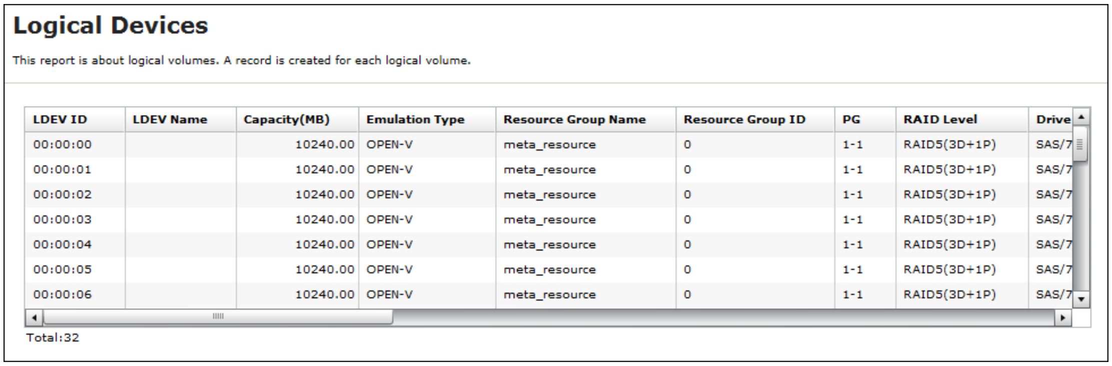
Total:4

Item	Description
Port Location	Name of the port
Type	Port type
Port Internal WWN	Port WWN
Port Security	Port security setting

Item	Description
Host Group Name / iSCSI Target Alias	Name of the host group / alias of the iSCSI target
iSCSI Target Name	Name of the iSCSI target
Host Mode	Host mode of the host group
Host Mode Option	Host group host mode option. When more than one host mode option is specified, they are separated by semicolons (;)
Host Name	Name of the host that can access the LU path through the port
HBA WWN / iSCSI Name	Host WWN / host iSCSI name. The name is in 16-digit hex format.

Logical Devices report

The following illustration shows an example of a logical volumes report. The table following the illustration describes the items in the report.



Logical Devices

This report is about logical volumes. A record is created for each logical volume.

LDEV ID	LDEV Name	Capacity(MB)	Emulation Type	Resource Group Name	Resource Group ID	PG	RAID Level	Drive
00:00:00		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:01		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:02		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:03		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:04		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:05		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7
00:00:06		10240.00	OPEN-V	meta_resource	0	1-1	RAID5(3D+1P)	SAS/7

Total:32

Item	Description
LDEV ID	The logical volume number
LDEV Name	The logical volume name
Capacity (MB)	Capacity of the logical volume
Emulation Type	Emulation type of the logical volume
Resource Group Name	Resource group name where LDEV belongs
Resource Group ID	Resource group ID where LDEV belongs
PG	The parity group number. • If the number starts with "E" (for example, E1-1), the parity group contains external volumes. • If the number starts with "M" (for example, M1-1), the parity group contains FICON DM volumes. A hyphen displays for Dynamic Provisioning or Thin Image V-VOLs.
RAID Level	RAID level of the parity group where the logical volume belongs[1]
Drive Type/RPM	Drive type and round-per-minute (RPM) of the drive of the parity group where the logical volume belongs.

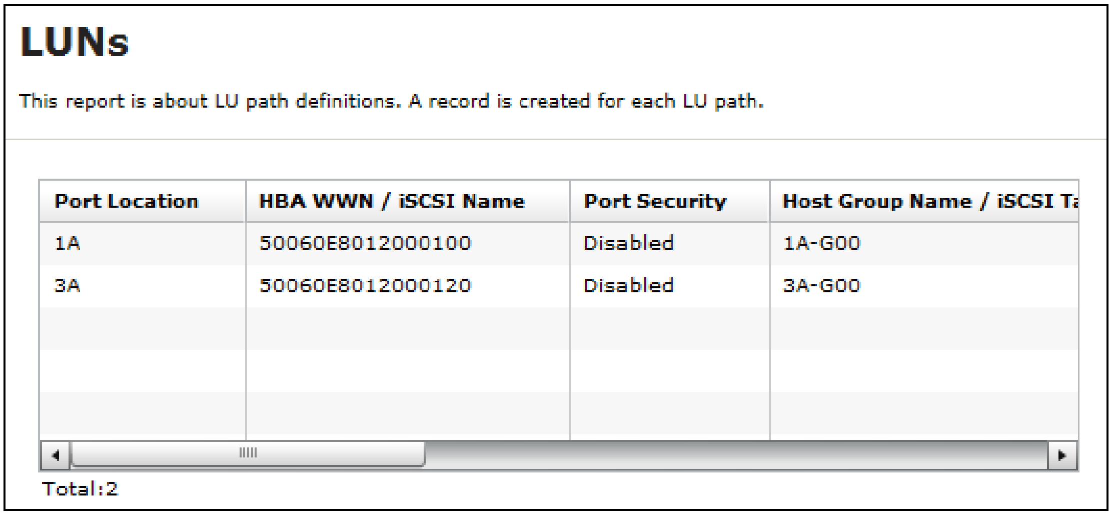
Item	Description
	A hyphen (-) is displayed as RPM when the drive is SSD.[1]
Drive Type-Code	Type code of the drive of the parity group where the logical volume belongs[1]
Drive Capacity	Capacity of the drive of the parity group where the logical volume belongs.[1]
PG Members	List of the drive locations of the parity group where the logical volume belongs[1]
Allocated	Information about whether the host can access the logical volume. For mainframe volumes and multi-platform volumes, "Y" is displayed unless the volumes are in the reserved status.
SSID	SSID of the logical volume
CVS	Information about whether the logical volume is a customized volume
OCS	Oracle checksum
Attribute	The attribute of the logical volume
Provisioning Type	Provisioning type of the logical volume
Pool Name	• For V-VOLs of Dynamic Provisioning, the name of the pool related to the logical volume is displayed[1] • If the logical volume attribute is Pool, the name of the pool where the logical volume belongs is displayed • When neither of the above are displayed, the pool name is blank
Pool ID	The ID of the pool indicated by "Pool Name" A hyphen (-) displays for volumes other than pool-VOLs or V-VOLs
Current MPU	The number of the MP unit that currently controls the logical volume
Setting MPU	The number of the MP unit that you specified to control the logical volume
Command Device: Security	Indicates whether Security is specified as the attribute for the command device. A hyphen (-) displays when "Attribute" is not "CMDDEV".
Command Device: User Authentication	Indicates whether User Authentication is specified as the attribute for the command device. A hyphen (-) displays when "Attribute" is not "CMDDEV".
Command Device: Device Group Definition	Indicates whether Device Group Definition is specified as the attribute for the command device. A hyphen (-) displays when "Attribute" is not "CMDDEV".
Encryption	Information about whether the parity group is where the LDEV belongs is encrypted or not • For Internal Volumes: Enable (encrypted) or Disable • For External Volumes: blank

Notes:

1. A hyphen (-) displays if the LDEV is an external volume.

LUNs report

The following illustration shows an example of a LU path definitions report. A record is created for each LU path. The table following the illustration describes the items in the report.


LUNs

This report is about LU path definitions. A record is created for each LU path.

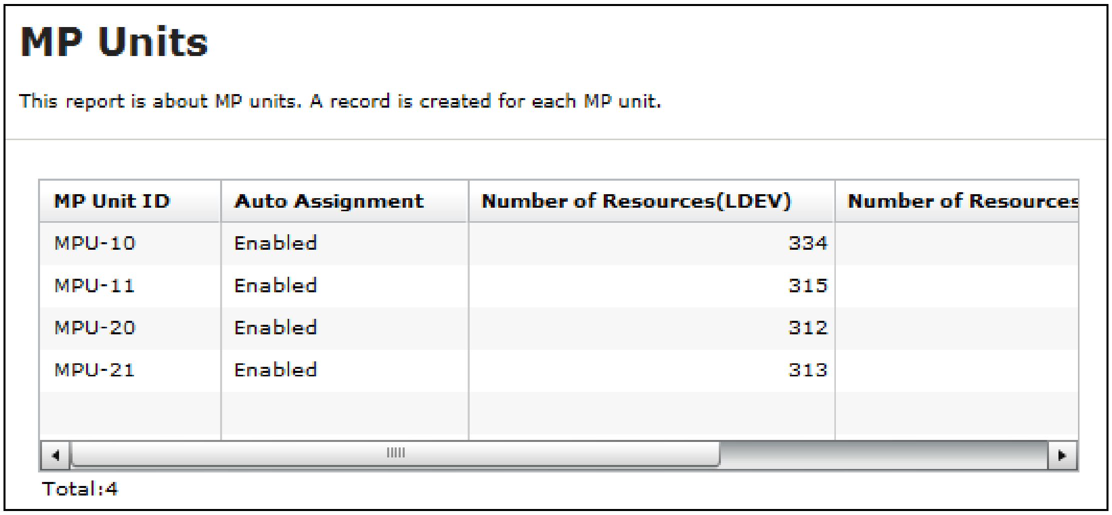
Port Location	HBA WWN / iSCSI Name	Port Security	Host Group Name / iSCSI Ta
1A	50060E8012000100	Disabled	1A-G00
3A	50060E8012000120	Disabled	3A-G00

Total:2

Item	Description
Port Location	Name of the port
HBA WWN / iSCSI Name	Port WWN or name of the iSCSI (16 digits in hexadecimal)
Port Security	Name of the type of security of the port
Host Group Name / iSCSI Target Alias	Name of the host group or alias of the iSCSI target
iSCSI Target Name	Name of the iSCSI target
Host Mode	Host mode of the host group
Host Mode Option	Host mode option of the host group. Host mode options are separated by semicolons (;) when more than one option is specified.
LUN	Logical unit number
LDEV ID	Logical volume number
Emulation Type	Emulation type of the logical volume
Capacity (MB)	Capacity of the logical volume

MP Units report

The following illustration shows an example of an MP units report. The table following the illustration describes the items in the report.



MP Units

This report is about MP units. A record is created for each MP unit.

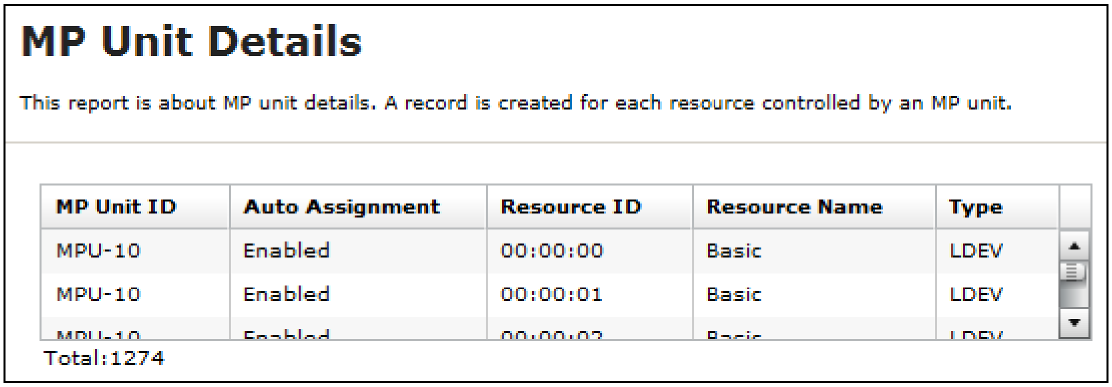
MP Unit ID	Auto Assignment	Number of Resources(LDEV)	Number of Resources
MPU-10	Enabled	334	
MPU-11	Enabled	315	
MPU-20	Enabled	312	
MPU-21	Enabled	313	

Total:4

Item	Description
MP Unit ID	MP unit ID
Auto Assignment	Auto assignment attribute for the MP unit
Number of Resources (LDEV)	Number of LDEVs that the MP unit controls
Number of Resources (Journal)	Number of journals that the MP unit controls
Number of Resources (External Volume)	Number of external volumes that the MP unit controls (includes volumes for FICON DM)
Number of Resources (Total)	The total number of resources that the MP unit controls. It is the total of Number of Resources (LDEV), Number of Resources (Journal), and Number of Resources (External Volume).

MP Unit Details report

The following illustration shows an example of an MP unit details report. The table following the illustration describes the items in the report.



MP Unit Details

This report is about MP unit details. A record is created for each resource controlled by an MP unit.

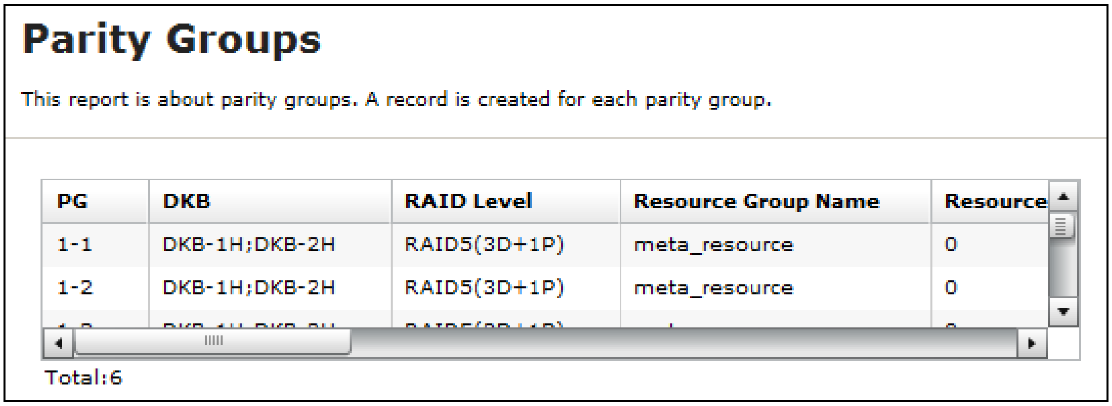
MP Unit ID	Auto Assignment	Resource ID	Resource Name	Type
MPU-10	Enabled	00:00:00	Basic	LDEV
MPU-10	Enabled	00:00:01	Basic	LDEV
MPU-10	Enabled	00:00:02	Basic	LDEV

Total:1274

Item	Description
MP Unit ID	MP unit ID
Auto Assignment	Auto assignment attribute for the MP unit
Resource ID	ID of this resource that the MP unit controls
Resource Name	The name of the resource that the MP unit controls. If "Type" is LDEV, the LDEV name that is set is displayed. A hyphen (-) displays for journal volumes or external volumes.
Type	The type of the resource that the MP unit controls

Parity Groups report

The following illustration shows an example of a parity groups report. The table following the illustration describes the items in the report.



Parity Groups

This report is about parity groups. A record is created for each parity group.

PG	DKB	RAID Level	Resource Group Name	Resource
1-1	DKB-1H;DKB-2H	RAID5(3D+1P)	meta_resource	0
1-2	DKB-1H;DKB-2H	RAID5(3D+1P)	meta_resource	0

Total:6

Item	Description
PG	Parity group number • If the number starts with "E" (for example, E1-1), the parity group contains external volumes (Hitachi Universal Volume Manager User Guide). • If the number starts with "M" (for example, M1-1), the parity group contains volumes for FICON DM.
DKB	Name of the disk board that controls the parity group[1]
RAID Level	RAID level of the parity group[1]
Resource Group Name	Name of the resource group in which the parity group belongs
Resource Group ID	ID for the resource group in which the parity group belongs
Emulation Type	Emulation type of the parity group
Number of LDEVs (Total)	The number of the logical volumes in the parity group
Number of LDEVs (Unallocated)	The number of the logical volumes in the parity group that the host cannot access
Total LDEV Capacity (MB)	Capacity of the logical volumes in the parity group
Unallocated LDEV Capacity (MB)	Capacity of the logical volumes in the parity group that the host cannot access

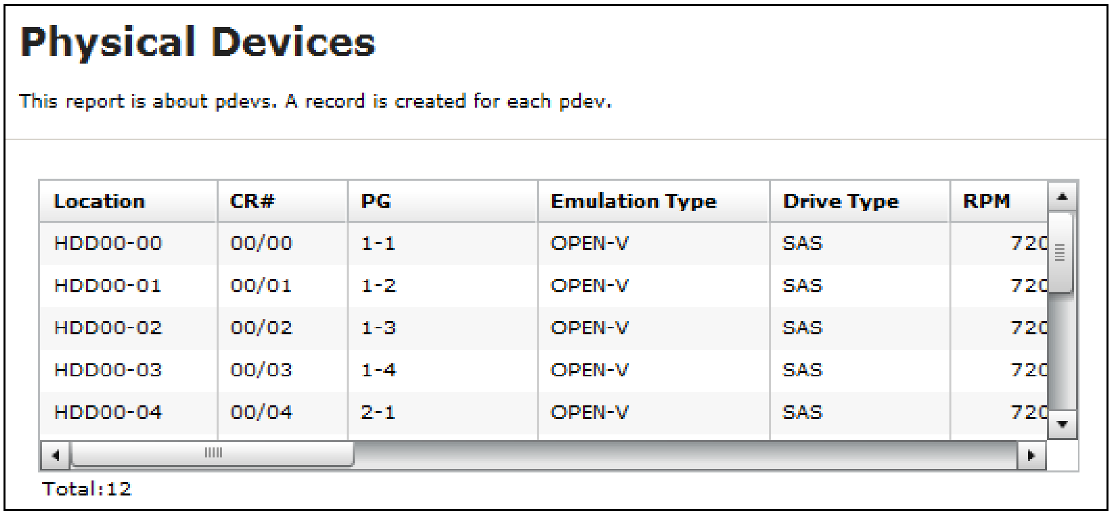
Item	Description
Drive Type-Code	The type code of the drive in the parity group. • The type code of the first drive in the parity group. • If the parity group contains external volumes, the drive type code displays the vendor, the model, and the serial number of the storage system. • Separated by semicolons (;) if multiple drive types are set.
Drive Type/RPM	Drive type and revolutions-per-minute (RPM) of the drive in the parity group[1] A hyphen (-) is displayed instead of the RPM when the drive is an SSD.
Drive Capacity	Capacity of the drive in the parity group[1]
RAID Concatenation #0	The number indicating a parity group #0 connected to this parity group[1,2]
RAID Concatenation #1	The number indicating a parity group #1 connected to this parity group[1,2]
RAID Concatenation #2	The number indicating a parity group #1,2 connected to this parity group[1,2]
Encryption	Information about whether the parity group is encrypted or not • For Internal Volumes: Enable (encrypted) or Disable • For External Volumes: A hyphen (-) is displayed

Notes:

1. A hyphen is displayed if the parity group contains external volumes.
2. A hyphen is displayed if the parity group is not connected with another parity group or if the parity group contains external volumes including volumes for FICON DM.

Physical Devices report

The following illustration shows an example of part of a Physical Devices report. The actual report includes more columns of information. A record is created for each physical device. The table following the illustration describes the items in the report.



Physical Devices

This report is about pdevs. A record is created for each pdev.

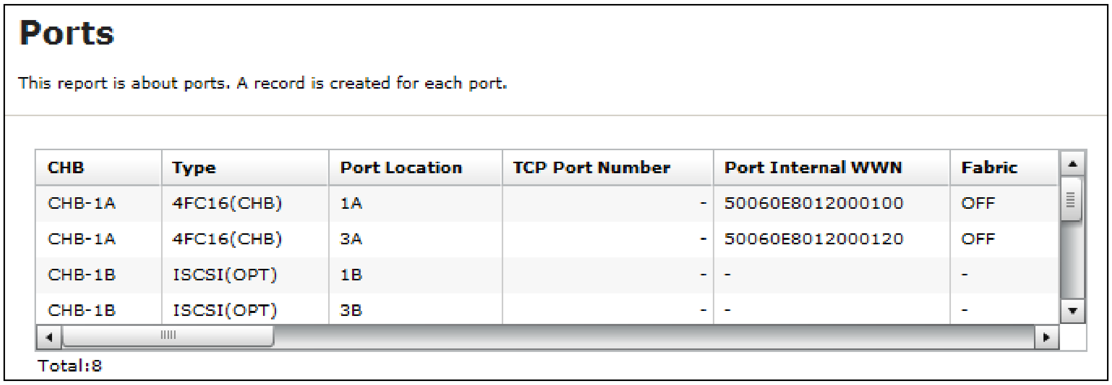
Location	CR#	PG	Emulation Type	Drive Type	RPM
HDD00-00	00/00	1-1	OPEN-V	SAS	720
HDD00-01	00/01	1-2	OPEN-V	SAS	720
HDD00-02	00/02	1-3	OPEN-V	SAS	720
HDD00-03	00/03	1-4	OPEN-V	SAS	720
HDD00-04	00/04	2-1	OPEN-V	SAS	720

Total:12

Item	Description
Location	Name of physical devices
CR#	C# and R# to define physical devices Output as "XX/YY"
PG	Parity group of physical devices
Emulation Type	Parity group of physical devices
Drive type	Drive type of physical devices • SAS • SSD
RPM	Revolutions-per-minute (RPM) in the parity group • 8000 • 15000 A hyphen (-) is displayed instead of the RPM when the drive type is an SSD.
Drive Type-Code	Type code of the drive in the parity group. Output example: SLR5B- M200SS;SFB5A-M200SS; (if multiple drive types are set)
Drive Size	Drive size (inches) • 2.5 • 3.5
Drive Capacity	Physical drive capacity (GB or TB)
Drive Version	Firmware version of the drive
DKB1	Name of the DKB1 which controls the physical devices
DKB2	Name of the DKB2 which controls the physical devices
Serial Number#	Serial product number of the physical devices • yy: year (last 2 digits) • mm: month (2 digits) • xxxxxxxx: product number of the physical devices
RAID Level	RAID level of the physical devices • RAID1(2D+2D) • RAID5(7D+1P) • RAID6(6D+2P) • RAID6(14D+2P)
RAID Concatenation#0	Number indicating a parity group #0 connected to this parity group Output example: 2-1, 3-1, 4-1
RAID Concatenation#1	Number indicating a parity group #1 connected to this parity group Output example: 2-1, 3-1, 4-1
RAID Concatenation#2	Number indicating a parity group #2 connected to this parity group Output example: 2-1, 3-1, 4-1
Resource Group Name	Name of resource group to which the parity group of physical devices belong
Resource Group ID	ID (0 to 1023 binary)
Encryption	Enable or disable status of the parity group to which the physical devices belong • Enabled: Encryption is enabled. • Disabled: Encryption is disabled.

Ports report

The following illustration shows an example of part of a ports report. The actual report includes several more columns of information. The table following the illustration describes the items in the report.



Ports

This report is about ports. A record is created for each port.

CHB	Type	Port Location	TCP Port Number	Port Internal WWN	Fabric
CHB-1A	4FC16(CHB)	1A	-	50060E8012000100	OFF
CHB-1A	4FC16(CHB)	3A	-	50060E8012000120	OFF
CHB-1B	ISCSI(OPT)	1B	-	-	-
CHB-1B	ISCSI(OPT)	3B	-	-	-

Total:8

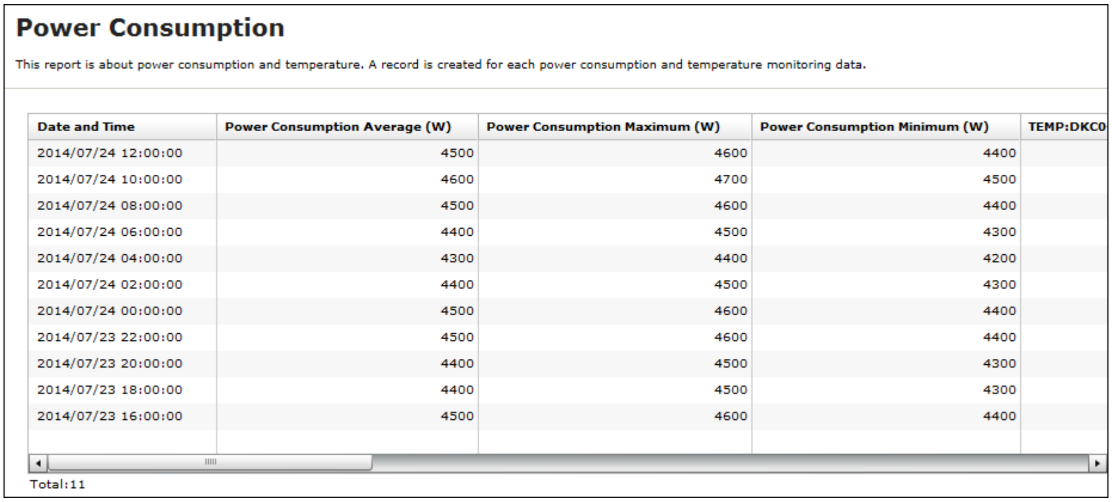
Item	Description
CHB	Name of the channel board
Type	Package type of the channel board
Port Location	Name of the port on the channel board
Port Attribute	Attribute of the port
TCP Port Number	Port number to use for a socket (decimal)
Port Internal WWN	WWN of the port
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch
Connection Type	One of the Fibre topology settings • Point to Point • FC-AL
IPv4 : IP Address	IPv4 address of the port Output example: 192.168.0.100
IPv4 : Subnet Mask	IPv4 subnet mask of the port Output example: 255.255.255.0
IPv4 : Default Gateway	IPv4 default gateway of the port Output example: 255.255.255.0
IPv6 : Mode	IPv6 settings of the port • Enabled • Disabled
IPv6 : Link Local Address	IPv6 link local address of the port (16-digit hexadecimal)
IPv6 : Global Address	IPv6 global address of the port.

Item	Description
	Output example: *xxx*:*xxx*:*xxx*:*xxx*:*xxx*:*xxx*:*xxx*:*xxx*
IPv6 : Assigned Default Gateway	Assigned IPv6 default gateway
Selective ACK	Selective ACK mode • Enabled • Disabled
Ethernet MTU Size (Byte)	MTU settings (binary) • 1,500
Keep Alive Timer	iSCSI keep alive timer (0 to 64,800) (sec)
VLAN : Tagging Mode	Tagging mode of VLAN • Enabled • Disabled
VLAN : ID	Number of VLAN set to the port (1 to 4,094)
iSNS Server : Mode	iSNS mode settings • ON • OFF
iSNS Server : IP Address	IP address of the iSNS server (30 to 65,535)
iSNS Server : TCP Port Number	Number of the TCP port used in iSNS (binary)
Address (Loop ID)	Fibre port address and Loop ID of the port
Port Security	Security of the port • Enabled • Disabled
Speed	Data transfer speed of the port
Resource Group Name	Name of the resource group to which the port belongs
Resource Group ID	ID for the resource group to which the port belongs (0 to 1023)
Number of Hosts	The number of the hosts registered to the port
Number of LUNs	The number of the LU paths defined to the port
Number of LDEVs	The number of the logical volumes that can be accessed through the port
Number of PGs	The number of the parity groups having the logical volumes that can be accessed through the port
Number of DKBs	The number of the disk boards controlling the parity group that contains the logical volumes that can be accessed through the port

Power Consumption report

The following illustration shows an example of a power consumption report. A record is created every two hours for each power consumption and temperature monitoring data. The table following the illustration describes the items in the report.

No records are created a system power failure or if the breakers are turned off. If the system is in maintenance mode or the SVP is rebooted, up to two hours of records could be lost.



Power Consumption

This report is about power consumption and temperature. A record is created for each power consumption and temperature monitoring data.

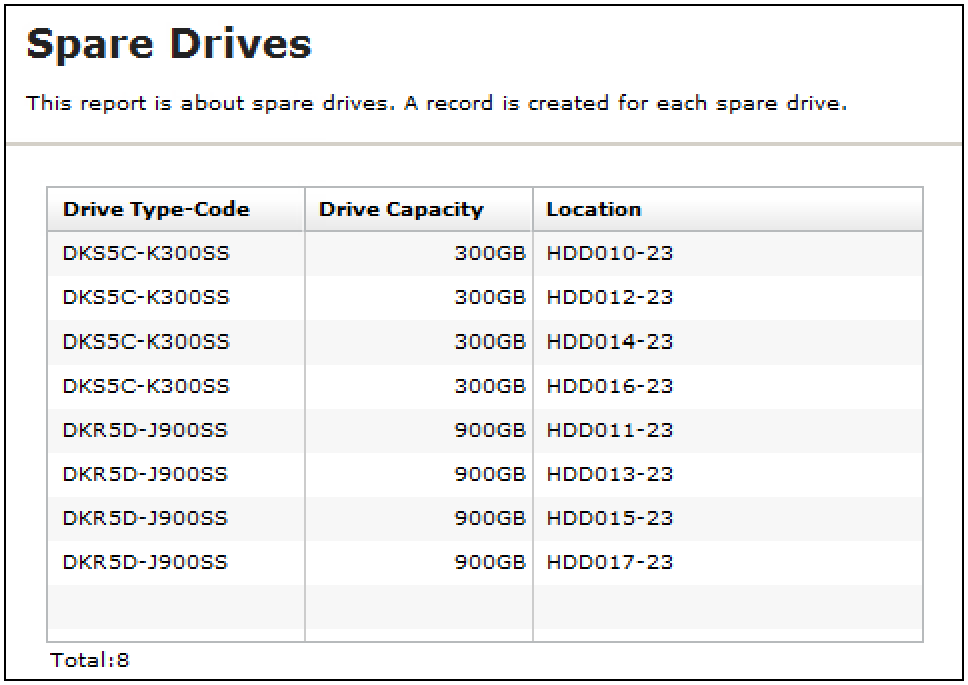
Date and Time	Power Consumption Average (W)	Power Consumption Maximum (W)	Power Consumption Minimum (W)	TEMP:DKC0
2014/07/24 12:00:00	4500	4600	4400	
2014/07/24 10:00:00	4600	4700	4500	
2014/07/24 08:00:00	4500	4600	4400	
2014/07/24 06:00:00	4400	4500	4300	
2014/07/24 04:00:00	4300	4400	4200	
2014/07/24 02:00:00	4400	4500	4300	
2014/07/24 00:00:00	4500	4600	4400	
2014/07/23 22:00:00	4500	4600	4400	
2014/07/23 20:00:00	4400	4500	4300	
2014/07/23 18:00:00	4400	4500	4300	
2014/07/23 16:00:00	4500	4600	4400	

Total:11

Item	Description
Date and Time	Date and time when power consumption and temperature were recorded for the two-hour period
Power Consumption Average (W)	Average of the power consumption
Power Consumption Maximum (W)	Maximum of the power consumption
Power Consumption Minimum (W)	Minimum of the power consumption
TEMP:DKC0-Cluster1 Average (degrees C)	Average temperature of DKC0:CL1
TEMP:DKC0-Cluster1 Maximum (degrees C)	Maximum temperature of DKC0:CL1
TEMP:DKC0-Cluster1 Minimum (degrees C)	Minimum temperature of DKC0:CL1
TEMP:DKC0-Cluster2 Average (degrees C)	Average temperature of DKC0:CL2
TEMP:DKC0-Cluster2 Maximum (degrees C)	Maximum temperature of DKC0:CL2
TEMP:DKC0-Cluster2 Minimum (degrees C)	Minimum temperature of DKC0:CL2

Spare Drives report

The following illustration shows an example of a spare drives report. The table following the illustration describes the items in the report.



Spare Drives

This report is about spare drives. A record is created for each spare drive.

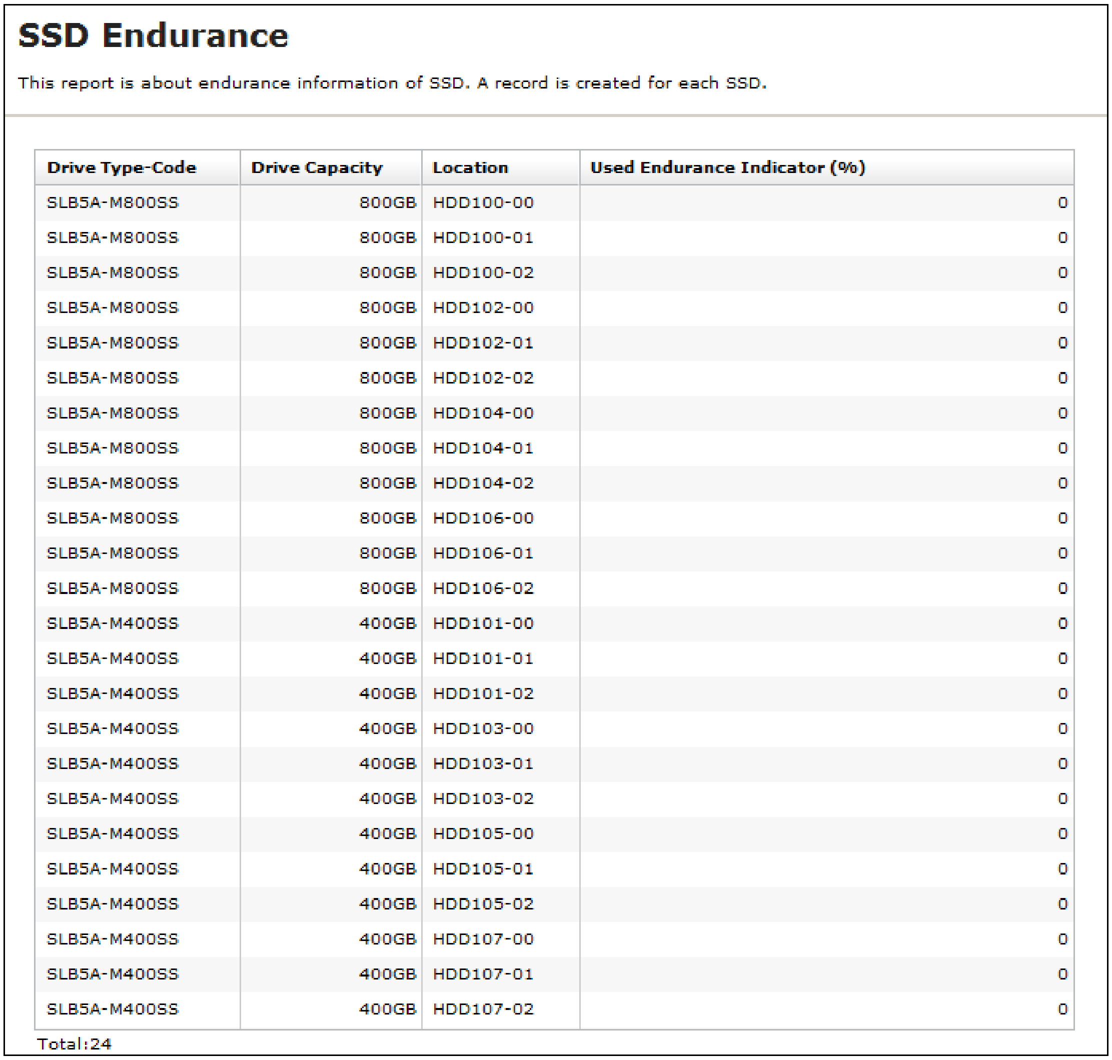
Drive Type-Code	Drive Capacity	Location
DKS5C-K300SS	300GB	HDD010-23
DKS5C-K300SS	300GB	HDD012-23
DKS5C-K300SS	300GB	HDD014-23
DKS5C-K300SS	300GB	HDD016-23
DKR5D-J900SS	900GB	HDD011-23
DKR5D-J900SS	900GB	HDD013-23
DKR5D-J900SS	900GB	HDD015-23
DKR5D-J900SS	900GB	HDD017-23

Total:8

Item	Description
Drive Capacity	Capacity of the spare drive
Drive Type-Code	Type code of the spare drive
Location	Location of the spare drive

SSD Endurance report

The following illustration shows an example of an SSD endurance report. The table following the illustration describes the items in the report.



SSD Endurance

This report is about endurance information of SSD. A record is created for each SSD.

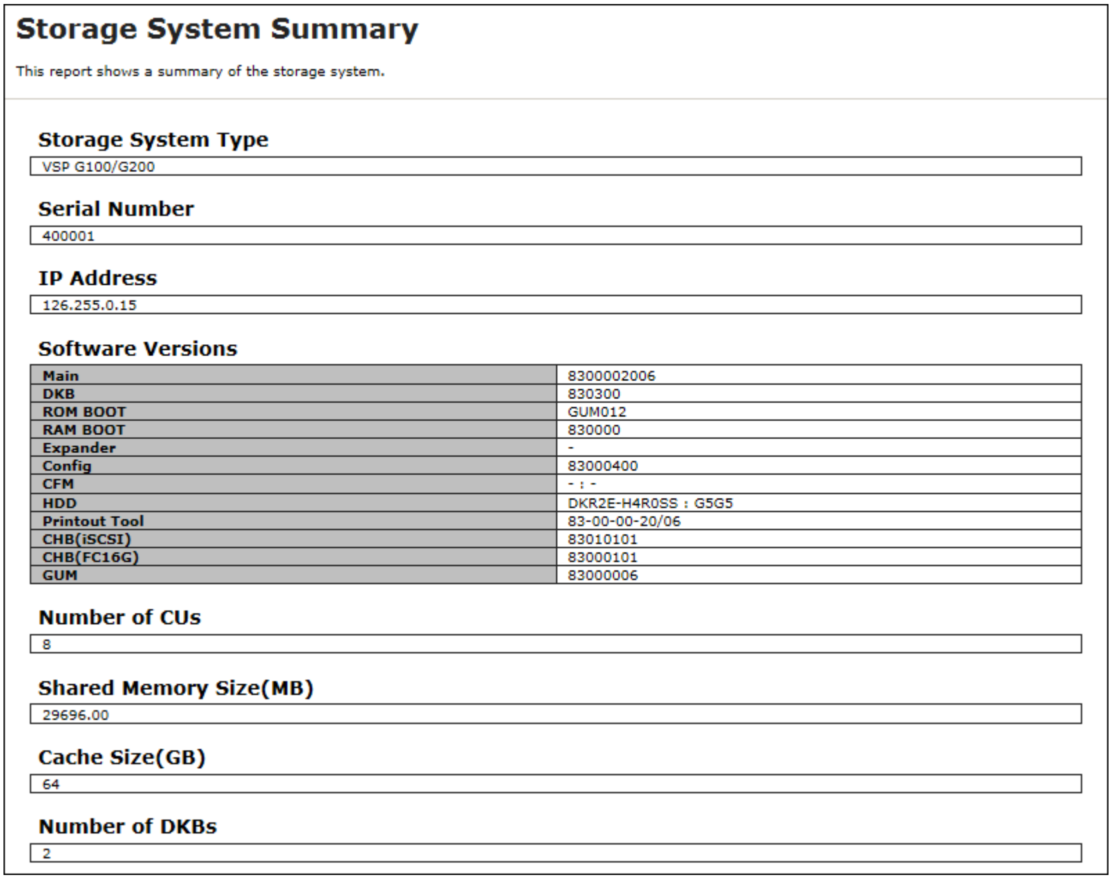
Drive Type-Code	Drive Capacity	Location	Used Endurance Indicator (%)
SLB5A-M800SS	800GB	HDD100-00	0
SLB5A-M800SS	800GB	HDD100-01	0
SLB5A-M800SS	800GB	HDD100-02	0
SLB5A-M800SS	800GB	HDD102-00	0
SLB5A-M800SS	800GB	HDD102-01	0
SLB5A-M800SS	800GB	HDD102-02	0
SLB5A-M800SS	800GB	HDD104-00	0
SLB5A-M800SS	800GB	HDD104-01	0
SLB5A-M800SS	800GB	HDD104-02	0
SLB5A-M800SS	800GB	HDD106-00	0
SLB5A-M800SS	800GB	HDD106-01	0
SLB5A-M800SS	800GB	HDD106-02	0
SLB5A-M400SS	400GB	HDD101-00	0
SLB5A-M400SS	400GB	HDD101-01	0
SLB5A-M400SS	400GB	HDD101-02	0
SLB5A-M400SS	400GB	HDD103-00	0
SLB5A-M400SS	400GB	HDD103-01	0
SLB5A-M400SS	400GB	HDD103-02	0
SLB5A-M400SS	400GB	HDD105-00	0
SLB5A-M400SS	400GB	HDD105-01	0
SLB5A-M400SS	400GB	HDD105-02	0
SLB5A-M400SS	400GB	HDD107-00	0
SLB5A-M400SS	400GB	HDD107-01	0
SLB5A-M400SS	400GB	HDD107-02	0

Total:24

Item	Description
Drive Type-Code	Type code of the SSD
Drive Capacity	Capacity of the SSD
Location	Location of the SSD
Used Endurance Indicator (%)	Used endurance of the SSD

Storage System Summary report

The following illustration shows an example of part of a report of a summary of the storage system. The actual report includes several more rows of information. The table following the illustration describes the items in the report.



Storage System Summary

This report shows a summary of the storage system.

Storage System Type

VSP G100/G200

Serial Number

400001

IP Address

126.255.0.15

Software Versions

Main	8300002006
DKB	830300
ROM BOOT	GUM012
RAM BOOT	830000
Expander	-
Config	83000400
CFM	- : -
HDD	DKR2E-H4R0SS : G5G5
Printout Tool	83-00-00-20/06
CHB(iSCSI)	83010101
CHB(FC16G)	83000101
GUM	83000006

Number of CUs

8

Shared Memory Size(MB)

29696.00

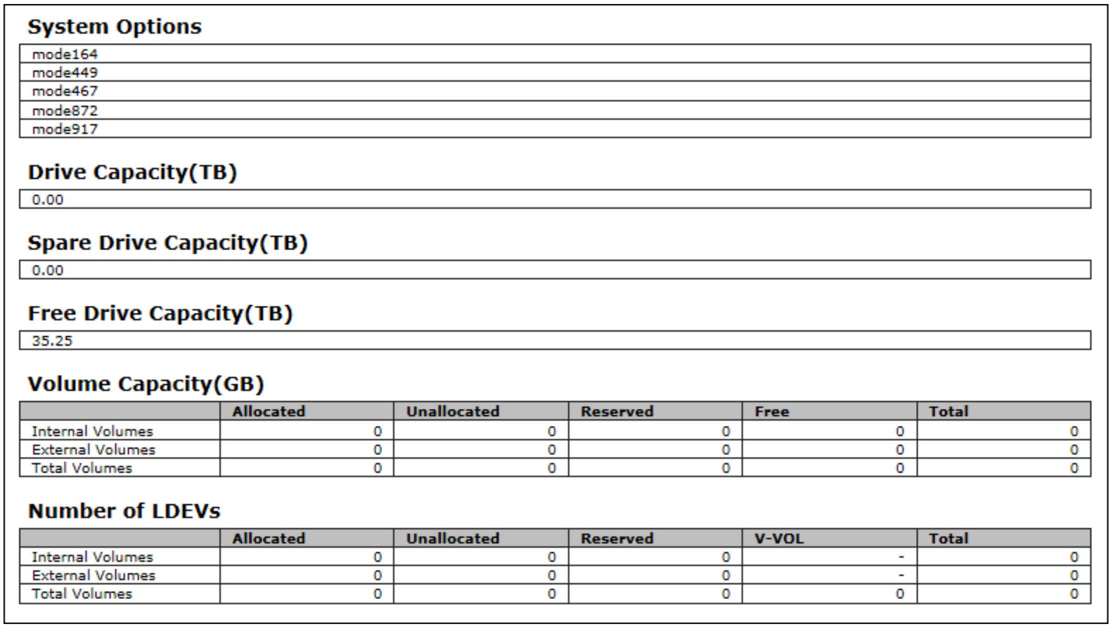
Cache Size(GB)

64

Number of DKBs

2

Figure 1 Storage System Summary report (VSP G200)



System Options

mode164
mode449
mode467
mode872
mode917

Drive Capacity(TB)

0.00

Spare Drive Capacity(TB)

0.00

Free Drive Capacity(TB)

35.25

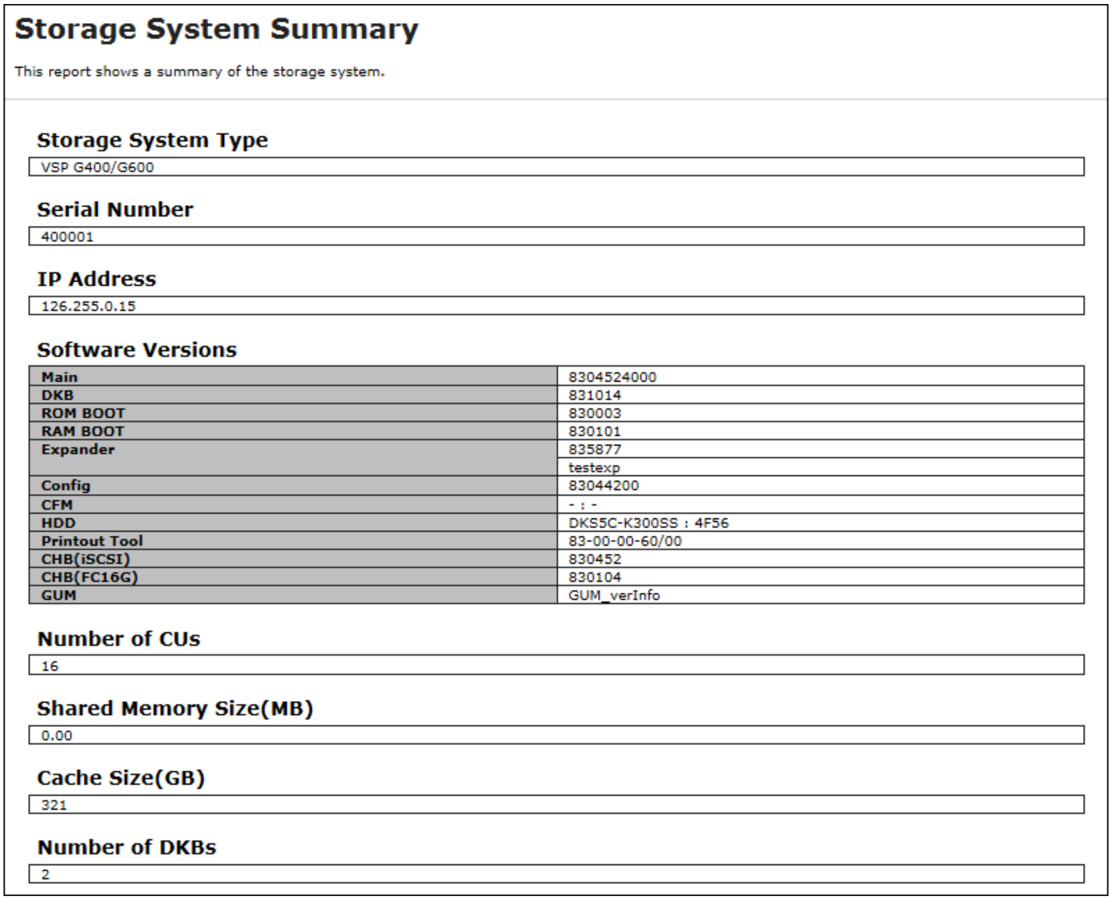
Volume Capacity(GB)

	Allocated	Unallocated	Reserved	Free	Total
Internal Volumes	0	0	0	0	0
External Volumes	0	0	0	0	0
Total Volumes	0	0	0	0	0

Number of LDEVs

	Allocated	Unallocated	Reserved	V-VOL	Total
Internal Volumes	0	0	0	-	0
External Volumes	0	0	0	-	0
Total Volumes	0	0	0	0	0

Figure 2 Storage System Summary report (VSP G200)



Storage System Summary

This report shows a summary of the storage system.

Storage System Type

VSP G400/G600

Serial Number

400001

IP Address

126.255.0.15

Software Versions

Main	8304524000
DKB	831014
ROM BOOT	830003
RAM BOOT	830101
Expander	835877 testexp
Config	83044200
CFM	- : -
HDD	DKS5C-K300SS : 4F56
Printout Tool	83-00-00-60/00
CHB(iSCSI)	830452
CHB(FC16G)	830104
GUM	GUM_verInfo

Number of CUs

16

Shared Memory Size(MB)

0.00

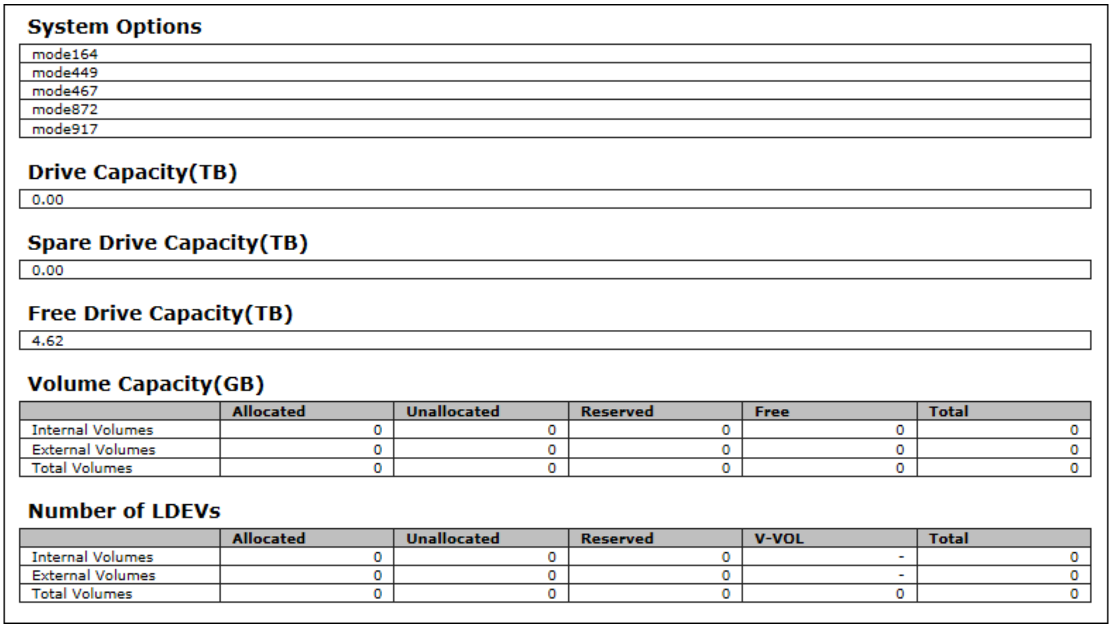
Cache Size(GB)

321

Number of DKBs

2

Figure 3 Storage System Summary report (VSP G400, VSP G600)



System Options

mode164
mode449
mode467
mode872
mode917

Drive Capacity(TB)

0.00

Spare Drive Capacity(TB)

0.00

Free Drive Capacity(TB)

4.62

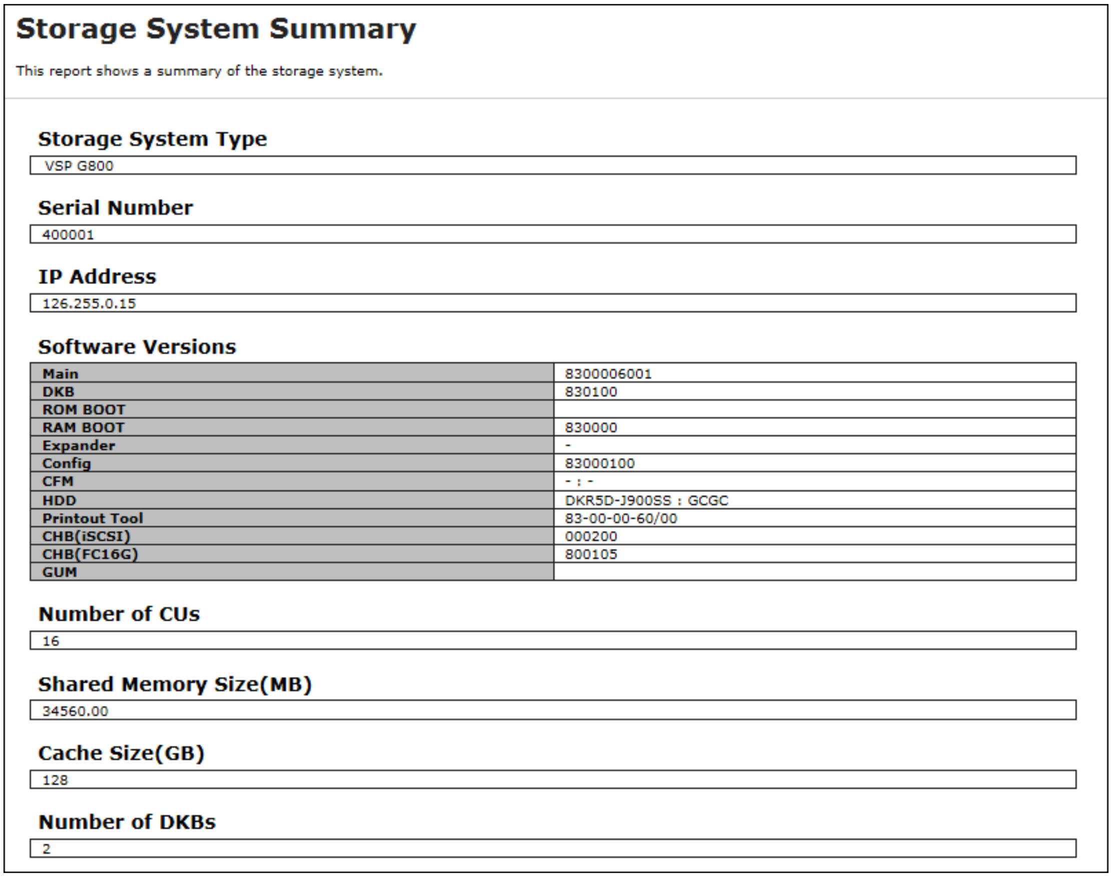
Volume Capacity(GB)

	Allocated	Unallocated	Reserved	Free	Total
Internal Volumes	0	0	0	0	0
External Volumes	0	0	0	0	0
Total Volumes	0	0	0	0	0

Number of LDEVs

	Allocated	Unallocated	Reserved	V-VOL	Total
Internal Volumes	0	0	0	-	0
External Volumes	0	0	0	-	0
Total Volumes	0	0	0	0	0

Figure 4 Storage System Summary report (VSP G400, VSP G600)



Storage System Summary

This report shows a summary of the storage system.

Storage System Type

VSP G800

Serial Number

400001

IP Address

126.255.0.15

Software Versions

Main	8300006001
DKB	830100
ROM BOOT	
RAM BOOT	830000
Expander	-
Config	83000100
CFM	- : -
HDD	DKR5D-J900SS : GCGC
Printout Tool	83-00-00-60/00
CHB(iSCSI)	000200
CHB(FC16G)	800105
GUM	

Number of CUs

16

Shared Memory Size(MB)

34560.00

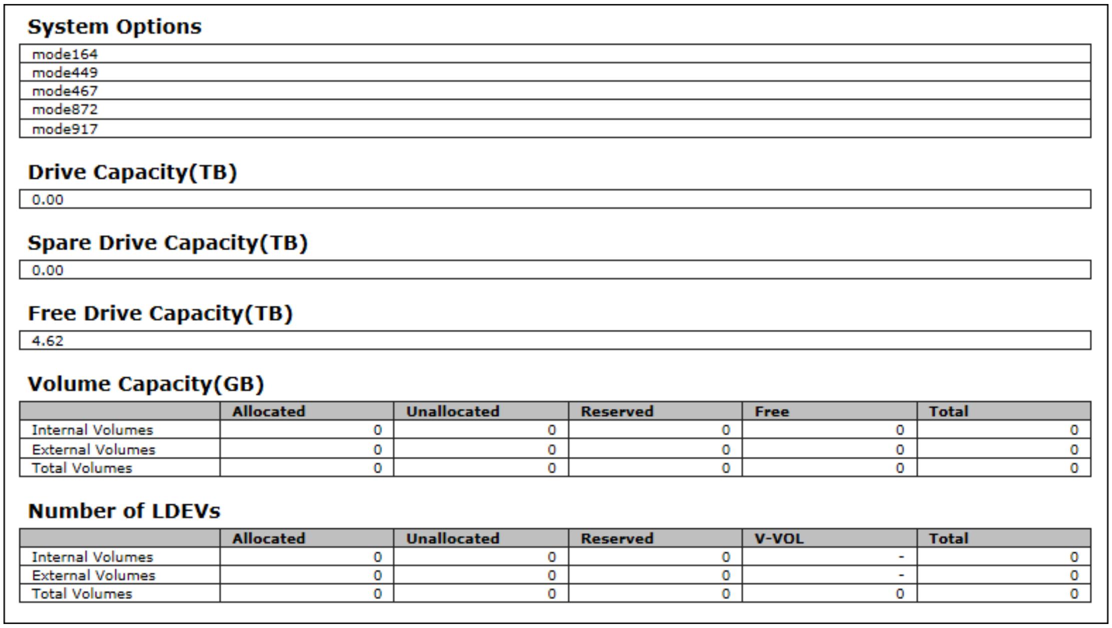
Cache Size(GB)

128

Number of DKBs

2

Figure 5 Storage System Summary report (VSP G800)



System Options

mode164
mode449
mode467
mode872
mode917

Drive Capacity(TB)

0.00

Spare Drive Capacity(TB)

0.00

Free Drive Capacity(TB)

4.62

Volume Capacity(GB)

	Allocated	Unallocated	Reserved	Free	Total
Internal Volumes	0	0	0	0	0
External Volumes	0	0	0	0	0
Total Volumes	0	0	0	0	0

Number of LDEVs

	Allocated	Unallocated	Reserved	V-VOL	Total
Internal Volumes	0	0	0	-	0
External Volumes	0	0	0	-	0
Total Volumes	0	0	0	0	0

Figure 6 Storage System Summary report (VSP G800)

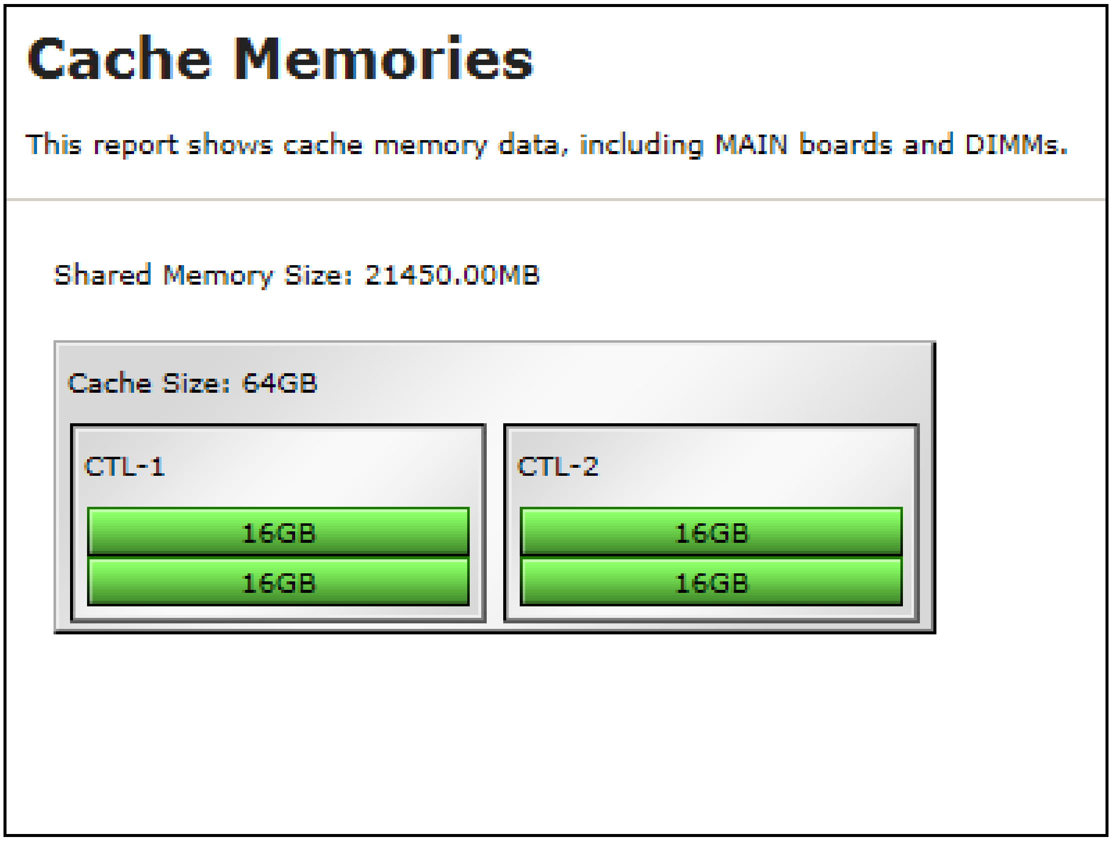
Item	Description
Storage System Type	Type of the storage system
Serial Number	Serial number of the storage system
IP Address	IP address of the SVP
Microcode Versions	Version of the following programs. • Main • DKB • ROM BOOT • RAM BOOT • Expander • Config • CFM • HDD • Printout Tool • CHB (iSCSI) • CHB (FC16G) • GUM
Number of CUs	The number of control units in the storage system
Shared Memory Size (GB)	Capacity of shared memory Includes the cache management information (directory)
Cache Size (GB)	Capacity of the cache
Number of DKBs	The number of disk boards on the module
System Options	List of the system options specified for the storage system
Drive Capacity (TB)	Total capacity of drives in the storage system except for external volumes
Spare Drive Capacity (TB)	Total capacity of the spare drives in the storage system
Free Drive Capacity (GB)	Total capacity of the free drives in the storage system
Volume Capacity (GB) [1]	List of the capacity of the open volumes
Number of LDEVs[1]	List of the numbers of the volumes in the following status. • Allocated • Unallocated • Reserved • V-VOL
Notes: **1.** 1. You cannot sort the list.	

Reports in graphical view

The reports described in this topic display as graphics. 📊 icons are displayed before the names of reports in graphical view. If the icons or graphics are not displayed properly, update the window.

Cache Memories report

This report shows cache memory data, including shared memory, main board, and DIMM capacity. The total cache memory is displayed for each module.



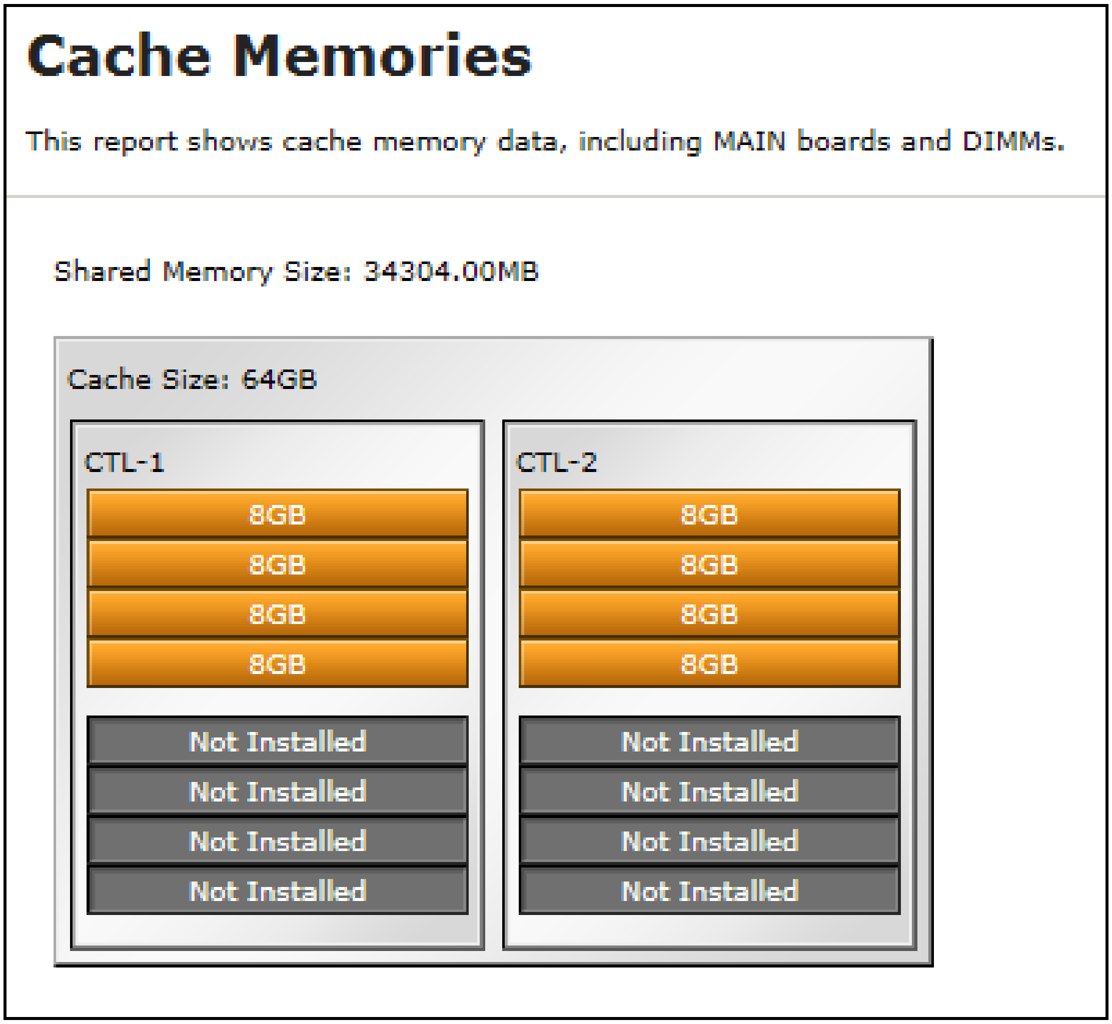
Cache Memories

This report shows cache memory data, including MAIN boards and DIMMs.

Shared Memory Size: 21450.00MB

Cache Size: 64GB

Figure 7 Cache Memories report (VSP G200)



Cache Memories

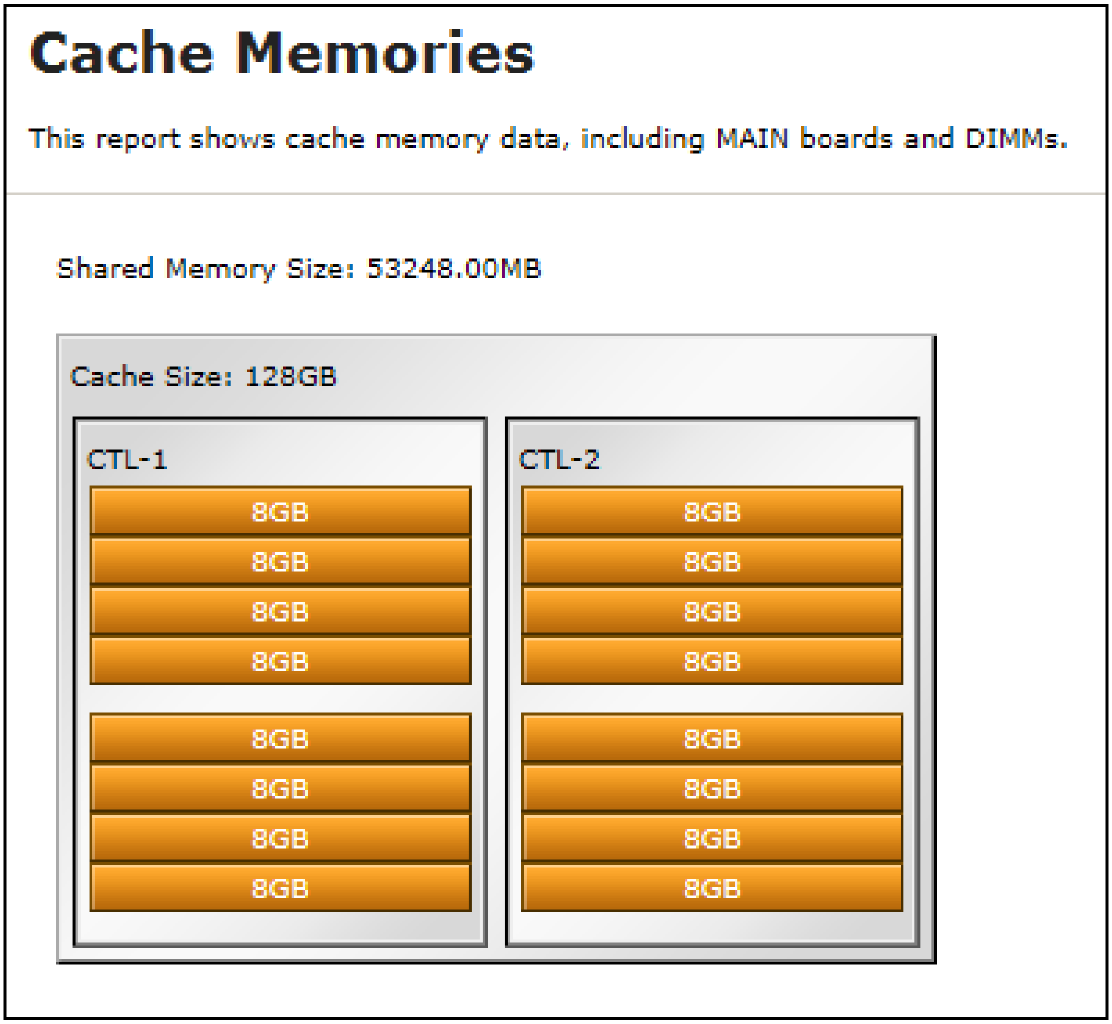
This report shows cache memory data, including MAIN boards and DIMMs.

Shared Memory Size: 34304.00MB

Cache Size: 64GB

CTL-1	CTL-2
8GB	8GB
8GB	8GB
8GB	8GB
8GB	8GB
Not Installed	Not Installed
Not Installed	Not Installed
Not Installed	Not Installed
Not Installed	Not Installed

Figure 8 Cache Memories report (VSP G400, VSP G600)



Cache Memories

This report shows cache memory data, including MAIN boards and DIMMs.

Shared Memory Size: 53248.00MB

Cache Size: 128GB

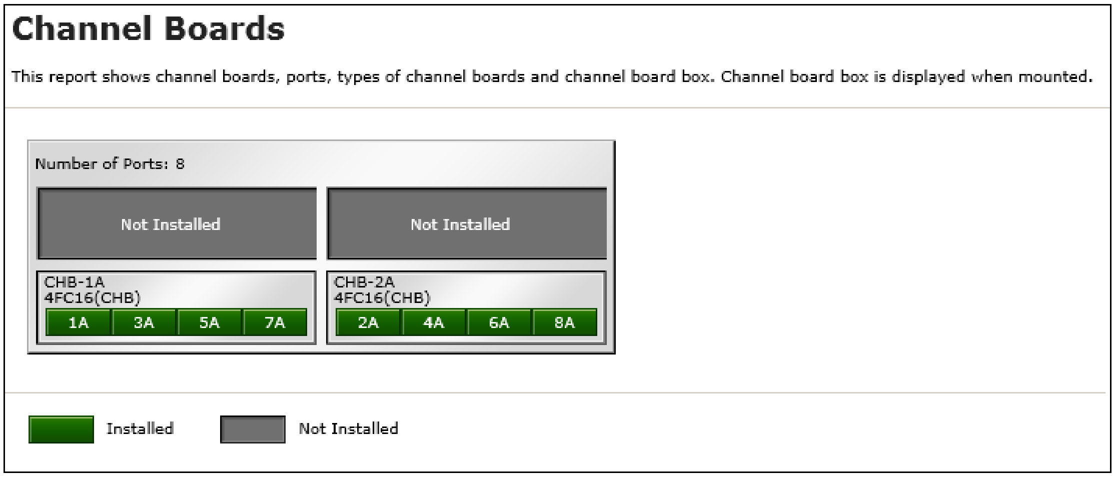
Figure 9 Cache Memories report (VSP G800)

Total capacity of the cache memory and shared memory is displayed separately for each module.

Channel Boards report

This report shows the channel boards and the ports and types of channel boards for each channel board. The keys (green = installed, gray= not installed) show which channel boards are installed and which are not installed.

If a PCIe channel board installed in the DKC is connected to a channel board box, the status of the channel board box is displayed.



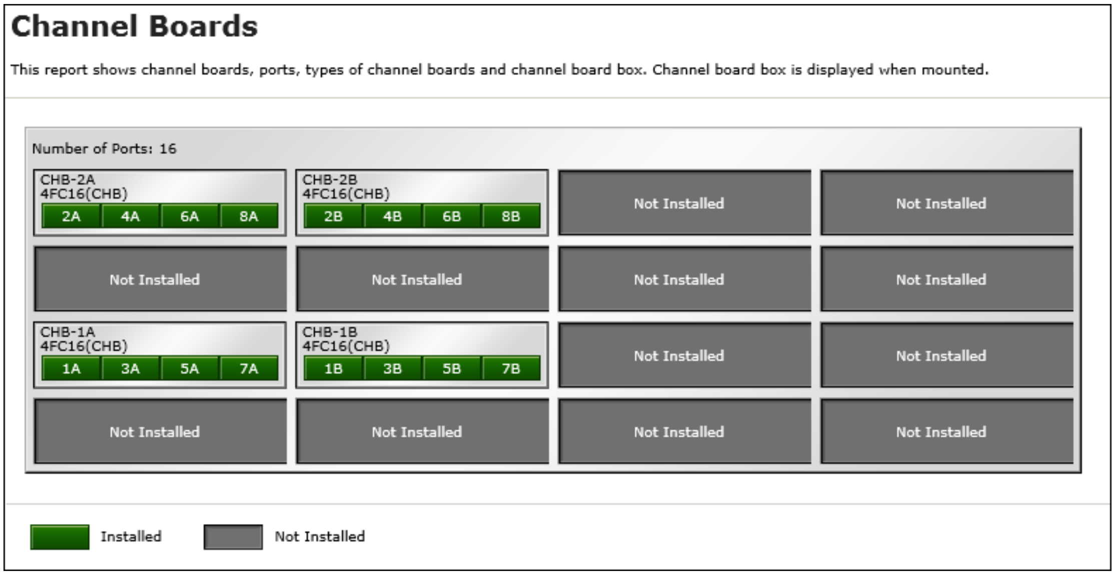
Channel Boards

This report shows channel boards, ports, types of channel boards and channel board box. Channel board box is displayed when mounted.

Number of Ports: 8

🟩 Installed ▨ Not Installed

Figure 10 Channel Boards (VSP G200)



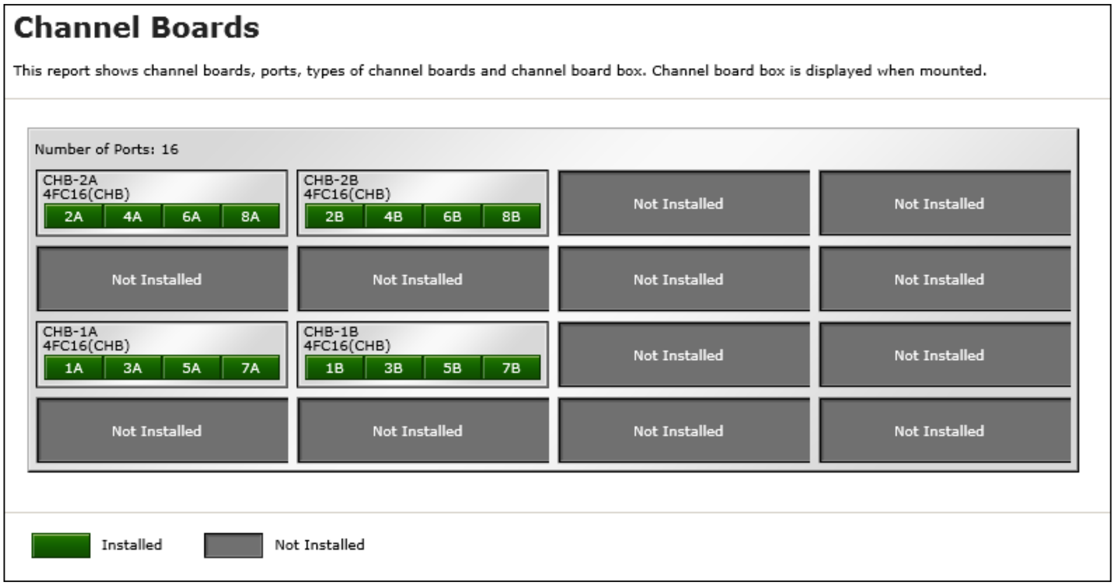
Channel Boards

This report shows channel boards, ports, types of channel boards and channel board box. Channel board box is displayed when mounted.

Number of Ports: 16

🟩 Installed ▨ Not Installed

Figure 11 Channel Boards report (VSP G400, VSP G600)



Channel Boards

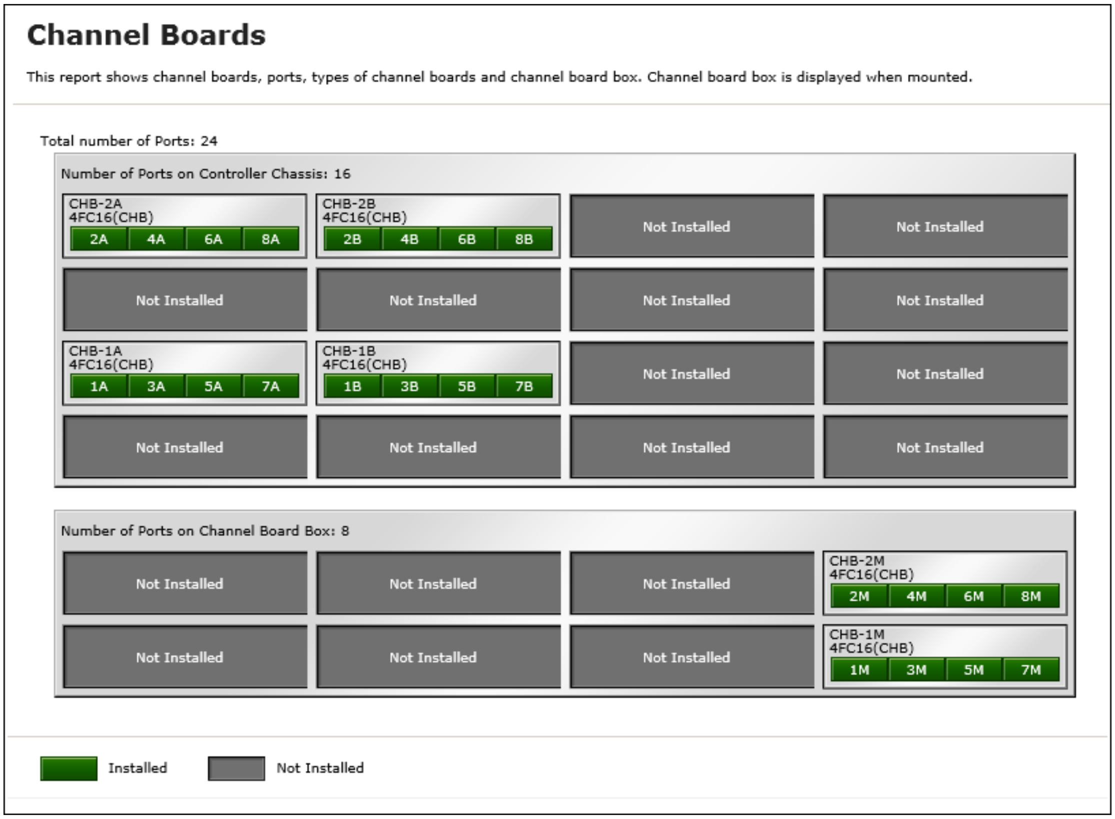
This report shows channel boards, ports, types of channel boards and channel board box. Channel board box is displayed when mounted.

Number of Ports: 16

CHB-2A 4FC16(CHB) 2A 4A 6A 8A	CHB-2B 4FC16(CHB) 2B 4B 6B 8B	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	Not Installed
CHB-1A 4FC16(CHB) 1A 3A 5A 7A	CHB-1B 4FC16(CHB) 1B 3B 5B 7B	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	Not Installed

🟩 Installed ▨ Not Installed

Figure 12 Channel Boards report (VSP G800)



Channel Boards

This report shows channel boards, ports, types of channel boards and channel board box. Channel board box is displayed when mounted.

Total number of Ports: 24

Number of Ports on Controller Chassis: 16

CHB-2A 4FC16(CHB) 2A 4A 6A 8A	CHB-2B 4FC16(CHB) 2B 4B 6B 8B	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	Not Installed
CHB-1A 4FC16(CHB) 1A 3A 5A 7A	CHB-1B 4FC16(CHB) 1B 3B 5B 7B	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	Not Installed

Number of Ports on Channel Board Box: 8

Not Installed	Not Installed	Not Installed	CHB-2M 4FC16(CHB) 2M 4M 6M 8M
Not Installed	Not Installed	Not Installed	CHB-1M 4FC16(CHB) 1M 3M 5M 7M

🟩 Installed ▨ Not Installed

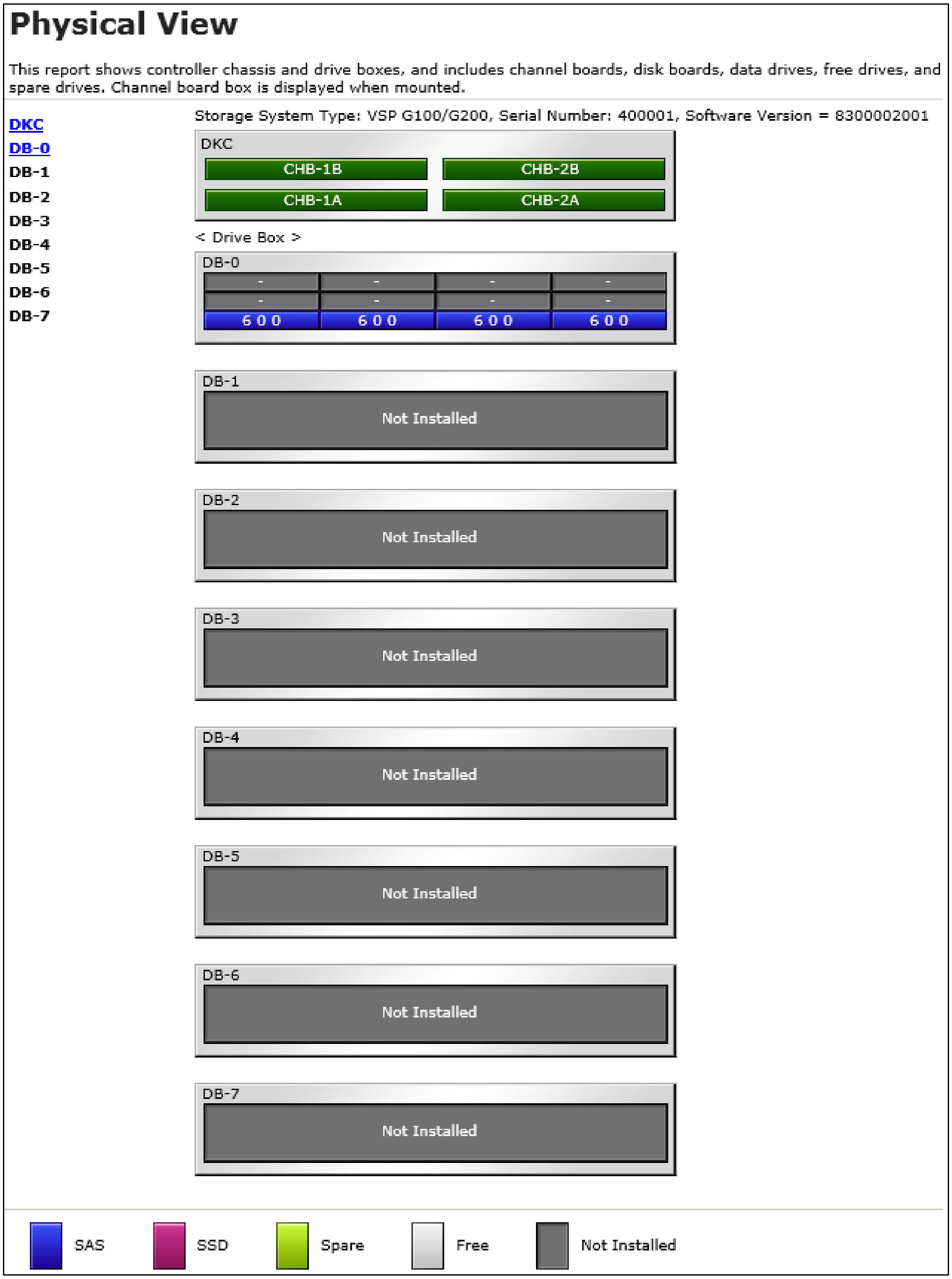
Figure 13 Channel Boards report (when a channel board box is connected)

Physical View report

This report shows disk controller chassis and drive boxes, and includes channel boards, disk boards, data drives, spare drives, and free drives.

It also shows the storage system type, serial number, and software version. You can check the legend for disk units, such as SAS, SSD, Spare, Free, or Not Installed.

If a PCIe channel board installed in the DKC is connected to a channel board box, the status of the channel board box is displayed.



Physical View

This report shows controller chassis and drive boxes, and includes channel boards, disk boards, data drives, free drives, and spare drives. Channel board box is displayed when mounted.

DKC
DB-0
DB-1
DB-2
DB-3
DB-4
DB-5
DB-6
DB-7

Storage System Type: VSP G100/G200, Serial Number: 400001, Software Version = 8300002001

DKC

CHB-1B	CHB-2B
CHB-1A	CHB-2A

< Drive Box >

DB-0

-	-	-	-
-	-	-	-
600	600	600	600

DB-1

Not Installed

DB-2

Not Installed

DB-3

Not Installed

DB-4

Not Installed

DB-5

Not Installed

DB-6

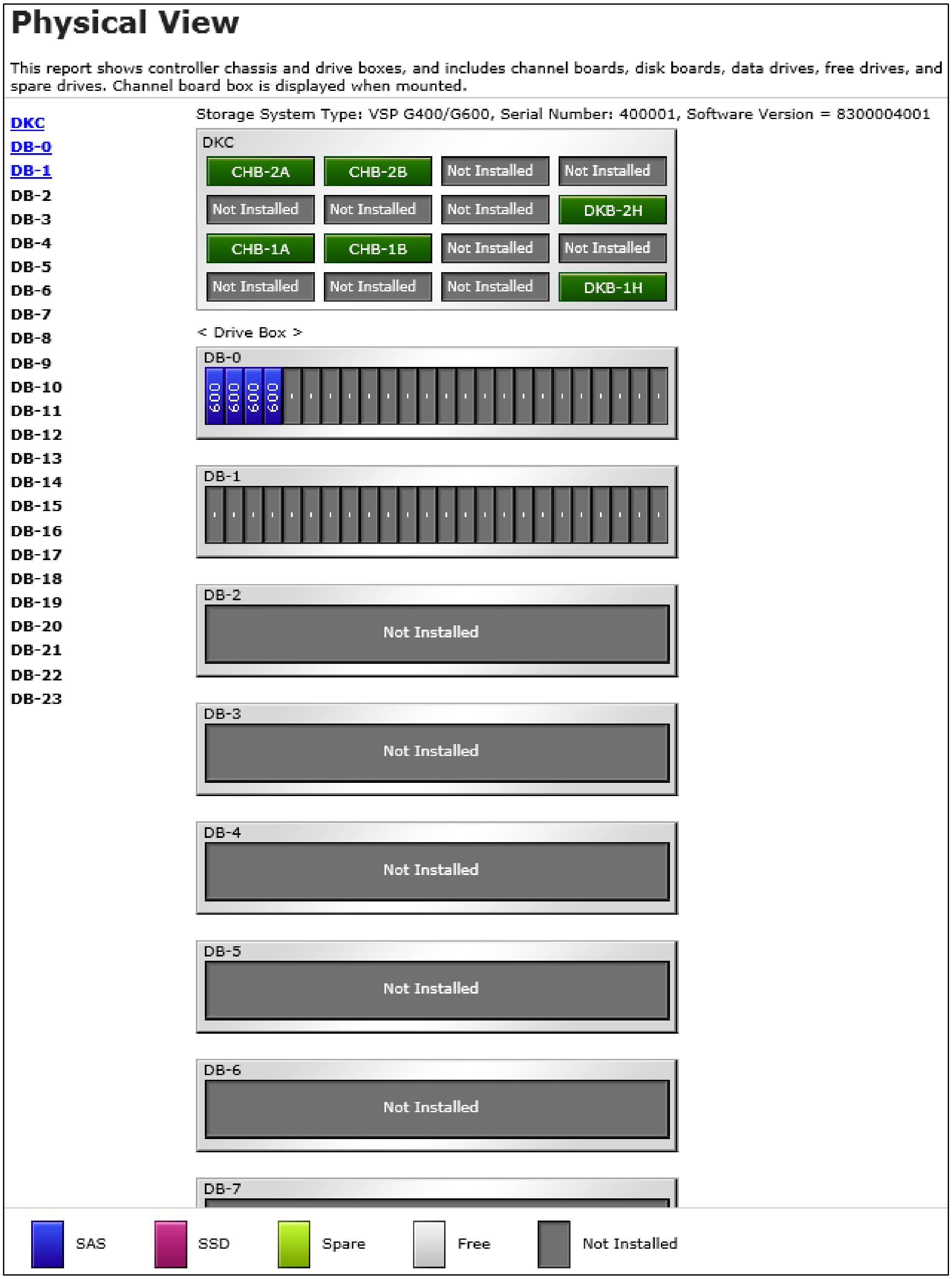
Not Installed

DB-7

Not Installed

🟦 SAS 🟪 SSD 🟩 Spare ⬜ Free ⬛ Not Installed

Figure 14 Physical View report (VSP G200)



Physical View

This report shows controller chassis and drive boxes, and includes channel boards, disk boards, data drives, free drives, and spare drives. Channel board box is displayed when mounted.

DKC
DB-0
DB-1
DB-2
DB-3
DB-4
DB-5
DB-6
DB-7
DB-8
DB-9
DB-10
DB-11
DB-12
DB-13
DB-14
DB-15
DB-16
DB-17
DB-18
DB-19
DB-20
DB-21
DB-22
DB-23

Storage System Type: VSP G400/G600, Serial Number: 400001, Software Version = 8300004001

DKC

CHB-2A	CHB-2B	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	DKB-2H
CHB-1A	CHB-1B	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	DKB-1H

< Drive Box >

DB-0

DB-1

DB-2

Not Installed

DB-3

Not Installed

DB-4

Not Installed

DB-5

Not Installed

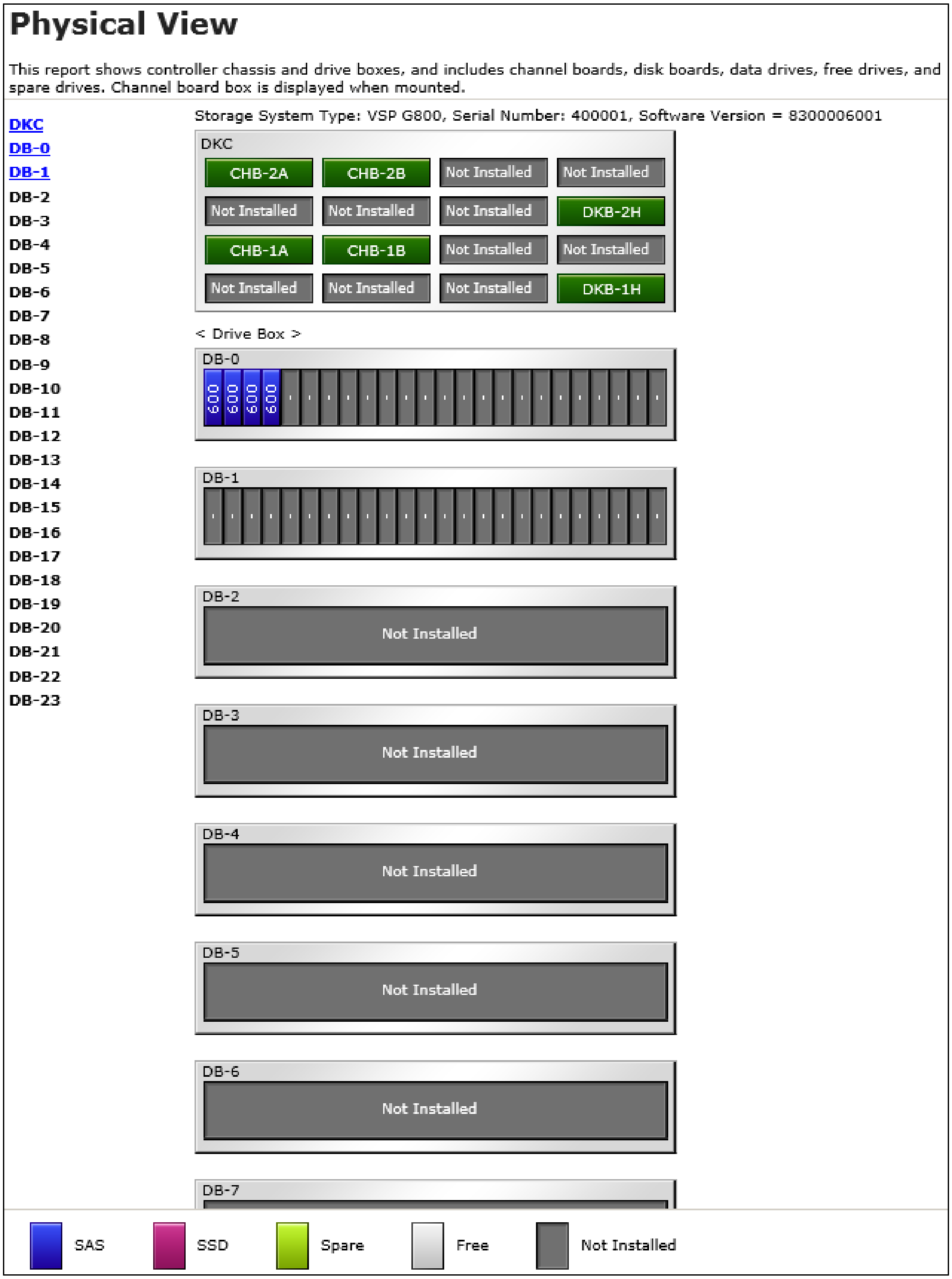
DB-6

Not Installed

DB-7

🟦 SAS 🟪 SSD 🟩 Spare ⬜ Free ⬛ Not Installed

Figure 15 Physical View report (VSP G400, VSP G600)



Physical View

This report shows controller chassis and drive boxes, and includes channel boards, disk boards, data drives, free drives, and spare drives. Channel board box is displayed when mounted.

DKC
DB-0
DB-1
DB-2
DB-3
DB-4
DB-5
DB-6
DB-7
DB-8
DB-9
DB-10
DB-11
DB-12
DB-13
DB-14
DB-15
DB-16
DB-17
DB-18
DB-19
DB-20
DB-21
DB-22
DB-23

Storage System Type: VSP G800, Serial Number: 400001, Software Version = 8300006001

DKC

CHB-2A	CHB-2B	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	DKB-2H
CHB-1A	CHB-1B	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	DKB-1H

< Drive Box >

DB-0

600 600 600 600

DB-1

DB-2

Not Installed

DB-3

Not Installed

DB-4

Not Installed

DB-5

Not Installed

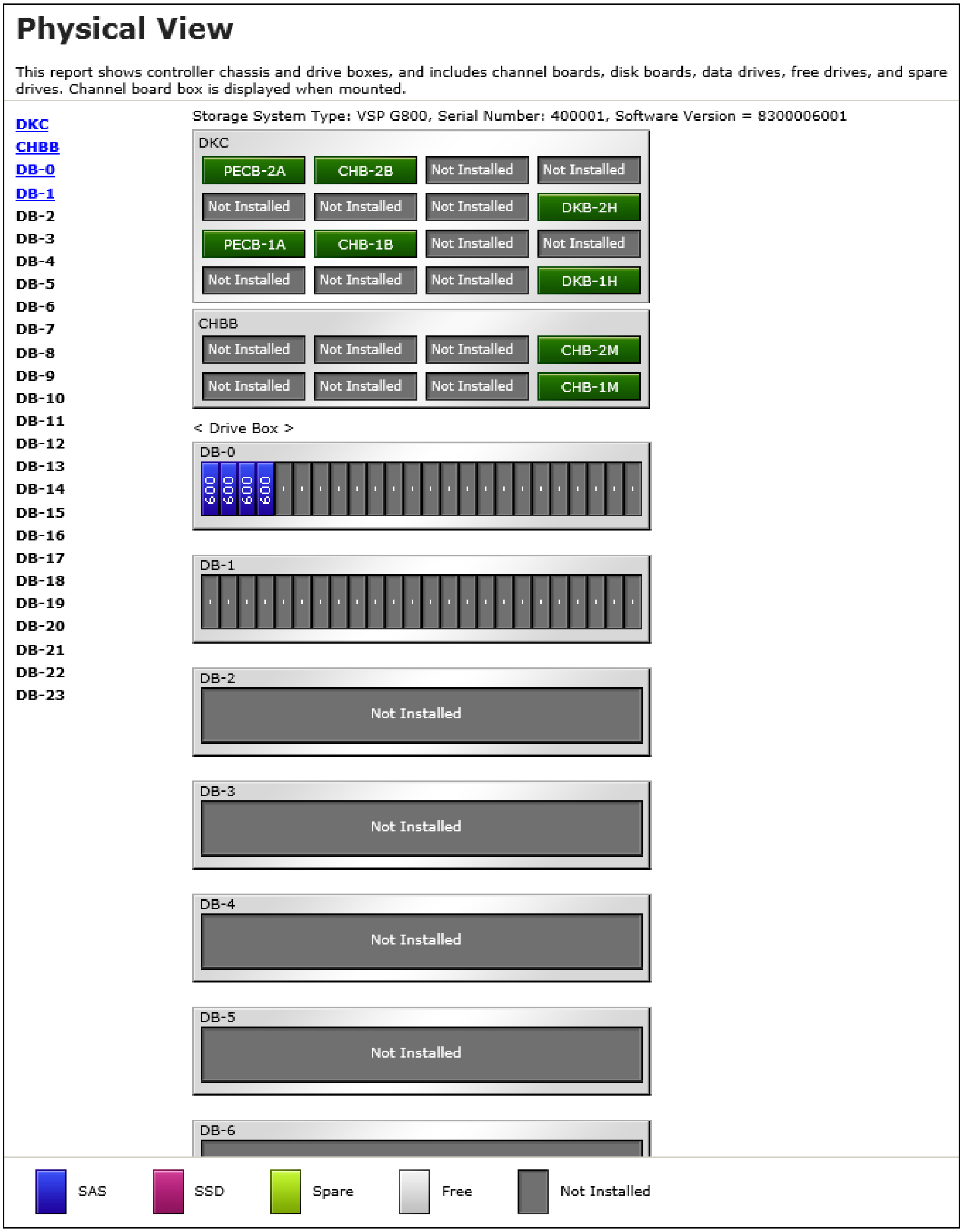
DB-6

Not Installed

DB-7

🟦 SAS 🟪 SSD 🟩 Spare ⬜ Free ⬛ Not Installed

Figure 16 Physical View report (VSP G800)



Physical View

This report shows controller chassis and drive boxes, and includes channel boards, disk boards, data drives, free drives, and spare drives. Channel board box is displayed when mounted.

DKC
CHBB
DB-0
DB-1
DB-2
DB-3
DB-4
DB-5
DB-6
DB-7
DB-8
DB-9
DB-10
DB-11
DB-12
DB-13
DB-14
DB-15
DB-16
DB-17
DB-18
DB-19
DB-20
DB-21
DB-22
DB-23

Storage System Type: VSP G800, Serial Number: 400001, Software Version = 8300006001

DKC

PECB-2A	CHB-2B	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	DKB-2H
PECB-1A	CHB-1B	Not Installed	Not Installed
Not Installed	Not Installed	Not Installed	DKB-1H

CHBB

Not Installed	Not Installed	Not Installed	CHB-2M
Not Installed	Not Installed	Not Installed	CHB-1M

< Drive Box >

DB-0

600 600 600 600

DB-1

DB-2

Not Installed

DB-3

Not Installed

DB-4

Not Installed

DB-5

Not Installed

DB-6

🟦 SAS 🟪 SSD 🟩 Spare ⬜ Free ⬛ Not Installed

Figure 17 Physical View report (when a channel board box is connected)

CSV files

This topic describes reports that are saved in CSV format.

AllConf.csv

This is the concatenated file of all the csv files.

CacheInfo.csv

This CSV file contains information about the cache memory on the controller board. A record is created for each cache memory.

Table 14 CacheInfo.csv file (Title: <<Cache>>)

Item	Content
Location	Name of the cache controller board on which the memory is installed
CMG#0 Size (GB) CMG#1 Size (GB)	Cache memory capacity in the controller board per CMG (16/32/64/128/ blank). The number of CMG differs by model and the displayed items are different. • VSP G200: Only CMG#0 Size displays • VSP G400, G600, G800 or VSP F400, F600, F800: CMG#0 Size and CMG#1 Size display Depending on the installed number of the cache memory (DIMM), one of the CMG capacities might be blank for VSP G400, G600, G800 or VSP F400, F600, F800.
Cache Size (GB)	Total cache memory capacity on the controller board (0 to 256)
SM Size (MB)	The capacity that cannot be used as data cache memory in the total cache memory capacity inside of the controller board. The capacity per cluster is displayed. Includes the shared memory capacity, cache directory capacity, and the fixed capacity. Fixed capacity is the cache memory capacity that is used for controlling the storage system with the controller board. • VSP G200: (0 to 18944) • VSP G400, G600 or VSP F400, F600: (0 to 37888) • VSP G800 or VSP F800: (0 to 47744)
CFM#0 Type CFM#1 Type	Type of CFM in the cluster (BM 10/BM 20/BM 30/blank). The number of CFM differs by model and the number of the displayed items are different. • • VSP G200: CFM#0 type only • VSP G400, G600, G800 or VSP F400, F600, F800: CFM #0 Type or CFM#1 Type Depending on the installed CFM number, one of the CFM types might be displayed as blank.

ChapUserInfo.csv

This CSV file contains information about the iSCSI CHAP authenticated user registered to the port in the channel board. A record is created for each target related to the CHAP authenticated user.

Table 15 ChapUserInfo.csv file Title: <<CHAP User Information>>)

Item	Content
Port	Port name
User Name	Name of the CHAP authenticated user[1]
iSCSI Target ID[2]	The iSCSI number of the target (00 to fe, hexadecimal)
Notes: **1.** If the character string contains a comma, the comma is converted to a tab. **2.** For the target information, see the record information with the same iSCSI target ID in IscsiTargetInfo.csv.	

ChaStatus.csv

This CSV file contains information about the status of each channel board (CHB). A record is created for each CHB.

Table 16 ChaStatus.csv file (Title: <<CHB Status>>)

Item	Content
CHB Location	CHB name
PCB Status	Status of this CHB[1]
Port#00, #01, …, #03	Status of ports on this CHB
Notes: **1.** 1 Normal, 0: Abnormal	

DeviceEquipInfo.csv

This CSV file contains information about equipment and devices that are part of the storage system, including power supplies and batteries for DKC, DB, and CHBB. A record is created for each device.

Table 17 DeviceEquipInfo.csv file (Title: <<Device Equipment Information>>)

Item	Content
Device Location	Device location name. For example: • For DKCPS: DKCPS-00 • For DKUPS: DKUPS000-1 • For Battery: BATTERY-1BA • For SVP: SVP-BASIC
Equip Status	Equipment status of the device: • Equipped • Not Equipped
Status	Status of the device: • Normal • Abnormal • Blank if "Equip Status" is Not Equipped

DkaInfo.csv

This CSV file contains information about disk boards (DKBs). A record is created for each DKB.

Table 18 DkaInfo.csv file (Title: <<DKB Information>>)

Item	Content
DKB Location	DKB name
Package Type	DKB type Output example: • Unecryption DKB (2Port) • Encryption EDKB (2Port)

DkaStatus.csv

This CSV file contains information about the status of disk boards (DKBs). A record is created for each DKB.

Table 19 DkaStatus.csv file (Title: <<DKB Status>>)

Item	Content
DKB Location	DKB name
PCB Status	Status of this DKB[1]
BECON#00	Status of BECON[1]
BEPORT#0000 to #0001	Status of BEPORT on this DKB[1] Items are output in the format BEPORT#*XXYY*, where: • *XX*: BE controller number (2-digit hexadecimal) • *YY*: BE port number (2-digit hexadecimal)
Notes: **1.** 1: Normal, 0: Abnormal	

DkcInfo.csv

This CSV file contains information about the DKC. A record is created for each module.

When Module #1 is not installed, the record for Module #1 is not created.

Table 20 DkcInfo.csv file (Title: <<DKC Information>>)

Item	Content
Storage System Type	Storage system type. Output example: • S: VSP G200 • M: VSP G400, G600 or VSP F400, F600[1]

Item	Content
	• H: VSP G800 or VSP F800
Serial Number #	Serial product number (decimal, from 400001 to 499999)
IP Address	IP address Output example: xxx.xxx.xxx.xxx (decimal, 0 to 255)
Subnet Mask	Subnet mask Output example: xxx.xxx.xxx.xxx (decimal, 0 to 255)
Number of CUs	Number of CUs (decimal, 0 to 64)
Number of DKBs	Number of DKBs (decimal, 0 to 8) Zero (0) is sometimes displayed if an HDD is not installed.
Configuration Type	Configuration type Output example: PCM
Model	Storage system model: S, M, or H

Notes:

- To determine the model type, see Model upgrade license in Program Product Name in PpInfo.csv on page 183.
  - VSP G400 or VSP F400: Install is Disabled for Model upgrade license
  - VSP G600 or VSP F600: Install is Enabled for Model upgrade license

ELunInfo.csv

This CSV file contains information about external volumes. Information about one external volume is output to multiple records according to the number of prioritized paths between the local and the external storage systems.

For details of external volumes, see *Hitachi Universal Volume Manager User Guide*.

Table 21 ELunInfo.csv file (Title: <<External LUN Information>>)

Item	Content
VDEV#	Virtual device number to which the external volume is mapped
Characteristic1	Identification number of the external volume[1]
Characteristic2	Extended information for identifying the external volume
Device	Product name reported to the host by the external volume[1]
Capacity(blocks)	Capacity of the external volume (in blocks)
Cache Mode	Indicates whether the write data from the host to the external storage system is reflected synchronously or asynchronously • Enabled: Asynchronously • Disabled: Synchronously
ECC Group	Number of parity group to which the external volume is mapped. If the number starts with "E" (for example, E1-1), the parity group contains external volumes. Range of values: E1-1 to E16384-4096

Item	Content
Current MPU	Number and name of a current MP unit controlling the parity group to which the external volume is mapped • MPU-10 • MPU-11 • MPU-20 • MPU-21
Setting MPU	Number and name of an MP unit configured to control the external volume indicated by ECC Group • MPU-10 • MPU-11 • MPU-20 • MPU-21
Vendor	Vendor name of the external storage system
Product Name	Product name of the external storage system
Serial Number#	Serial product number of the external storage system
Path Mode	Mode which indicates how the paths between local and external storage systems operate • Multi • Single • ALUA
Port	Name of a local port from which the external path is connected to the external storage system
WWN	Port identifier number of the external storage system Blank if "Package Type" is iSCSI
LUN	LU number set for the external volume.
Priority	Priority of the paths between the storage systems to be used for connection with the external volume. "1" indicates the path of the highest priority.
Status	Status of the path between storage systems. • Normal • Blocked
IO TOV	I/O timeout value for the external volume Range of values: 5 to 240
QDepth	The number of Read/Write commands that can be issued to the external volume at a time Range of values: 2 to 128
Resource Group ID (ECC Group)	Resource group ID for the parity group that is mapping external volumes (in decimal format) Range of values: 0 to 1023
Resource Group Name (ECC Group)	Resource group name of the parity group that is mapping external volumes
Load Balance Mode	I/O load balance distribution logic specified for external volume • Normal Round-robin • Extended Round-robin • Disabled

Item	Content
	A hyphen is displayed if Single is specified in Path Mode
Path Mode on Profile	Path mode on profile information of the external storage system: • Multi • Single
ALUA Settable	Indicates whether ALUA mode can be set as path mode on the external storage system • Yes: ALUA mode can be set • No: ALUA mode cannot be set
ALUA Permitted	Indicates whether ALUA is used as path mode on the local storage system: • Enabled: ALUA mode is used • Disabled: ALUA mode is not used
Target Port Asymmetric Access State	Status of the port on the external storage system when the path mode is ALUA: • Active/Optimized • Active/Non-Optimized
Package Type	Type of CHB to which a port of the local storage system connecting to the external storage system belongs • Fibre: 8FC4 (CHB), 16FC2 (CHB) • iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB)
IP Address	IP address for iSCSI Target of an external storage system • IPv6 *XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX* (hexadecimal) • IPv4 *XXX*.*XXX*.*XXX*.*XXX* (decimal) • Blank if "Package Type" is iSCSI.
TCP Port Number	TCP port number (1 through 65535) for iSCSI Target of an external storage system. Blank if "Package Type" is Fibre.
iSCSI Target Name	iSCSI Target name of an external storage system Blank if "Package Type" is Fibre.
Notes: **1.** If the character string contains a comma, the comma is converted to a tab.	

EnvMonInfo.csv

This CSV file contains information about the power and temperature of the storage system. Power and temperature measurements from the environment monitor are recorded every two hours.

No records are created during a system power failure or if the breakers are turned off. If the system is in maintenance mode or the SVP is rebooted, up to two hours of records could be lost.

Table 22 EnvMonInfo.csv file (Title: <<Electric power and temperature Information>>)

Item	Description
Date	Year, month, and date when record data was acquired for the two-hour period in the format:

Item	Description
	YYYY/*MM*/*DD HH*:*MM*:*SS*
Electric power average	Average value of electric power (W)
Electric power maximum value	Maximum value of electric power (W)
Electric power minimum value	Minimum value of electric power (W) In the following cases, a lower value might be temporarily displayed: • When the storage system is starting up • Right after replacing storage system parts • During or after microcode update
DKC0 CL1 Temperature average	DKC0: Average temperature of CL1 (°C)
DKC0 CL1 Temperature maximum value	DKC0: Maximum temperature of CL1 (°C)
DKC0 CL1 Temperature minimum value	DKC0: Minimum temperature of CL1 (°C)
DKC0 CL2 Temperature average	DKC0: Average temperature of CL2 (°C)
DKC0 CL2 Temperature maximum value	DKC0: Maximum temperature of CL2 (°C)
DKC0 CL2 Temperature minimum value	DKC0: Minimum temperature of CL2 (°C)

FcSpNameInfo.csv

This CSV file contains information about Fibre Channel Security Protocols (FCSPs). A record is created for each initiator (host).

For details of port setting, see the *Provisioning Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*.

Table 23 FcSpNameInfo.csv file (Title: <<FC-SP Name Information>>)

Item	Content
Port	Port name
Host Group	Host group name
Target Username	WWN information about the storage system required for authentication (16-digit hexadecimal number)
Authentication of Group	Information about whether to perform authentication or not • Enabled • Disabled
Initiator Username	WWN information about the host required for authentication (16-digit hexadecimal number)
Protocol	Protocol used for authentication ("CHAP" or blank)

FcSpPortInfo.csv

This CSV file contains information about ports related to Fibre Channel Security Protocols (FCSPs). A record is created for each port.

For details of port setting, see the *Provisioning Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*.

Table 24 FcSpPortInfo.csv file (Title: <<FC-SP Port Information>>)

Item	Content
Port	Port name
Time out(Sec)	Time interval (in seconds) before retrying authentication in case of failure in authentication
Refusal Intvl.(Min)	Time interval (in minutes) before starting next authentication in case of failure in authentication for the number of times displayed by "Refusal Freq(Counts)"
Refusal Freq.(Counts)	Number of times of authentication allowable for connection to a port
Switch Port Username	WWN information about the Fabric switch required for authentication (16-digit hexadecimal number)
Mode	Mode of authentication between ports and FC switches • Bidirectional • Unidirectional
Authentication of Fabric Switch	Information about whether to perform authentication of the FC switch identified by "Switch Port Username" • Enabled • Disabled

HduInfo.csv

This CSV file contains information about hard drive boxes (DB). A record is created for each drive box.

Table 25 DBInfo.csv file (Title: <<DB Information>>)

Item	Description
DB Location	DB location name
DB Status	Information about whether this DB is installed • Installed • Not installed
Slot Size	Slot size (inches) • 2.5 • 3.5 • Blank for DBF (FMC and FMD)
DB Type	DB type • DBS (DB for 2.5-inch drives) • DBL (DB for 3.5-inch drives) • DB60 (dense drive box for 3.5-inch drives) • DBF (DB for FMC and FMD)

IscsiHostInfo.csv

This CSV file contains information about iSCSI Initiator (Host) set to the channel board port. A record is created for each iSCSI Host (Initiator) target.

Table 26 IscsiHostInfo.csv file (Title: <<iSCSI Host Information>>)

Item	Content
Port	Port name
iSCSI Name	iSCSI host name
Host Name	Nickname for iSCSI host name
iSCSI Target ID[1]	iSCSI target number (hexadecimal format, 00 to fe)

Notes:

1. For the target information, see the record information with the same iSCSI target ID in IscsiTargetInfo.csv.

IscsiPortInfo.csv

This CSV file contains information about iSCSI information set to the channel board port. A record is created for each iSCSI host (initiator) target.

Table 27 IscsiPortInfo.csv file (Title: <<iSCSI Port Information>>)

Item	Content
Port	Port name
IPv4 | IP Address	IPv4 address Output example: *xxx.xxx.xxx.xxx* (decimal)
IPv4 | Subnet Mask	IPv4 subnet mask (decimal) Output example: *xxx.xxx.xxx.xxx* (decimal)
IPv4 | Default Gateway	Port IPv4 default gateway Output example: *xxx.xxx.xxx.xxx* (decimal)
IPv6 | Mode	Port IPv6 settings • Enabled • Disabled
IPv6 | Link Local Address	Port IPv6 link local address • Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal) • Output example: Auto Auto is displayed if the link local address is automatically set. Blank if "IPv6 | Mode" is Disabled.
IPv6 | Global Address	IPv6 global address of the port • Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal) • Output example: Auto Auto is displayed if the global address is automatically set. Blank if "IPv6 | Mode" is Disabled.
IPv6 | Assigned Default Gateway	Port IPv6 assigned default gateway • Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal)

Item	Content
	Blank if "IPv6 | Mode" is Disabled.
Channel Speed	Data transfer speed of the port (10Gbps)
Security Switch	Port security switch settings • On • Off
TCP Port Number	The number of the port for using socket (1 to 65535)
Ethernet MTU Size (Byte) | MTU	MTU settings • 1500 • 4500 • 9000
Keep Alive Timer (sec.)	Keep alive timer value of iSCSI (30 to 64800) (sec)
Selective ACK	Selective ACK mode • Enabled • Disabled
Delayed ACK	Delayed ACK mode • Enabled • Disabled
Maximum Window Size (KB)	Window scale option settings • 64KB • 128KB • 256KB • 512KB • 1024KB
iSNS Server | Mode	iSNS mode settings • On • Off
iSNS Server | IP Address	IP address of the iSNS server • IPv4: *xxx.xxx.xxx.xxx* (decimal) • IPv6: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal) • Blank if "iSNS Server | Mode" is Off.
iSNS Server | TCP Port Number	Port number of TCP used for iSNS (1 to 65535). Blank if "iSNS Server | Mode" is Off.
VLAN | Tagging Mode	VLAN tagging mode set to the port • On • Off
VLAN | ID	VLAN number set to the port (1 to 4094) Blank if "VLAN | Tagging Mode" is set to Off.
Resource Group ID (Port)	Resource group ID of the port (0 to 1023 in decimal)
Resource Group Name(Port)	Resource group name of the port
iSCSI Name	iSCSI name of the port
CHAP User Name	Authenticated user name of the port

IscsiTargetInfo.csv

This CSV file contains information about iSCSI target information set to the channel board port. A record is created for each iSCSI target.

Table 28 IscsiTargetInfo.csv file (Title: <<iSCSI Target Information>>)

Item	Content
Port	Port name
iSCSI Target Alias	iSCSI target alias
iSCSI Target ID	Number of the iSCSI target (00 to fe, hexadecimal)
iSCSI Target Name	Name of the iSCSI target
Host Mode	Host mode set to the iSCSI target (hexadecimal)
Host Mode Option	Host mode option set to the iSCSI target (0 to 127, decimal) Separated with a semicolon (;) if multiple host mode options are set.
Security Switch	Security switch status set to the iSCSI target port • On • Off
Authentication | Method	Authentication method settings of the iSCSI target • CHAP • None • Comply with Host Setting
Authentication | Mutual CHAP	Mutual CHAP authentication function settings of the iSCSI target • Enabled • Disabled
Authentication | User Name	User name set when iSCSI target was authenticated
Resource Group ID (iSCSI Target)	Resource group ID of the iSCSI target (0 to 1023)
Resource Group Name (iSCSI Target)	Resource group name of the iSCSI target

JnlInfo.csv

This CSV file contains information about journals. A record is created for each journal.

Table 29 JnlInfo.cvs file (Title: <<JNL Information>>)

Item	Content
JNL#	Journal number (in hexadecimal)
Current MPU	Number and name of MP unit currently controlling the journal (MPU-10, MPU-11, MPU-20, MPU-21)
Setting MPU	Number and name of MP unit configured to control the journal (MPU-10, MPU-11, MPU-20, MPU-21)

LdevCapaInfo.csv

This CSV file contains information about LDEV capacities. A record is created for each of the classifications shown in "Volume Kind".

Table 30 LdevCapaInfo.csv file (Title: <<LDEV Capacity Information>>)

Item	Content
Volume Kind	The following classifications are output: - Internal OPEN Volumes - External OPEN Volumes - Total OPEN Volumes
Allocated LDEV Capacity (GB)	Allocated LDEV capacity
Unallocated LDEV Capacity (GB)	Unallocated LDEV capacity
Reserved Capacity (GB)	Reserved LDEV capacity
Total Volume Capacity (GB)	Total capacity of "Allocated LDEV Capacity", "Unallocated LDEV Capacity" and "Reserved Capacity"
Free Space (GB)	Free Space
Total Capacity (GB)	Total Capacity The sum of "Total Volume Capacity" and "Free Space"

LdevCountInfo.csv

This CSV file contains information about the number of logical devices (LDEVs). A record is created for each of the classifications shown in "Volume Kind".

Table 31 LdevCountInfo.csv file (Title: <<LDEV Count Information>>)

Item	Content
Volume Kind	The following classifications are output: - Internal Volumes - External Volumes - Total Volumes
Allocated OPEN LDEVs	The number of allocated open-system volumes (LDEVs).
Unallocated OPEN LDEVs	The number of unallocated open-system volumes (LDEVs).
Reserved OPEN LDEVs	The number of reserved open-system volumes (LDEVs).
V-VOL	The number of virtual volumes. Output only when "Volume Kind" is Total Volumes.
Total(All LDEVs)	Total number of LDEVs.
ECC Groups	Total number of parity groups.

LdevInfo.csv

This CSV file contains information about logical devices (LDEVs). A record is created for each LDEV.

For details of LDEVs, see the *Provisioning Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*.

Table 32 Ldevinfo.csv file (Title: <<LDEV Status>>)

Item	Content
ECC Group	Number of parity group where the LDEV belongs. Output example: *X*-*Y* (decimals) • If the number starts with "E" (for example, E1-1), the parity group contains external volumes. • If "LDEV Type" is Dynamic Provisioning or Thin Image, a hyphen is output.
LDEV#	LDEV number (00:00:00 to 00:3f:ff)
LDEV Name	LDEV name[1]
LDEV Emulation	LDEV emulation type
LDEV Type	LDEV type: • Basic • Dynamic Provisioning • External • Thin Image • ALU
LDEV Attribute	LDEV Attribute: • CMDDEV (Command device) • CMDDEV[1] (Remote command device) • Journal (Journal volume) • Pool (Pool volume) • Quorum disk (used with global-active device) • ALU • SLU • Regular (Others)
Volume Size(Cyl)	LDEV capacity (in cylinders)
Volume Size(MB)	LDEV capacity (in MB)
Volume Size(Blocks)	LDEV capacity (in blocks)
CVS	Information about whether the LDEV is a custom-sized volume: • On: Custom-sized volume • Off: Others
Pool ID	Pool number. This is blank except for the following cases: • If "LDEV Type" is Dynamic Provisioning • If LDEV Attribute is Pool
RAID Concatenation#0	Number of parity group to be concatenated to parity group (#0) identified by ECC Group. Blank if the parity group is not concatenated to another parity group.
RAID Concatenation#1	Number of parity group to be concatenated to parity group (#1) identified by ECC Group. Blank if the parity group is not concatenated to another parity group.
RAID Concatenation#2	Number of parity group to be concatenated to parity group (#2) identified by ECC Group. Blank if the parity group is not concatenated to another parity group.
ORACLE CHECK SUM	Information about whether this LDEV is an Oracle check sum target. • On • Off
Current MPU	Number of the MP unit currently controlling the LDEV. (MPU-10, MPU-11, MPU-20, MPU-21)

Item	Content
Setting MPU	Number of the MP unit configured to control LDEV. (MPU-10, MPU-11, MPU-20, MPU-21)
Allocated	Information about whether this LDEV is allocated to a host. • "Y" is output for volumes accessible to the host.
Pool Name	The pool's name[1] • If the provisioning type is Dynamic Provisioning, the name of the pool related to the logical volume is displayed. • If the attribute is Pool, the name of the pool where the logical volume belongs is displayed. • When neither of the above are displayed, the pool name is blank.
CmdDevSecurity	Indicates whether Security is specified as the attribute for the command device. • Enabled: Command device security setting is set. • Disabled: Command device security setting is not set. • Blank: "LDEV Attribute" is not CMDDEV.
CmdDevUserAuth	Indicates whether User Authentication is specified as the attribute for the command device. • Enabled: User authentication setting is set. • Disabled: User authentication setting is not set. • Blank: "LDEV Attribute" is not CMDDEV.
CmdDevDevGrpDef	Indicates whether Device Group Definition is specified as the attribute for the command device. • Enabled: Device group definition setting is set. • Disabled: Device group definition setting is not set. • Blank: "LDEV Attribute" is not CMDDEV.
Resource Group ID (LDEV)	LDEV resource group ID (number in the decimal format)
Resource Group Name (LDEV)	LDEV resource group name (0 to 1,023, decimal)
Encryption	Information about whether the parity group identified by ECC Group is encrypted. • For Internal Volumes: Enabled (encrypted) or Disabled • For External Volumes: blank
T10 PI	Indicates the T10 PI attribute set for the LDEV. • Enabled • Disabled • Blank if "LDEV Emulation" is not OPEN-V.
Notes: **1.** If the character string contains a comma, the comma is converted to a tab.	

LdevStatus.csv

This CSV file contains information about the status of logical devices (LDEVs). A record is created for each LDEV.

Table 33 LdevStatus.csv file (Title: <<LDEV Status>>)

Item	Content
VDEV#	Virtual device number in which the LDEV is defined
VDEV Status	VDEV status of "VDEV#"

Item	Content
	- 1: Normal - 0: Abnormal
HDEV#	LDEV number
HDEV Status	LDEV status - 1: Normal - 0: Abnormal
LDEV Emulation	LDEV emulation type
ECC Group	Number of the parity group where the LDEV belongs. - If the number starts with "E" (for example, E1-1), the parity group contains external volumes. - If the type of the LDEV is a Dynamic Provisioning or Thin Image virtual volume, a hyphen is output. Refer to "LdevInfo.csv" for information about the LDEV type.

LPartition.csv

This CSV file contains information about the cache logical partitioning function. A record is created for each cache partition for a managed resource.

For details of the cache logical partitioning function, see the *Performance Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*.

Table 34 LPartition.csv file (Title: <<Logical Partitioning>>)

Item	Content
CLPR#	CLPR ID (in decimal)
CLPR Name	CLPR name
Cache Size(MB)	Cache size allocated to this CLPR (in MB)
ECC Group	Number of parity group allocated to this CLPR. - If the number starts with "E" (for example, E1-1), the parity group contains external volumes. - If the type of the LDEV is a Dynamic Provisioning or Thin Image virtual volume, a hyphen is output. Refer to "LdevInfo.csv" for information about the LDEV type.
LDEV#(V-VOL)	LDEV number allocated to this CLPR. - VSP G200: (00:00:00 to 00:07:ff) - VSP G400, G600 or VSP F400, F600: (00:00:00 to 00:0f:ff) - VSP G800 or VSP F800: (00:00:00 to 00:3f:ff) The type of this LDEV is Dynamic Provisioning, Thin Image, or ALU.

LunInfo.csv

This CSV file contains information about LU path definitions. A record is created for each host group. For more information about LU path definitions, see the *Provisioning Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*.

Table 35 LunInfo.csv file (Title: <<LUN Information>>)

Item	Description
Port	Port name
Host Group	Host group name If "Package Type" is iSCSI, the iSCSI target alias is output.
Host Mode	Host mode specified for this host group (hexadecimal)
Host Mode Option	Host mode option set for this host group (0 to 127, hexadecimal) If more than one option is specified, the options are separated by semicolons (;).
LUN#	LUN number for this LU path definition (hexadecimal)
LDEV#	LDEV number for this LU path definition
Command Device	Information about whether the LDEV is a command device: • On: Command Device • On*: Remote Command Device • Off: Others
Command Security	Information about whether the command device is secured: • On • Off
CVS	Information about whether the LDEV is a custom-sized volume: • On: Customized volume • Off: Other volumes
CHB Location	Name of the CHB on which this port is installed
Package Type	CHB type for CHB Location: • Fibre: ○ `8FC4 (CHB)` ○ `16FC2 (CHB)` • iSCSI: ○ `10iSCSI2o (CHB)` ○ `10iSCSI2c (CHB)`
Resource Group ID (Host Group)	Resource group ID of a host group (0 to 1,023, decimal)
Resource Group Name (Host Group)	Resource group name of a host group
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port for which the LU path is defined. • Enabled • Disabled • Blank if "Package Type" is not 16FC2 (CHB)
T10 PI	Information about the T10 PI attribute which is set for the LDEV number of the LU path definition. • Enabled • Disabled • Blank if LDEV# is blank

LunPortInfo.csv

This CSV file contains information about LU path definition. A record is created for each port.

For details of LU path definition, see the *Provisioning Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*.

Table 36 LunPortInfo.csv file (Title: <<LUN Port Information>>)

Item	Content
Port	Port name.
Security Switch	The setting status of the security switch • On • Off
Port Address	Port address (2-digit hexadecimal number) Blank if "Package Type" is iSCSI
Loop ID	Port address (0 - 125, decimal) Blank if "Package Type" is iSCSI
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch: • On • Off • Blank if "Package Type" is iSCSI
Connection	One of the Fibre topology settings: • Point to Point • FC-AL • Blank if "Package Type" is iSCSI
Channel Speed	Channel Speed of this port • 1 Gbps • 2Gbps • 4Gbps • 8Gbps • 10Gbps • 16Gbps • Auto
WWN	WWN of this port (hexadecimal number) Blank if "Package Type" is iSCSI
CHB Location	CHB on which the port is installed
Package Type	CHB type for CHB Location • Fibre: ○ `8FC4 (CHB)` ○ `16FC2 (CHB)` • iSCSI: ○ `10iSCSI2o (CHB)` ○ `10iSCSI2c (CHB)`
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port. • Enabled • Disabled • Blank if "Package Type" is not 16FC2 (CHB)

MicroVersion.csv

This CSV file contains information about software versions.

Table 37 MicroVersion.csv file (Title: <<Software Version>>)

Item	Content
DKCMAIN	The version of the firmware for the RAID storage system (10 digits)
ROM BOOT	ROM BOOT firmware version (6 digits)
RAM BOOT	RAM BOOT firmware version (6 digits)
Config	Config version (8 digits)
HDD	HDD firmware version (4 digits) HDD version in the format "(*HDD-device-type - code*):(*version*)". If an HDD drive is not installed, only a colon is displayed.
Expander	Expander firmware version (6 digits)
CFM	CFM firmware version (8 digits)
DKB	DKB firmware version (6 digits)
Printout Tool	Printout tool version (xx-yy-zz-mm/aa)
CHB (FC16G)	16G FC protocol chip firmware version (8 digits)
CHB (iSCSI)	CHB(iSCSI) protocol chip firmware version (8 digits)
GUM	GUM firmware version (8 digits)

MlcEnduranceInfo.csv

This CSV file contains information about endurance information of MLC. A record is created for each MLC endurance information.

If you change the SVP time 1 month or more, the history acquisition months will not be in order.

Table 38 MlcEnduranceInfo.csv file (Title: <<MLC Endurance Information>>)

Item	Content
ECC Group	Number of parity group of which this MLC (including FMD and FMC) is a component • If it is a spare drive, Spare Drive is displayed. • If it is a free drive, Free Drive is displayed.
CR#	C# and R# (2-digit hexadecimal numbers), which identify the PDEV Output in the format of "*XX*/*YY*" *XX*: C# *YY*: R#
Device Type-Code	Drive type code of this drive Output example: SLR5A-M800SS
Used Endurance Indicator (%)	Current SSD life (0 to 100)
History1 (date)	Date on which SSD life was acquired (1 month ago)

Item	Content
	Output example: *yyyy/mm/dd*
History1 (%)	SSD life (0 to 100)(1 month ago)
History2 (date)	Date on which SSD life was acquired (2 months ago) Output example: *yyyy/mm/dd*
History2 (%)	SSD life (0 to 100) (2 months ago)
History3 (%) ... History 119 (%)	SSD life (0 to 100) (3 months ago ...119 months ago)
History120 (date)	Date on which SSD life was acquired (120 months ago)
History120 (%)	SSD life (0 to 100) (120 months ago)

ModePerLpr.csv

This CSV file contains information about system option modes. A record is created for each system option mode.

Table 39 ModePerLpr.csv file (Title: <<System Option Mode Per LPR>>)

Item	Content
System Option Mode#	System option mode # (0 to 2047, decimal number)
LPR#0, LPR#1, ..., LPR#31	System option mode for LPR#0 to LPR#31 • If the system option mode is on: On • If the system option mode is not on: Blank

MpPathStatus.csv

This CSV file contains information about the status of logical paths. A record is created for each MP blade or LR.

Table 40 MpPathStatus.csv file (Title: <<MP Path Status>>)

Item	Content
MPU#/CTL#	MP unit number or CTL number (2-digit hexadecimal number) • For MP unit number MPU#00 to MPU#03 • For CTL number CTL#00 to CTL#01
CMG#00-00 to 01 CMG#01-00 to 01	Path status[1] for the MP unit number with the cache module (CMG#*XX*-*YY*) *XX*: I path, *YY*: CMG# For VSP G200, CMG#00-00 to 01 only
MPU#00-00 to 03 MPU#01-00 to 03	Path status[1] and the MP unit for the MP unit number (MPU#*XX*-*YY*) *XX*: I path, *YY*: MPU#

Item	Content
	For VSP G200, MPU#00-00 to 03 only
CMG#00-00 to 01 CMG#01-00 to 01	Path status[1] with the cache module for the CTL number (CMG#*XX*-*YY*) *XX*: I path, *YY*: CMG# For VSP G200, CMG#00-00 to 01 only
MPU#00-00 to 03 MPU#01-00 to 03	Path status[1] with the MP unit number for the CTL number (MPU#*XX*-*YY*) *XX*: I path, *YY*: MPU# For VSP G200, MPU#00-00 to 03 only

Note:

1. 1=Normal, 0=Abnormal

MpPcbStatus.csv

This CSV file contains information about the status of MP Unit. A record is created for each MP unit.

Table 41 MpPcbStatus.csv file (Title: <<MP PCB Status>>)

Item	Content
MPU ID	MP unit ID (MPU-10, MPU-11, MPU-20, MPU-21)
Auto Assignment	Information about whether this MP unit is set to be automatically assigned to each resource. • Enabled: Set to be automatically assigned • Disabled: Not set to be automatically assigned
PCB Status	MP unit status[1]
MP#00, #01,..., #07	MP status[1] The number of output items differs for each model, because the number of installed MPs is different. • VSP G200: MP#00,01 • VSP G400, G600 or VSP F400, F600: MP#00, 01,..., 03 • VSP G800 or VSP F800: MP#00, 01,..., 07

Note:

1. 1=Normal, 0=Abnormal

PcbRevInfo.csv

This CSV file contains information about revisions of packages such as channel boards (CHBs) and others. A record is created for each package.

Table 42 PcbRevInfo.csv file (Title: <<PCB Revision Information>>)

Item	Content
Cluster#	Cluster number • 1 • 2

Item	Content
Location	Name of the part
FRU number	Product name of the package or some other name
PK Revision	Revision of the package
Factory	Factory manufacturing the package
Number	Serial number of the package
MAC Address	MAC address of the package

PdevCapaInfo.csv

This CSV file contains information about physical device (PDEV) capacities. A record is created for each of the classifications shown in "PDEV Kind".

Table 43 PdevCapaInfo.csv file (Title: <<PDEV Capacity Information>>)

Item	Content
PDEV Kind	The following four classifications are output: • OPEN System (TB) • Total Capacity (TB) • Number of PDEVs
SAS Drive	SAS drive capacity (TB)
Spare Drive	Spare drive capacity (TB)
SSD Drive	SSD capacity (TB)
Free Drive	Free drive capacity (TB)

PdevInfo.csv

This CSV file contains information about physical devices (PDEVs). A record is created for each PDEV.

Table 44 PdevInfo.csv file (Title: <<PDEV>>)

Item	Content
ECC Group	Number of parity group of which this PDEV is a component. • Spare Drive: For spare drives • Free Drive: For free drives
Emulation Type	Emulation type for the parity group indicated by "ECC Group" • Blank: "ECC Group" is Spare Drive. • Free Drive: "ECC Group" is Free Drive.
CR#	C# and R# (2-digit hexadecimal numbers), which identify the PDEV Output in the format *XX*/*YY*, where: • *XX*: C# • *YY*: R#
PDEV Location	PDEV location name
Device Type	Drive type

Item	Content
	• SAS • SSD
RPM	Revolutions per minute Blank displays as RPM when the drive is SSD.
Device Type-Code	Device type code of this drive Output example: DKR5D-J600SS
Device Size	Drive size (inches) • 2.5 • 3.5 • Blank when DBF (FMC or FMD)
Device Capacity	Drive capacity (GB or TB)
Drive Version	Drive firmware version (4-digit hexadecimal number)
DKB1	Name of the DKB1 controlling the PDEV
DKB2	Name of the DKB2 controlling the PDEV
Serial Number #	Serial number of this drive (*yymm xxxxxx*), where: • *yy* Year (last 2 digits) • *mm* Month (2 digits) • *xxxxxx*: Serial number of this drive
RAID Level	RAID level of the parity group indicated by "ECC Group" Blank if the "ECC Group" is Spare Drive or Free Drive
RAID Concatenation #0	Number of parity group to be concatenated to parity group (#0) identified by "ECC Group"[1]
RAID Concatenation #1	Number of parity group to be concatenated to parity group (#1) identified by "ECC Group"[1]
RAID Concatenation #2	Number of parity group to be concatenated to parity group (#2) identified by "ECC Group"[1]
Resource Group ID (ECC Group)	Resource group ID of parity group (0 to 1023, decimal number)
Resource Group Name (ECC Group)	Resource group name of parity group
Encryption	Encryption status of the parity group to which the PDEV belongs • Enabled: Encryption enabled • Disabled: Encryption disabled

Notes:

1. Blank if the parity group is not concatenated to another parity group or is Spare Drive.

PdevStatus.csv

This CSV file contains information about the status of physical devices (PDEVs). A record is created for each PDEV.

Table 45 PdevStatus.csv file (Title: <<PDEV Status>>)

Item	Content
CR#	C# and R# (2-digit hexadecimal numbers), which identify the PDEV Output in the format *XX*/*YY*, where: • *XX*: C# • *YY*: R#
Pdev Status	PDEV status[1]
Port0 Status	Status of Port 0 on this PDEV[1]
Port1 Status	Status of Port 1 on this PDEV[1]
Pdev Location	Location name of this PDEV
Notes: **1.** 1=Normal, 0=Abnormal	

PECBInfo.csv

This CSV file contains information about the PECB (PCIe channel board) and connecting destination for VSP G800 or VSP F800.

For all other VSP Gx00 models or VSP Fx00 models, hyphens are displayed for all contents.

Table 46 PECBInfo.csv file (Title: <<PECB Information>>)

Item	Content
Location	PECB location name
Status	Whether the PECB is installed • Installed • Not Installed
Type	Destination module type of the PECB • CHBB
Expansion mode	Expansion mode set in the destination module of the PECB • 1:2 • 1:4

PkInfo.csv

This CSV file contains information about channel boards (CHBs). A record is created for each CHB.

Table 47 PkInfo.csv file (Title: <<PK>>)

Item	Content
CHB Location	CHB name
Port#	Number of the port installed on the CHB (2-digit hexadecimal number)

Item	Content
Port	Name of port installed on the CHB
Package Type	CHB type indicated on the CHB Location • Fibre: 8FC4 (CHB), 16FC2 (CHB) • iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB)
SFP Kind	SFP (Small Form factor Pluggable) Kind • Short Wave • Long Wave • Blank if "Package Type" is 10iSCSI2c (CHB).
SFP Status	SFP Status: • Normal • Failed • Not Fix • Blank if "Package Type" is 10iSCSI2c (CHB).
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch: • On • Off • Blank if "Package Type" is iSCSI.
Connection	One of the Fibre topology settings • Point to Point • FC-AL • Blank if "Package Type" is iSCSI.
Port Address	Port address (00 to ff, 2-digit hexadecimal number) Blank if "Package Type" is iSCSI.
Resource Group ID (Port)	Resource group ID of port (0 to 1023, decimal number)
Resource Group Name (Port)	Resource group name of the port.
Port Internal WWN	Port WWN Blank if "Package Type" is iSCSI.
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port. • Enabled • Disabled • Blank if "Package Type" is not 16FC2 (CHB)

PpInfo.csv

This CSV file contains information about the software. A record is created for each software product.

For details about the license key, see License keys on page 101.

Table 48 PpInfo.csv file (Title: <<PP Information>>)

Item	Content
Program Product Name	Software name.
Install	Information about whether the installed license key is enabled or not • Enabled: Installed and the software can be used • Disabled: Installed but the software cannot be used

Item	Content
Key Type	Installed license key type - Permanent - Temporary - Emergency - Term If no license key is installed, "Not Installed" is output.
Permitted Volumes(TB)	Permitted volume capacity for this software (in TB) If no upper limit value is set for the capacity, "Unlimited" is output.
Expiration Date	Expiration date of the software. The format is *mm/dd/yyyy* (Month/Day/Year).
Status	License key status of the software - Installed - Not Enough License - Grace Period - Expired - Not Installed - Installed (Disabled)

SMfundat.csv

This CSV file contains information about SM functions. A record is created for each of the classifications shown in "SM Install Function".

Table 49 SMfundat.csv file (Title: <<SM Install function>>)

Item	Content
SM Install function	The following classifications are output for VSP G200: **1.** Base **2.** Extension 1 **3.** Extension 2 The following classifications are output for VSP G400, G600, G800 or VSP F400, F600, F800: **1.** Base **2.** Extension1 **3.** Extension2 **4.** Extension3 **5.** Extension4
Availability	Information about whether the function of "SM Install function" is enabled - Enabled - Disabled

SsdDriveInfo.csv

This CSV file contains information about SSDs. A record is created for each SSD.

Table 50 SsdDriveInfo.csv file (Title: <<SSD Drive Status>>)

Item	Content
ECC Group	Number of the parity group of which this SSD is a component. • Spare Drive: The SSD is a spare drive. • Free Drive: The SSD is a free drive.
CR#	C# and R# (2-digit hexadecimal numbers), which identify the PDEV Output in the format *XX*/*YY*, where: • *XX*: C# • *YY*: R#
PDEV Location	Drive type code of the PDEV location name for this drive
Device Type-Code	Drive type code Output example: SLR5A-M800SS
Device Capacity	Drive capacity in GB or TB
SSD Device Type	SSD drive type • MLC • FMC • FMD
Used Endurance Indicator (%)	SSD life (0 to 100)
Used Endurance Indicator Threshold (%)	SSD life threshold (0 to 100)
Used Endurance Indicator Warning SIM (%)	Warning SIM threshold (0 to 100)
FMD Battery Life Indicator Warning SIM (%)	Threshold of battery life warning SIM (0 to 100) Blank if SSD is other than FMD
FMD Battery Life Indicator (%)	Used battery life (0 to 100) Blank if SSD is other than FMD

SsidInfo.csv

This CSV file contains information about SSIDs. A record is created for each SSID.

Table 51 SsidInfo.csv file (Title: <<Subsystem ID >>)

Item	Content
DEV# Start	First LDEV number for the SSID
DEV# End	Last LDEV number for the SSID
SSID	Subsystem ID (hexadecimal)

SysoptInfo.csv

This CSV file contains information about system options.

Table 52 Sysoptinfo.csv file (Title: <<System Option Information>>)

Item	Content
Spare Disk Recover	Speed of copying data to the spare drive. • Interleave mode • Full Speed mode
Dynamic Sparing	Information about whether to perform automatic copy to a spare drive if the occurrences of drive failures exceed the threshold. • On • Off
Correction Copy	Information about whether to perform correction copy to a spare drive if a drive is blocked. • On • Off
Disk Copy pace	Speed of copying the spare drive in the Interleave mode. • Faster • Medium • Slower
System Option On	System options that are set to ON. Output example: mode*XXXX* (0 to 2047, decimal number)
Link Failure Threshold	Threshold to notify the link failure (0 to 255, decimal)

WwnInfo.csv

This CSV file contains information about hosts. A record is created for each host.

For details about the host setting, see the *Provisioning Guide for Hitachi Virtual Storage Platform Gx00 and Fx00 Models*.

Table 53 WwnInfo.csv file (Title: <<World Wide Name Information>>)

Item	Content
Port	Port name.
Host Group	Host group name iSCSI target alias is output if the "Package Type" is iSCSI.
Host Mode	Host mode that is set for the host group (0 to 127, hexadecimal)
Host Mode Option	Host mode option that is set for the host group (decimal) Multiple options are separated by semicolons (;)
WWN	World Wide Name of the host bus adapter registered to the host group (hexadecimal number) Blank if the "Package Type" is iSCSI.
Nickname	Nickname of the host Blank if the "Package Type" is iSCSI.
Host Group#	Host group number (00 to ff, hexadecimal)

Item	Content
	iSCSI target ID will be output if the "Package Type" is iSCSI.
CHB Location	Name of port installed on the CHB
Package Type	CHB type indicated on the CHB Location • Fibre: 8FC4 (CHB), 16FC2 (CHB) • iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB)
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port. • Enabled • Disabled • Blank if "Package Type" is not 16FC2 (CHB)

Glossary

#

2DC

two-data-center. Refers to the local and remote sites, or data centers, in which TrueCopy (TC) and Universal Replicator (UR) combine to form a remote replication configuration.

In a 2DC configuration, data is copied from a TC primary volume at the local site to the UR master journal volume at an intermediate site, then replicated to the UR secondary volume at the remote site. Since this configuration side-steps the TC secondary volume at the intermediate site, the intermediate site is not considered a data center.

3DC

three-data-center. Refers to the local, intermediate, and remote sites, or data centers, in which TrueCopy and Universal Replicator combine to form a remote replication configuration.

In a 3DC configuration, data is copied from a local site to an intermediate site and then to a remote site (3DC cascade configuration), or from a local site to two separate remote sites (3DC multi-target configuration).

A

array

See disk array

audit log

Files that store a history of the operations performed from Device Manager - Storage Navigator and the commands that the storage system received from hosts, and data encryption operations.

B

back-end director (BED)

The hardware component that controls the transfer of data between the drives and cache. A BED feature consists of a pair of boards. A BED is also referred to as a disk board (DKB).

BED

See *back-end director*.

bind mode

In bind mode the Cache Residency Manager extents are used to hold read and write data for specific extent(s) on volume(s). Data written to the Cache Residency Manager bind area is not destaged to the drives. For bind mode, all targeted read and write data is transferred at host data transfer speed.

blade

A computer module, generally a single circuit board, used mostly in servers.

C

cache logical partition (CLPR)

Consists of virtual cache memory that is set up to be allocated to different hosts in contention for cache memory.

capacity

The amount of data storage space available on a physical storage device, usually measured in bytes (MB, GB, TB, etc.).

CCI

Command Control Interface

CHAP

challenge handshake authentication protocol

CLPR

See *cache logical partition (CLPR)*.

cluster

Multiple-storage servers working together to respond to multiple read and write requests.

command device

A dedicated logical volume used only by Command Control Interface and Business Continuity Manager to interface with the storage system. Can be shared by several hosts.

controller

The component in a storage system that manages all storage functions. It is analogous to a computer and contains a processors, I/O devices, RAM, power supplies, cooling fans, and other sub-components as needed to support the operation of the storage system.

copy pair

A pair of volumes in which one volume contains original data and the other volume contains the copy of the original. Copy operations can be synchronous or asynchronous, and the volumes of the copy pair can be located in the same storage system (local copy) or in different storage systems (remote copy).

A copy pair can also be called a volume pair, or just pair. A pair created by Compatible FlashCopy® is called a relationship.

copy-on-write (COW)

Point-in-time snapshot copy of any data volume within a storage system. Copy-on-write snapshots only store changed data blocks, therefore the amount of storage capacity required for each copy is substantially smaller than the source volume.

COW

See *copy-on-write (COW)*.

COW Snapshot

Copy-on-Write Snapshot

custom volume (CV)

A custom-size volume whose size is defined by the user using Virtual LVI/ Virtual LUN.

CV

See *custom volume*.

CVS

custom volume size

CXFS

clustered version of XFS file system

D

data drive

A physical data storage device that can be either a hard disk drive (HDD) or a flash drive (also called a solid-state device).

DBV

Hitachi Database Validator

DC

data center

delta resync

A disaster recovery solution in which TrueCopy and Universal Replicator systems are configured to provide a quick recovery using only differential data stored at an intermediate site.

device

A physical or logical unit with a specific function.

device emulation

Indicates the type of logical volume. Mainframe device emulation types provide logical volumes of fixed size, called logical volume images (LVIs), which contain EBCDIC data in CKD format. Typical mainframe device emulation types include 3390-9 and 3390-M. Open-systems device emulation types provide logical volumes of variable size, called logical units (LUs), that contain ASCII data in FBA format. The typical open-systems device emulation type is OPEN-V.

disaster recovery

A set of procedures to recover critical application data and processing after a disaster or other failure.

disk array

Disk array, or just array, is a complete storage system, including the control and logic devices, storage devices (HDD, SSD), connecting cables, and racks

disk controller (DKC)

The hardware component that manages front-end and back-end storage operations. The term DKC can refer to the entire storage system or to the controller components.

DKC

See *disk controller (DKC)*.

DKCMAIN

disk controller main. Refers to the software for the storage system.

DKU

disk unit. Refers to the cabinet (floor model) or rack-mounted hardware component that contains data drives and no controller components.

dump

A collection of data that is saved to a file when an error or crash occurs. The data is used by support personnel to determine the cause of the error or crash.

Dump tool

Downloads Device Manager - Storage Navigator configuration information onto recording media for backup and troubleshooting purposes.

E

emulation

The operation of the Hitachi Virtual Storage Platform storage system to emulate the characteristics of a different storage system. For device emulation, the mainframe host recognizes the logical devices on the storage system as 3390-x devices. For controller emulation, the mainframe host recognizes the control units (CUs) on the storage system as 2105 or 2107 controllers.

The Virtual Storage Platform storage system operates the same as the storage system being emulated.

emulation group

A set of device emulation types that can be intermixed within a RAID group and treated as a group.

external application

A software module that is used by a storage system but runs on a separate platform.

external volume

A logical volume whose data resides on drives that are physically located outside the Hitachi storage system.

F

FC

Fibre Channel; FlashCopy

FC-AL

fibre-channel arbitrated loop

FCP

fibre-channel protocol

FCSP

fibre-channel security protocol

FICON

Fibre Connectivity

flash drive

A data drive that uses a solid-state memory device instead of a rotating hard disk.

flash module

A high speed data storage device that includes a custom flash controller and several flash memory sub-modules on a single PCB.

FMD

See flash module

H

HBA

host bus adapter

HDD

hard disk drive

HDT

Hitachi Dynamic Tiering

HDU

hard disk unit

head LDEV

See *top LDEV*.

host group

A group of hosts of the same operating system platform.

host mode

Operational modes that provide enhanced compatibility with supported host platforms. Used with fibre-channel ports on RAID storage systems.

host mode option

Additional options for fibre-channel ports on RAID storage systems. Provide enhanced functionality for host software and middleware.

HP XP7 CVAE

HP XP7 Command View Advanced Edition - a set of software applications included in the system firmware. Via the GUI, they are used to configure, control, and monitor the storage system.

I

in-system replication

The original data volume and its copy are located in the same storage system. ShadowImage in-system replication provides duplication of logical volumes; Thin Image in-system replication provides "snapshots" of logical volumes that are stored and managed as virtual volumes (V-VOLs).

See also *remote replication*.

initiator

An attribute of the port that is connected to the port with RCU target attribute.

internal volume

A logical volume whose data resides on drives that are physically located within the storage system. See also *external volume*.

J

JNL

journal

journal volume

A volume that records and stores a log of all events that take place in another volume. In the event of a system crash, the journal volume logs are used to restore lost data and maintain data integrity.

In Universal Replicator, differential data is held in journal volumes on until it is copied to the S-VOL.

JRE

Java Runtime Environment

K

key management server

A server that manages encryption keys. On the Hitachi Virtual Storage Platform G400, G600, G800 storage system, users can back up and restore encryption keys on a key management server that complies with the Key Management Interoperability Protocol (KMIP).

keypair

Two mathematically-related cryptographic keys: a private key and its associated public key.

L

LBA

logical block address

LCP

local control port; link control processor

LD

local directory; logical device

LDAP

lightweight directory access protocol

LDEV

logical device

LDKC

See *logical disk controller (LDKC)*.

LDM

Logical Disk Manager

license key

A specific set of characters that unlocks an application and allows it to be used.

local control port (LCP)

A serial-channel (ESCON) port configured to receive I/Os from a host or remote I/Os from a TrueCopy main control unit (MCU).

local copy

See *in-system replication*.

local storage system

A storage system connected to the management client.

logical device (LDEV)

An individual logical data volume (on multiple drives in a RAID configuration) in the storage system. An LDEV may or may not contain any data and may or may not be defined to any hosts. Each LDEV has a unique identifier or "address" within the storage system composed of the logical disk controller (LDKC) number, control unit (CU) number, and LDEV number. The LDEV IDs within a storage system do not change.An LDEV formatted for use by mainframe hosts is called a logical volume image

(LVI). An LDEV formatted for use by open-system hosts is called a logical unit (LU).

logical disk controller (LDKC)

A group of 255 control unit (CU) images in the RAID storage system that is controlled by a virtual (logical) storage system within the single physical storage system. For example, the Hitachi Universal Storage Platform V storage system supports two LDKCs, LDKC 00 and LDKC 01.

logical partition (LPAR)

A subset of a system's hardware resources that is virtualized as a separate system. For a storage system, logical partitioning can be applied to cache memory and/or storage capacity.

logical unit (LU)

A logical volume that is configured for use by open-systems hosts (for example, OPEN-V).

logical unit (LU) path

The path between an open-systems host and a logical unit.

logical volume (LV)

See *volume*.

logical volume image (LVI)

A logical volume that is configured for use by mainframe hosts (for example, 3390-9).

LU

See *logical unit (LU)*.

LUN

See logical unit number

LUN volume

A custom-size volume whose size is defined by the user using Virtual LUN. Also called a custom volume (CV).

LV

logical volume

LVI

See *logical volume image*.

M

MF, M/F

mainframe

modify mode

The mode of operation of Device Manager - Storage Navigator that allows changes to the storage system configuration. See also *view mode*.

O

OPEN-V

A logical unit (LU) of user-defined size that is formatted for use by open-systems hosts.

OPEN-x

A logical unit (LU) of fixed size (for example, OPEN-3 or OPEN-9) that is used primarily for sharing data between mainframe and open-systems hosts using Hitachi Cross-OS File Exchange.

P

P-VOL

This term is used only in the earlier version of the Device Manager - Storage Navigator GUI (still in use) for the primary volume. See *primary volume*.

pair

Two logical volumes in a replication relationship in which one volume contains original data to be copied and the other volume contains the copy of the original data. The copy operations can be synchronous or asynchronous, and the pair volumes can be located in the same storage system (in-system replication) or in different storage systems (remote replication).

parity group

See *RAID group*.

PAV

Hitachi Compatible PAV

PCB

printed circuit board

PDEV

physical device

PG

parity group. See *RAID group*.

physical device

See *device*.

pool

A set of volumes that are reserved for storing pool volumes (pool-VOL), and used by Thin Image, Dynamic Provisioning, Dynamic Tiering, or active flash data.

pool volume (pool-VOL)

A logical volume that is reserved for storing snapshot data for Thin Image operations or write data for Dynamic Provisioning, Dynamic Tiering, or active flash.

port attribute

Indicates the type of fibre-channel port: target, RCU target, or initiator.

primary volume (P-VOL)

The volume in a copy pair that contains the original data to be replicated. The data on the P-VOL is duplicated synchronously or asynchronously on the secondary volume (S-VOL).

The following Hitachi products use the term P-VOL: Thin Image, Copy-on-Write Snapshot, ShadowImage, TrueCopy, Universal Replicator, Universal Replicator for Mainframe, and High Availability Manager.

See also *secondary volume*.

prio

priority mode. Used in Cache Residency Manager.

Q

quick format

The quick format feature in Virtual LVI/Virtual LUN in which the formatting of the internal volumes is done in the background. This allows system configuration (such as defining a path or creating a TrueCopy pair) before the formatting is completed. To execute quick formatting, the volumes must be in blocked status.

quick restore

A reverse resynchronization in which no data is actually copied: the primary and secondary volumes are swapped.

R

RAID

redundant array of inexpensive disks

RAID group

A set of RAID disks that have the same capacity and are treated as one group for data storage and recovery. A RAID group contains both user data and parity information. This allows user data to be accessed in the event that one or more of the drives within the RAID group are not available. The RAID level of a RAID group determines the number of data drives and parity drives and how the data is "striped" across the drives. For RAID1, user data is duplicated within the RAID group, so there is no parity data for RAID1 RAID groups.

A RAID group can also be called an array group or a parity group.

RAID level

The type of RAID implementation. RAID levels include RAID0, RAID1, RAID2, RAID3, RAID4, RAID5 and RAID6.

RCU

See *remote control unit*.

RCU target port

A fibre-channel port that is configured to receive remote I/Os from an initiator port on another storage system.

remote control unit (RCU)

A storage system at a secondary or remote site that is configured to receive remote I/Os from one or more storage systems at the primary or main site.

remote copy

See *remote replication*.

resync

resynchronize.

RMI

Remote Method Invocation

S

S-VOL

See *secondary volume* or *source volume*. When used for "secondary volume", "S-VOL" is only seen in the earlier version of the Device Manager - Storage Navigator GUI (still in use).

SAS

serial-attached SCSI

secondary volume (S-VOL)

The volume in a copy pair that is the copy of the original data on the primary volume (P-VOL). The following Hitachi products use the term "secondary volume": Thin Image, Copy-on-Write Snapshot, ShadowImage, TrueCopy, Universal Replicator, Universal Replicator for Mainframe, and High Availability Manager.

See also *primary volume*.

service information message (SIM)

Messages generated by a RAID storage system when it detects an error or service requirement. SIMs are reported to hosts and displayed on Device Manager - Storage Navigator.

service processor

The computer in aHitachi Virtual Storage Platform G1000 storage system that hosts the Device Manager - Storage Navigator software and is used to configure and maintain the storage system.

severity level

Applies to service information messages (SIMs) and Device Manager - Storage Navigator error codes.

SFP

small form-factor pluggable

shared memory

Memory that exists logically in the cache. It stores common information about the storage system and the cache management information (directory). The storage system uses this information to control exclusions and differential table information. Shared memory is managed in two segments and is used when copy pairs are created.

In the event of a power failure, the shared memory is kept alive by the cache memory batteries while the data is copied to the cache flash memory (SSDs).

shredding

See *volume shredding*.

SIM

See *service information message*.

size

Generally refers to the storage capacity of a memory module or cache. Not usually used for storage of data on disk or flash drives.

SM

shared memory

SMTP

simple mail transfer protocol

snapshot

A point-in-time virtual copy of a Hitachi Thin Image primary volume (P-VOL). The snapshot is maintained when the P-VOL is updated by storing pre-updated data (snapshot data) in a data pool.

SNMP

See *Simple Network Management Protocol*.

SOM

See *system option mode*.

source volume (S-VOL)

Used only in the earlier version of the Device Manager - Storage Navigator GUI (still in use). This is the volume in a mainframe copy pair containing the original data that is duplicated on the target volume (T-VOL). The following Hitachi products use the term source volume: ShadowImage for Mainframe, Dataset Replication, and Compatible FlashCopy®.

In the current version of the GUI, "target volume" and "T-VOL" are replaced with "primary volume".

See also *source volume*.

space

Generally refers to the data storage capacity of a disk drive or flash drive.

SRM

Storage Replication Manager

SSD

solid-state drive. Also called flash drive.

SSID

See *storage subsystem identifier*.

SSL

secure socket layer

storage cluster

See *cluster*.

storage tiers

See *tiered storage*.

SVP

See *service processor*.

SVS

Storage Virtualization System

SW, sw

short wavelength, software

syslog

The file on the SVP that includes both syslog and audit log information, such as the date and time.

system disk

The volume from which an open-systems host boots.

system option mode (SOM)

Additional operational parameters for the RAID storage systems that enable the storage system to be tailored to unique customer operating requirements. SOMs are set on the service processor.

T

T-VOL

See *target volume*.

target

An attribute of the port that is connected to the host.

target port

A fibre-channel port that is configured to receive and process host I/Os.

target volume (T-VOL)

The volume in a mainframe copy pair that is the copy of the original data on the source volume (S-VOL). The term is used only in the earlier version of the Device Manager - Storage Navigator GUI (still in use), for the following Hitachi products: ShadowImage for Mainframe, Dataset Replication, and Compatible FlashCopy® V2.

See also *source volume*.

TC

Hitachi TrueCopy

TI

See Thin Image.

tiered storage

A layered structure of performance levels, or tiers, that matches data access requirements with the appropriate performance tiers. The tiers are:

Tier 1: Static content. Tier 1 is fully supported computing expected to be production quality.

Tier 2: Application logic. Tier 2 platforms are not supported by the security officer and release engineering teams. Tier 2 systems are targeted for Tier 1 support, but are still under development.

Tier 3: Database. Tier 3 platforms are architectures for which hardware is not or will not be available or that are considered legacy systems unlikely to see broad future use.

Tier 4 systems are not supported.

total capacity

The aggregate amount of storage space in a data storage system.

TPF

Transaction Processing Facility

V

V-VOL

virtual volume

VDEV

See *virtual device*.

view mode

The mode of operation of Device Manager - Storage Navigator that allows viewing only of the storage system configuration. The two Device Manager - Storage Navigator modes are view mode and modify mode.

virtual device (VDEV)

A group of logical devices (LDEVs) in a RAID group. A VDEV typically consists of some fixed volumes (FVs) and some free space. The number of fixed volumes is determined by the RAID level and device emulation type.

virtual volume (V-VOL)

A logical volume in a storage system. A V-VOL has no physical storage space.

Thin Image uses V-VOLs as secondary volumes of copy pairs.

In Dynamic Provisioning, Dynamic Tiering, and active flash, V-VOLs are called DP-VOLs.

VLUN

Hitachi Virtual LUN

VM

volume migration; volume manager

volume (VOL or vol)

A logical device (LDEV), or a set of concatenated LDEVs in the case of LUSE, that has been defined to one or more hosts as a single data storage unit. An open-systems volume is called a logical unit (LU), and a mainframe volume is called a logical volume image (LVI).

volume shredding

Deleting the user data on a volume by overwriting all data in the volume with dummy data.

Index

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-94HM8016-02

November 2015