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-94HM8016-06
October 2016

© 2014, 2016 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Data Systems Corporation (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials 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 products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi 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 authorized 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.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Contents

Preface 11

Intended audience 12
Product version 12
Release notes 12
Changes in this revision 12
Related documents 12
Document conventions 13
Conventions for storage capacity values 14
Accessing product documentation 15
Getting help 15
Comments 16

1 System administration overview 17

System management architecture 18
Ways to administer the storage system 18
Overview of Storage Advisor 19
Unified management of block storage and file storage 20
Dashboard 21
Inventory and resource information 25
Device Manager - Storage Navigator 26
Maintenance utility 27
NAS Manager 28

2 Preparing your management software 31

Installing Storage Advisor 32
Installing Storage Advisor with the application installer 32
Installing Storage Advisor with the virtual appliance 33
Installing Hitachi Storage Advisor in a DHCP environment 33
Installing Hitachi Storage Advisor in a static environment 35
Changing the root password immediately after installation 38
Logging in to Storage Advisor 38
Logging in when Storage Advisor is not available 39

Generating and installing a signed SSL certificate....40
Using Device Manager - Storage Navigator....41
Setting up a management client....41
Requirements for management clients....41
Setting up TCP/IP for a firewall....44
Configuring the web browser....44
Installing Adobe Flash Player....46
Logging in to Device Manager - Storage Navigator....46
Initial super-user login....47
Normal login....47
Changing your password....49
Adding your SVP to the trusted sites zone for Windows Server computers....49
Onboarding and configuring a storage system....50
Overview....51
Adding the first storage system....51
Adding a fabric switch....52
Adding servers....53
Creating parity groups....54
Using the maintenance utility....56
Starting from Hitachi Command Suite....57
Starting from Hitachi Device Manager - Storage Navigator....57
Accessing a storage system without management software....58

3 System configuration....61

System administration tasks at a glance....62
System administration using Hitachi Storage Advisor....63
Configure block storage....63
Enabling or disabling port security....64
Adding a fabric switch....64
Creating parity groups....67
Creating a pool....76
Create and attach volumes to servers....83
Managing storage systems....86
Managing servers....93
Managing volumes....96
Configure file storage....102
Managing file pools....102
Managing virtual file servers....106
Managing file systems....107
Managing shares and exports....109
System administration using Device Manager - Storage Navigator....113
Setting storage system information....113
Backing up HDvM - SN configuration files....114
Restoring HDvM - SN configuration files....115
System administration using the maintenance utility....116
Changing the date and time....116
Changing the controller clock settings....116
Changing the SVP clock settings....116
Changing network settings....117
Setting up TCP/IP for a firewall....117
Enabling IPv6 communication....117

Changing the administrator password....118
Creating a login message....119
Forcing the system lock to release....119
Registering the primary SVP host name....120
System administration using NAS Manager....121
Changing the system date and time of the NAS modules....121
Miscellaneous system administration considerations....122
Report configuration tool....122
Prerequisites for the report configuration tool....123
Installing the report configuration tool....123
Using the report configuration tool....123
Modifying SVP port numbers....124
Viewing the port number used in SVP....125
Effects of changing SVP port numbers....125
Changing the SVP port number....127
Initializing the SVP port number....128
Reassigning an automatically assigned port number....128
Initializing and reassigning an automatically assigned port number....129
Changing the range of an automatically assigned port number....130
Initializing the range of an automatically assigned port number....131
Releasing HTTP communication blocking....132
Blocking HTTP communication to the SVP....132

4 User Administration....133

User administration for maintenance utility....134
Required roles for operating Maintenance Utility....134
Setting up user accounts....135
Disabling user accounts....137
Removing user accounts....141
Backing up user accounts....143
Restoring user account information....144
User administration for Device Manager - Storage Navigator....146
User administration overview....146
Workflow for creating and managing user accounts....146
Administrator tasks....147
User tasks....147
Managing user accounts....147
Creating user accounts....148
Character restrictions for user names and passwords....149
Changing user passwords....151
Changing user permissions....152
Enabling or Disabling user accounts....153
Deleting user accounts....154
Releasing a user lockout....154
Managing user groups....155
Roles....155
Built-in groups, roles, and resource groups....156
Verifying the roles available to a user group....158
Checking if a role is available to a user group....158
Creating a new user group....159
Changing a user group name....160

Changing user group permissions..... 160
Changing assigned resource groups..... 161
Deleting a user group..... 161
Using an authentication server and authorization server..... 162
Authentication server protocols..... 163
Authorization server requirements..... 164
Connecting two authentication servers..... 164
Connecting authentication and authorization servers..... 165
Naming a user group in Device Manager - Storage Navigator..... 165
Creating configuration files..... 166
Creating an LDAP configuration file..... 166
Creating a RADIUS configuration file..... 169
Creating a Kerberos configuration file..... 172
User Administration for NAS Manager..... 176
Administrator types and responsibilities..... 176
Adding an SMU user (an administrator)..... 177
Changing the password for a currently logged in user..... 180
Changing your own password..... 181
Changing another user's password..... 182
Changing an SMU user profile..... 184
SMU user authentication..... 187
Active Directory user authentication..... 188
Using Transport Layer Security (TLS) with Active Directory authentication..... 188
Configuring Active Directory servers..... 189
Configuring Active Directory groups..... 192
User authentication through RADIUS servers (HNAS server only)..... 196
Displaying list of RADIUS servers..... 197
Adding a RADIUS server..... 198
Displaying details of RADIUS server..... 200

5 Setting up security..... 203

Working with certificates..... 204
Managing HCS certificates..... 204
Registering HCS certificates..... 204
Deleting HCS certificates..... 204
Managing SSL certificates..... 205
Flow of SSL communication settings..... 205
Creating a keypair..... 206
Obtaining a signed certificate..... 208
Verifying and releasing an SSL certificate passphrase..... 209
Converting SSL certificates to PKCS#12 format..... 210
Updating a signed certificate..... 210
Notes on updating a signed certificate for the service processor..... 211
Returning the certificate to default..... 211
Selecting a cipher suite..... 212
Problems with website security certificates..... 213
Updating the certificate files..... 213
Configuring SMU security (NAS module only)..... 215

6 Alert notifications..... 217
Viewing alert notifications..... 218
Configuring alert notifications..... 218
General settings..... 219
Email settings..... 220
Syslog settings..... 220
SNMP settings..... 222
Sending test messages..... 222
Sending a test email message..... 223
Example of a test email message..... 223
Sending a test Syslog message..... 223
Sending a test SNMP trap..... 224
Using the Windows event log..... 224
Monitoring failure information in the Windows event log..... 224
Viewing the Windows event log..... 225
Output example of the failure information..... 225

7 License keys..... 229
Overview..... 230
License key types..... 230
Using the permanent key..... 230
Using the term key..... 231
Using the temporary key..... 231
Using the emergency key..... 231
Cautions on license capacities in license-related windows..... 232
Managing licenses..... 232
Installing block and file licenses using NAS Manager..... 233
Adding a license key..... 233
Installing block licenses using maintenance utility..... 235
Enabling a license..... 235
Disabling a license..... 235
Removing a software license..... 236
Removing a Data Retention Utility license..... 236
Examples of license information..... 237
License key expiration..... 238

8 Configuring audit logs..... 239
Audit log settings..... 240
Setting up a syslog server..... 240
Exporting an audit log..... 241
Send test message to syslog server..... 242

9 Managing storage system reports..... 243
About storage system reports..... 244
Viewing a Device Manager - Storage Navigator report..... 244
Viewing a report in the Reports window..... 245
Creating a configuration report..... 245
Deleting a configuration report..... 245
Collecting dump files using the Dump tool 246

A Raidinf command reference (obtaining configuration reports and tier relocation logs)..... 249
raidinf command list and command description.....250
raidinf -login..... 251
raidinf add report..... 252
raidinf delete report.....253
raidinf download report.....254
raidinf get reportinfo.....255
raidinf add relocationlog.....256
raidinf download relocationlog.....257
raidinf delete relocationlog.....258
raidinf get relocationloginfo.....258
raidinf -logout..... 259
raidinf -h..... 260

B Storage configuration reports..... 261
Reports in table view..... 262
CHAP Users report..... 262
Disk Boards report..... 263
Host Groups / iSCSI Targets report.....264
Hosts report..... 265
Logical Devices report..... 266
LUNs report.....268
MP Units report.....268
MP Unit Details report..... 269
Parity Groups report.....270
Physical Devices report.....271
Ports report.....273
Power Consumption report..... 275
Spare Drives report.....276
SSD Endurance report.....277
Storage System Summary report.....278
Reports in graphical view..... 282
Cache Memories report..... 283
Channel Boards report.....285
Physical View report.....289
CSV files..... 295
AllConf.csv.....295
CacheInfo.csv.....296
ChapUserInfo.csv.....296
ChaStatus.csv.....297
DeviceEquipInfo.csv.....297
DkaInfo.csv..... 298
DkaStatus.csv.....298
DkcInfo.csv..... 298
DkuTempAveInfo.csv.....299
DkuTempInfo.csv..... 300
DkuTempMaxInfo.csv..... 302
DkuTempMinInfo.csv.....303
ELunInfo.csv.....304

EnvMonInfo.csv..... 306
FcSpNameInfo.csv..... 307
FcSpPortInfo.csv..... 307
HduInfo.csv..... 308
IscsiHostInfo.csv..... 308
IscsiPortInfo.csv..... 309
IscsiTargetInfo.csv..... 310
JnlInfo.csv..... 311
LdevCapaInfo.csv..... 311
LdevCountInfo.csv..... 312
LdevInfo.csv..... 312
LdevStatus.csv..... 315
LPartition.csv..... 315
LunInfo.csv..... 316
LunPortInfo.csv..... 317
MicroVersion.csv..... 318
MlcEnduranceInfo.csv..... 319
ModePerLpr.csv..... 320
MpPathStatus.csv..... 320
MpPcbStatus.csv..... 321
PcbRevInfo.csv..... 321
PdevCapaInfo.csv..... 322
PdevInfo.csv..... 322
PdevStatus.csv..... 324
PECBInfo.csv..... 324
PkInfo.csv..... 324
PpInfo.csv..... 326
SMfundat.csv..... 326
SsdDriveInfo.csv..... 327
SsidInfo.csv..... 327
SysoptInfo.csv..... 328
WwnInfo.csv..... 328

Glossary..... 331

Index..... 351

Preface

This document provides information and instructions to help you use the maintenance utility and some of the functions in Device 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
- ☐ Product version
- ☐ Release notes
- ☐ Changes in this revision
- ☐ Related documents
- ☐ Document conventions
- ☐ Conventions for storage capacity values
- ☐ Accessing product documentation
- ☐ Getting help
- ☐ Comments

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 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:

- VSP Gx00 models and VSP Fx00 models: firmware 83-04-0*x* or later
- SVOS 7.0 or later

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. Release notes are available on Hitachi Data Systems Support Connect: https://knowledge.hds.com/Documents.

Changes in this revision

- Removed references to unsupported DBF2 drives.
- Updated available tasks in Administration tasks and tools table.

Related documents

The documents below are referenced in this document or contain more information about the features described in this document.

- *Product Overview*, MK-92HM8051
- *Hitachi Command Suite User Guide*, MK-90HC172
- *Hitachi Command Suite Installation and Configuration Guide*, MK-90HC173

- *Hitachi Audit Log User Guide*, MK-94HM8028
- *Encryption License Key User Guide*, MK-92RD8009
- *Performance Guide*, MK-94HM8012
- *Hitachi ShadowImage® User Guide*, MK-94HM8021
- *Hitachi SNMP Agent User Guide*, MK-94HM8015
- *Hitachi Device Manager - Storage Navigator Messages*, MK-94HM8017
- *Hitachi TrueCopy® User Guide*, MK-94HM8019
- *Hitachi Universal Replicator User Guide*, MK-94HM8023
- *Global-Active Device User Guide*, MK-92RD8072
- *Hitachi Virtual Storage Platform G200 Hardware Reference Guide*, MK-94HM8020
- *Hitachi Virtual Storage Platform G400, G600 Hardware Reference Guide*, MK-94HM8022
- *Hitachi Virtual Storage Platform G800 Hardware Reference Guide*, MK-94HM8026
- *Hitachi Virtual Storage Platform F400, F600 Hardware Reference Guide*, MK-94HM8045
- *Hitachi Virtual Storage Platform F800 Hardware Reference Guide*, MK-94HM8046

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.

Convention	Description
	• 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 and/or consequences (for example, disruptive operations, data loss, or a system crash).
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

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 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
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://knowledge.hds.com/Documents. 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 system administration tasks for the Hitachi Virtual Storage Platform G200, G400, G600, G800 or Hitachi Virtual Storage Platform F400, F600, F800 storage systems. It describes:

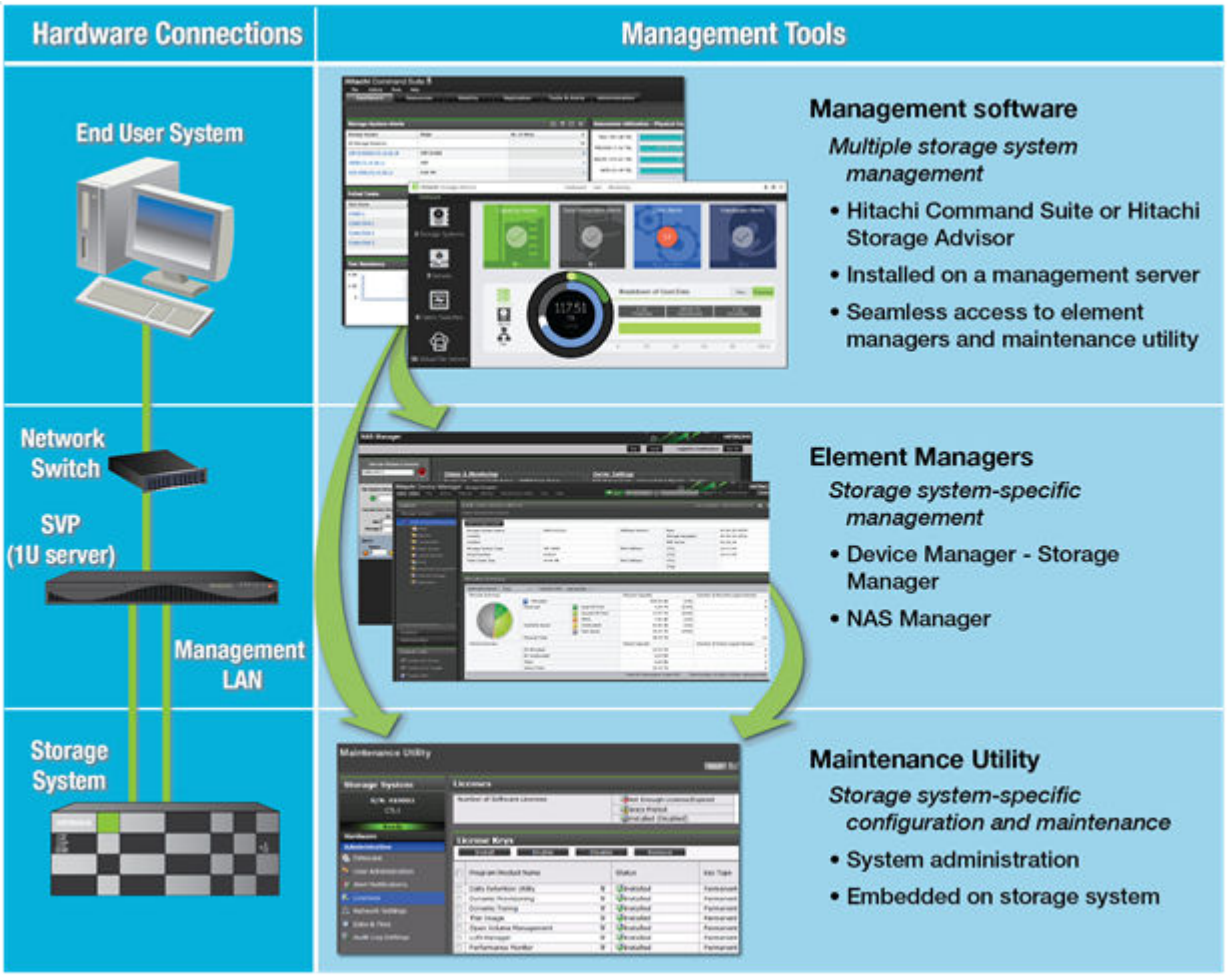
- Software architecture and access to system administration tools from management software (Hitachi Storage Advisor and Hitachi Command Suite).
- System administration tasks for the VSP Gx00 models and VSP Fx00 models storage systems, including some with NAS modules installed to provide native file functionality (VSP G400, G600, G800).

☐ System management architecture

☐ Ways to administer the storage system

System management architecture

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



Related tasks

- Accessing a storage system without management software on page 58

Ways to administer the storage system

The system administration tasks described in this guide apply to all VSP Gx00 models and Hitachi Virtual Storage Platform F400, F600, F800 storage systems, including those with NAS modules.

Users with storage systems that do not have NAS modules use Hitachi Storage Advisor (HSA), Device Manager - Storage Navigator, and the maintenance utility to administer block operations. If your storage system

includes NAS modules, use NAS Manager to administer file operations, and then use the maintenance utility to verify that the settings are synchronized with block operations.

For more information about administration tasks for file operations, see the following documentation:

- *Storage Subsystem Administration Guide* (MK-92HNAS012)
- *Storage System User Administration Guide* (MK-92HNAS013)
- *File Services Administration Guide Hitachi Unified NAS Module and Hitachi NAS Platform File Services Administration Guide* (MK-92HNAS006)
- *Server and Cluster Administration Guide* (MK-92HNAS010)
- *System Access Guide* (MK-92HNAS014)

For more information about HSA, see the following documentation:

- *Hitachi Storage Advisor Getting Started Guide* (MK-94HSA001)
- *Hitachi Storage Advisor RESTful API Reference Guide* (MK-94HSA003)
- *Hitachi Storage Advisor User Guide* (MK-94HSA004)

You can also perform some administration tasks from a command line. For information, see Command Control Interface User and Reference Guide (MK-90RD7010) and the Command Control Interface Command Reference (MK-90RD7009), which you can access from the Documentation page of NAS Manager.

Overview of Storage Advisor

Hitachi Storage Advisor is a unified software management tool that reduces the complexity of managing storage systems by simplifying the setup, management, and maintenance of storage resources.

Storage Advisor reduces infrastructure management complexities and enables a new simplified approach to managing storage infrastructures. It provides intuitive graphical user interfaces and recommended configuration practices to streamline system configurations and storage management operations. You can leverage Storage Advisor to easily provision new storage capacity for business applications without requiring in-depth knowledge of the underlying infrastructure resource details. It provides centralized management while reducing the number of steps to configure, optimize, and deploy new infrastructure resources.

Some of the key Storage Advisor capabilities include:

- Simplified user experience for managing infrastructure resources. Visual aids enable easy viewing and interpretation of key management information, such as used and available capacity, and guide features to help quickly determine appropriate next steps for a given management task.
- Recommended system configurations to speed initial storage system setup and accelerate new infrastructure resource deployments.

- Integrated configuration workflows with Hitachi recommended practices to streamline storage provisioning and data protection tasks.
- Common, centralized management for supported storage systems.
- A REST-based API to provide full management programmability and control in addition to unified file-based management support.
- Storage Advisor enables automated SAN zoning during volume attach and detach. Optional auto-zoning eliminates the need for repetitive zoning tasks to be performed on the switch.

Unified management of block storage and file storage

Storage Advisor can be used to onboard and configure both block storage and file storage if NAS modules are included in the chassis of a supported storage system.

Understand block and file storage

- Block storage:
  In block storage, volumes of storage are created. A server-based operating system can connect to each block of storage and control it as an individual hard drive. Each storage block can be individually formatted with the required file system, such as NTFS or VMFS. Block storage systems are typically deployed in a Storage Area Network (SAN) environment.
  From the dashboard of Storage Advisor, you can discover, register, and onboard a block storage system.
- File storage:
  Storage Advisor supports unified onboarding and configuration of file storage in the form of NAS modules.
  If a supported storage system includes NAS modules, the file storage is automatically added with the block storage. Then file pools and other file resources can be created in the Storage Advisor interface or by using the API.

Adding block and file storage together

Storage Advisor enables you to add block and file storage in a single step. The only requirements are the SVP IP address, user name, and password. When the file storage is added, the cluster is automatically registered in Storage Advisor.

Unified configuration

Once a storage system is onboarded, all block and file resources can be configured and managed from a single Storage System page. File pool creation workflow incorporates best practices that simplify workflow and enhance usability. The file pools are used to easily create virtual file servers, file systems, and shares and exports. File system creation automatically mounts and formats the new file system.

Unified reporting

Capacity is reported for all aggregated storage systems in the dashboard.

Capacity is also displayed for each storage system in the Storage System detail page.

Three views of capacity are available: file only, block only, or a unified view of block and file.

Dashboard

Once a storage system has been onboarded to Storage Advisor, the dashboard displays as soon as you log in. The Storage Advisor dashboard provides the tools to easily configure, manage, and monitor storage systems.



From the Storage Advisor dashboard, you can access managed resources and provision storage in the context of a given storage system or server. The provided templates and configurations make it possible to quickly and easily provision a storage system, without knowing the details of the underlying hardware and software.

The top navigation menu provides access to Jobs and Monitoring pages. Links to the following settings are available, based on the user role:

- Tier Management
- Security Settings
- SNMP Settings
- Change Local Password

The dashboard has three distinct sections:

- **Resource side panel:** The left pane provides quick access to review the configuration of your storage systems, servers, and fabric switches. If the storage system includes NAS modules, virtual file servers can also be accessed.
- **Alert tiles:** Four alert tiles represent various aspects of the health of the storage system. When Storage Advisor detects a problem with a storage system environment, a number appears in the tile. The number indicates the number of alerts for that aspect of the storage system. Click the alert tile to go directly to a summary of the problems.
- **Resource summary:** The middle area, with the information gauge, provides a summary of the capacity allocated from the registered storage systems.

Resource side panel

The resource side panel enables quick access to storage systems and to servers.

- Click **Storage Systems** to view and add storage systems.
- Click **Servers** to view and add servers.
- Click **Fabric Switches** to view and add fabric switches.
- Click **Virtual File Servers** to view and add virtual file servers. Displays if the storage system includes NAS modules.

Alert tiles

Across the top of the dashboard are tiles that display alerts for storage capacity, data protection, jobs, and hardware.

If a tile includes a circled check mark, there are no alerts for that part of the storage system, and everything is functioning normally. A number in a red circle within a tile indicates one or more problems with that part of the storage system.

You can click a tile for Capacity Alerts, Data Protection Alerts, or Hardware Alerts to view the summary for the category in the Monitoring tab.

The Jobs Alert tile displays the number of jobs in the last 24 hours with a status of **Failed** or **Success with Errors**.

Resource summary

The circular information gauge, which shows information about the available storage.

- If the storage systems include file storage, you can click **Block** or **File** next to the information gauge to view a legend and capacity values for either type of storage. Click **Unified** to view a legend and capacity values for both block and file.
- For block-only storage systems, the numerical data for each capacity parameter in the ring is displayed to the left of the information gauge.

- The number in the center of the rings shows the total usable capacity of all storage systems. The total usable capacity is the capacity available from all the parity groups across all storage systems.
  If you do not have any parity groups configured on the storage system, this number is zero and all other data points in the capacity visualization are zero.
- The white, middle ring indicates the sum of all pool capacity available across all storage systems. The light grey indicates the parity group capacity that is not yet allocated to pools.
  If you do not have any pools created, the white ring indicates zero. As you create pools, this number increases to eventually become equal to the total usable capacity when you have consumed all parity groups for pool creation.
- The black, outer ring indicates the subscribed capacity, which is the sum of all volumes created on storage pools. As you start creating volumes on storage pools, the subscription starts to increase.
  If volume allocation results in oversubscription, a thick line extends out to the right from the top of the ring. This extended line is a key visual indicator that helps track allocation oversubscription.
- The medium green ring indicates the storage utilization. As you create volumes on the pools and start consuming capacity, the utilization of thin pools increases and you will notice the value in green starting to increase.
  If the Thin Used (medium green ring) starts to increase and get closer to your total pool capacity, that indicates that the pools may be starting to fill up.
- Physical capacity allocated to file pools is indicated by medium blue in the File view and by light blue in the Unified view.
- File pool utilization is indicated by light blue in the File view and by light green in the Unified view.
- File over-commit capacity is represented by dark gray.

If you notice the total pool capacity (white) and Thin used (light green) values getting closer to total capacity, you may be running out of storage on one or more storage systems and may need to add disks to increase storage capacity. Review the information gauge for each storage system to identify which storage system needs additional capacity.

The right side of the resource summary offers alternate views:

- **Protection:** is the breakdown of data protection metrics including a representation of types of protected, unprotected, and secondary capacity and gauge of the total percentage of capacity protected.
- **Tier Breakdown:** is a visualization of the amount of each tier that is allocated to pools.

Analyzing data in the dashboard

The dashboard is a visual display of the important information needed to analyze the overall capacity utilization and health of your storage system. It provides visual indicators such as total usable capacity, current utilization, data protection summary, and monitoring alerts.

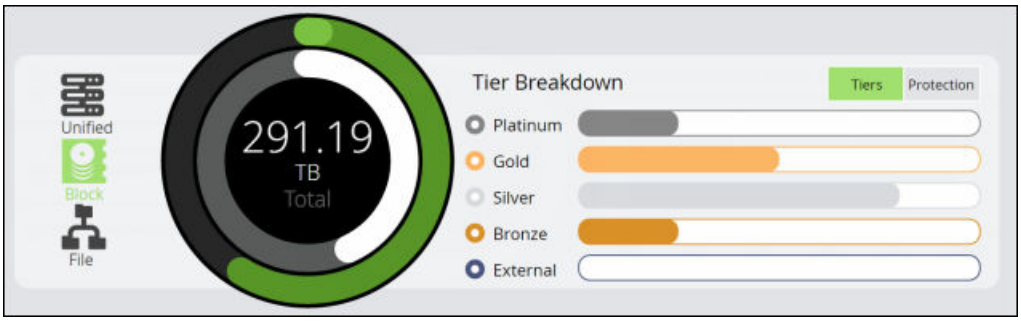
Analyzing data shown in alert tiles

The alert tiles collectively present the health of the storage system environment. In one glance you can verify that the overall health is sound if you see no alerts on the alert tiles. This means that there are no capacity or hardware issues in the environment, no failed jobs in the last 24 hours and that the data protection is working without any issues.

If there are any alerts, you can drill down to the relevant alert page to investigate the cause. Storage Advisor provides alerts for capacity utilization, hardware, data protection, and jobs status.

Analyzing data in the information gauge

The information gauge provides a visual indication of the total capacity of all storage systems managed by Storage Advisor.



The capacity indicated in the center of the ring is the total usable capacity available via the configured parity groups. After you add a storage system and configure parity groups, the total capacity indicator will show the capacity from the newly added storage system. The Thin Used capacity (green ring) indicates the total capacity that is currently being used. If the usage is around 70-80% of the total capacity, you may receive capacity alerts based on the thresholds set by your storage administrator. The default thresholds are 70% and 80%, and can be changed during pool creation.

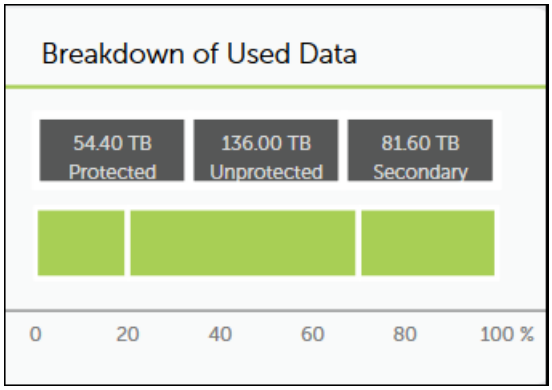
The white ring that provides a sum of capacities of all pools in the systems should be closer to 100% capacity. This would mean that you are using your entire parity group capacity by allocating it to pools. If the Thin Used capacity in green ring nears the total capacity (white ring) then you may run out of pool capacity soon. In such a case, expand the pool to consume more capacity.

If you notice that the total pool capacity (white) and Thin used (light green) values are getting closer to total capacity, you may be running out of disk capacity on one or more storage systems and would need to add disk space to increase storage capacity. Review the information gauge for each storage system to identify which storage system needs additional capacity.

Capacity subscription beyond the total available capacity should not be an issue if your thin capacity utilization is well within the total capacity.

Analyzing data protection metrics

The balance of your protected primary volumes and secondary volumes depends on the number of copies you have chosen to maintain, and also on the type of the data protection technology being used. If you choose to set aside more volumes for data protection, then the overall usable capacity may be affected. On the other hand, if you have a large amount of unprotected data, you may want to consider data protection options.



Inventory and resource information

The inventory pages display details about the storage system resources in Storage Advisor. These resources include storage systems, servers, ports, and pools, volumes, parity groups, external parity groups (if the storage system has external storage), and replication groups. If the storage system has NAS modules, resources will also include file pools, virtual file servers, file systems, and shares and exports. Common actions can be performed on the inventory pages, such as the following:

- You can select one or more resources and delete them.
  When you delete a storage system, you disassociate it from Storage Advisor. When you delete a pool or volume, the resource is de-provisioned and removed from the storage system.
- When a parity group is deleted, it is removed from the storage system and the disks used to create the parity group are no longer in use. You can delete the parity group if you want to reconfigure the storage system with some other RAID configuration or simply decommission the array. If the parity group is in use by a pool, the parity group deletion will fail.

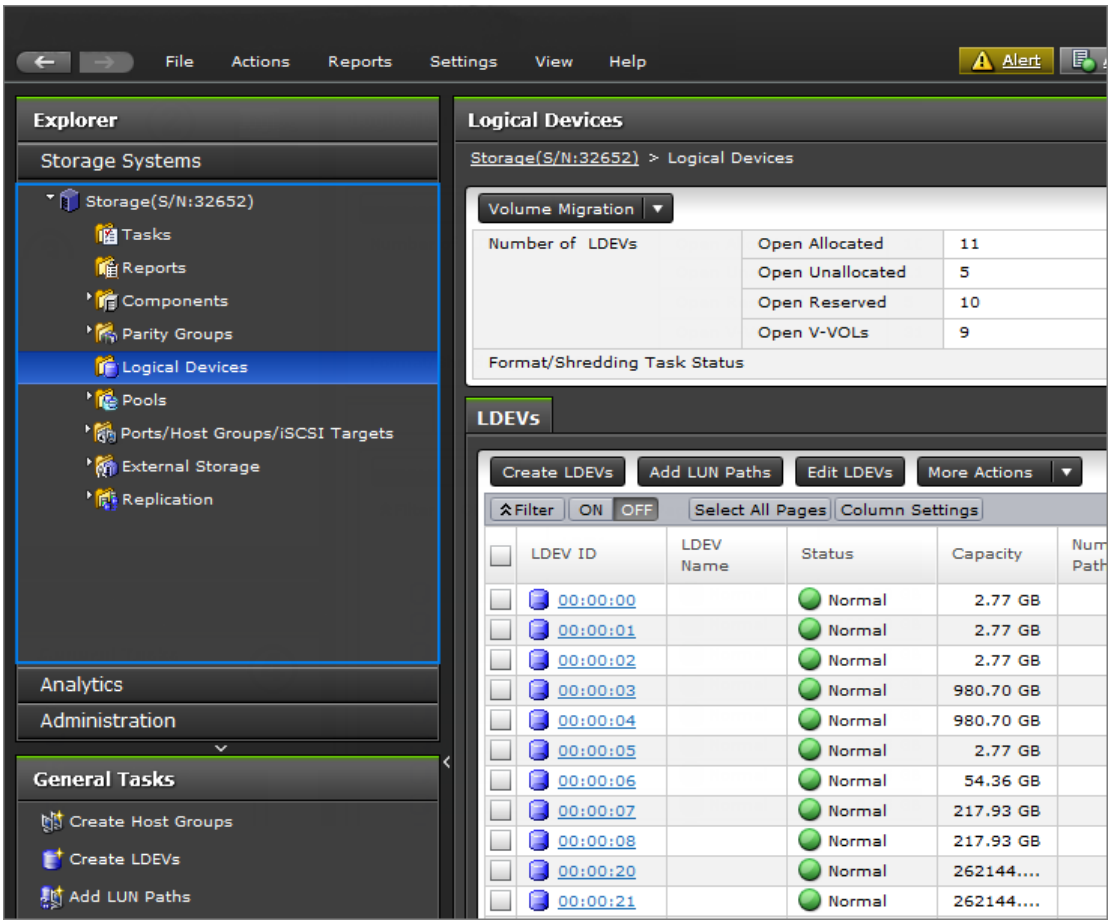
- You can select one or more of the same type of resources and update their properties. The properties that can be updated depend on the type of resource.
- You can click a particular resource to see more details about it on its resource detail page.
    - When you delete a block pool, the parity groups used by the pool will no longer be in In Use status. The pool volumes on these parity groups will be formatted and the parity group will eventually be in Available status.
    - When you delete a volume, the pool subscription will go down. Volume deletion will fail if the volume participates in data protection or is attached to a server.
    - When you delete a file pool, the underlying related block pool is deleted.
    - When you delete a server, the server is disassociated from Storage Advisor. You will no longer be able to provision volumes to the server (or its WWNs). Server deletion will fail if it has volumes attached to it.

Device Manager - Storage Navigator

Device Manager - Storage Navigator (HDvM - SN) is the element manager for managing block operations on VSP G200, G400, G600, G800 and VSP F400, F600, F800 storage systems. It is a factory-installed application that runs on the service processor (SVP) 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.

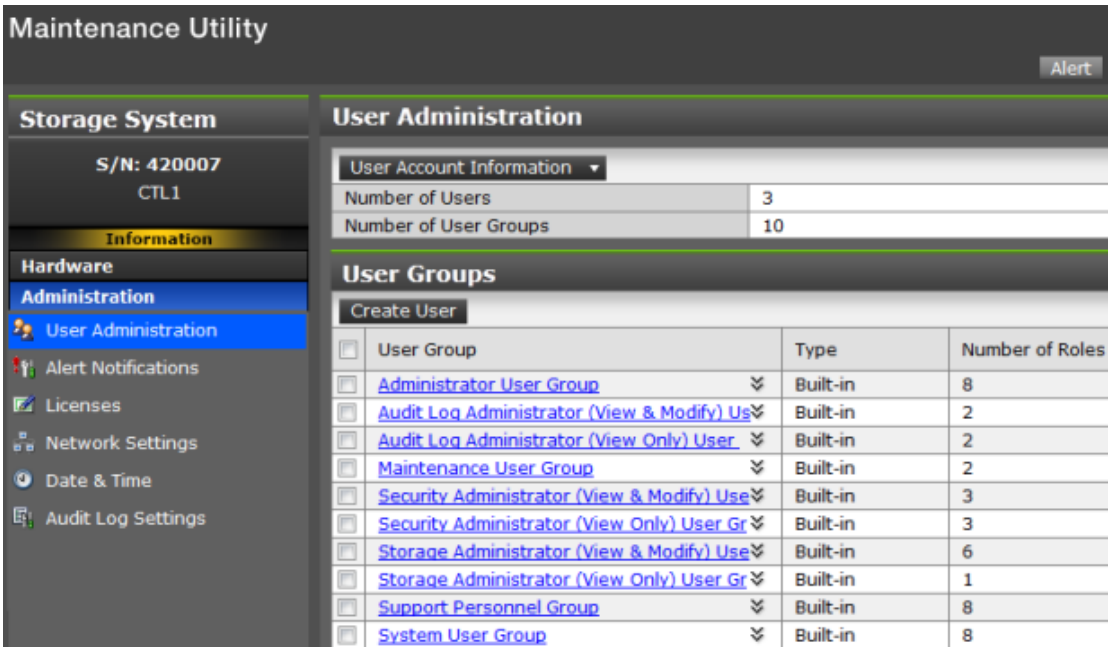
In addition to the information in this guide, the HDvM - SN online help has procedures for setting up and managing the storage system.



Maintenance utility

The maintenance utility allows you to perform administration tasks on VSP Gx00 models or VSP Fx00 models. You can access this tool from either HDvM - SN, SMU, 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.



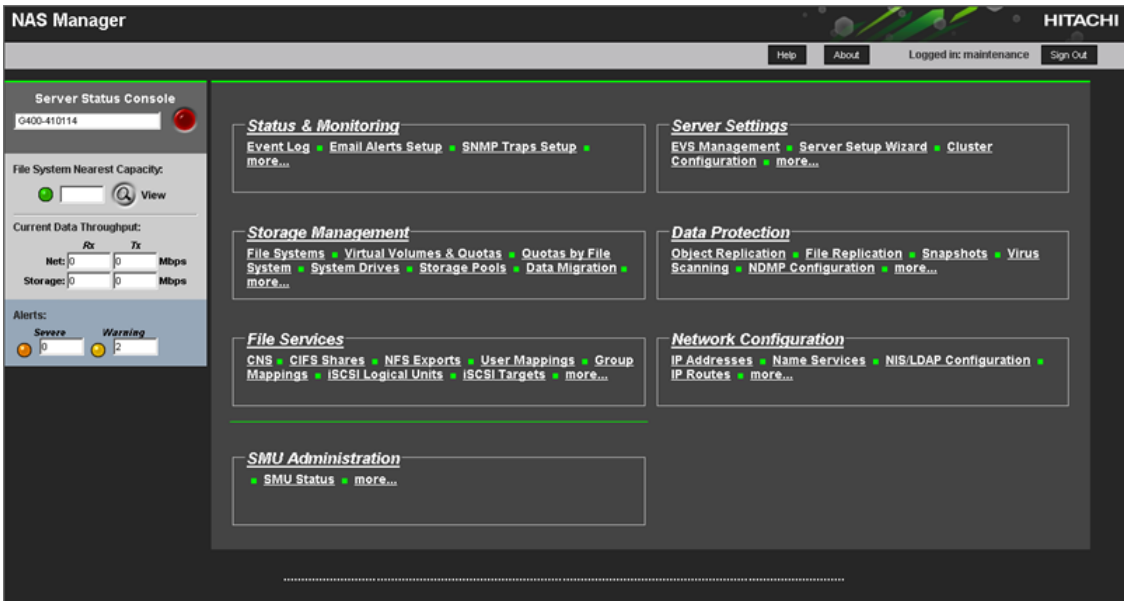
The maintenance utility online help provides procedural information for supported storage system administration tasks. Links to storage system tasks, search functions, and a glossary are included.

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 customer support personnel or by authorized service providers.

NAS Manager

NAS Manager is the element manager for NAS modules. It is a factory-installed application running on the NAS module.

NAS Manager provides a web-based interface for managing stand-alone or clustered servers and their attached storage systems. This tool allows you to perform most administrative tasks from any client on the network using a network browser. To access NAS Manager, point your browser to the following URL: `https://<unified-management-IP-address>:20443`. You can also access NAS Manager from a command line interface. For information, see the *Command Line Reference*, which is accessible through the **Documentation** page of NAS Manager or the *NAS Platform System Access Guide*.


NAS Manager
HITACHI
Help
About
Logged in: maintenance
Sign Out
Server Status Console
G400-410114
File System Nearest Capacity:
View
Current Data Throughput:
Rx
Tx
Net:
Storage:
Mbps
Alerts:
Severe
Warning
Status & Monitoring
Event Log
Email Alerts Setup
SNMP Traps Setup
more...
Server Settings
EVS Management
Server Setup Wizard
Cluster Configuration
more...
Storage Management
File Systems
Virtual Volumes & Quotas
Quotas by File System
System Drives
Storage Pools
Data Migration
more...
Data Protection
Object Replication
File Replication
Snapshots
Virus Scanning
NDMP Configuration
more...
File Services
CNS
CIFS Shares
NFS Exports
User Mappings
Group Mappings
iSCSI Logical Units
iSCSI Targets
more...
Network Configuration
IP Addresses
Name Services
NIS/LDAP Configuration
IP Routes
more...
SMU Administration
SMU Status
more...

2

Preparing your management software

Use the information in this chapter to prepare the management software you want to use to administer your storage system.

- ☐ Installing Storage Advisor
- ☐ Using Device Manager - Storage Navigator
- ☐ Onboarding and configuring a storage system
- ☐ Using the maintenance utility
- ☐ Accessing a storage system without management software

Installing Storage Advisor

Storage Advisor is deployed on a virtual machine and accessed by a client computer. Review the minimum requirements before installing.

Installing Storage Advisor with the application installer

You can install Storage Advisor on Linux, where Docker v1.11.2 is already installed.

In order to enable maximum control of the environment, the application installer does not include Docker, an operating system, or a VM.

Before you begin

The following are required:

- Root access to the operating system where Storage Advisor will be installed.
- Docker v1.11.2 installed in a Linux environment.
- The recommended available space on the server at the time of installation is 100 GB. This is due to the additional capacity required for the installer file and Docker requirements for image installation. After installation is complete, the required space is reduced to 40 GB.
- 16 GB RAM



Note: It is recommended that the location where Storage Advisor is installed not include any other applications.

Procedure

1. On the Linux environment, configure the network interface that will be used to access Storage Advisor.

   Storage Advisor supports user interface and API access via an IPv4 address.
2. Copy the tar file `installer.tar.gz` from the installation media to any folder in the Linux environment and unzip it.
3. Navigate to the installer script: `HSA-2.1.0.xx-all-installer` and execute it.

   At the prompts, enter the following:

   1. `Enter the username for the installer`: Enter `sysadmin`
   2. `Enter the <users> password`: Enter `sysadmin`
   3. `Enter host's IP`: Enter the IP address that will be used to access Storage Advisor. This IP address will also be used for SNMP communications into the storage system.

   The installation may take a few minutes. At completion, messages will indicate the following:

- The application was successfully added.
- The API is ready.
- Any pre-existing app manager containers have been removed.

4. Set the SNMP IP address in Virtual Appliance Manager:
   a. Open a browser and enter `https://ip-address/vam` in the address bar.
      - User name: sysadmin
      - Password: sysadmin
   b. In the **Network** tab, enter the SNMP IP address for the storage system.

Troubleshooting the installation

If the installation fails, try the following:

- If the installation fails with the (401) error code, the user name and password specified by the installer was incorrect. Retry the installation and ensure that `sysadmin` is entered for both user name and password.
- Delete all Storage Advisor containers and images and start the installation again.
- Check the Docker logs.
- Consult Docker documentation for more information on how to perform these actions.

If the installation produces any warnings, they may point to the cause of the problem. Correct any issues the installer identifies, delete any Storage Advisor containers and images and start the installation again.

Next steps

Change the root password.

If required, you can generate and install a signed SSL certificate.

Installing Storage Advisor with the virtual appliance

Installing Hitachi Storage Advisor in a DHCP environment

If your environment includes DHCP servers, you can use the Virtual Appliance Manager to set up your Storage Advisor server.

Before you begin

The initial setup of a discovered supported storage system has been completed by an authorized service provider.

Procedure

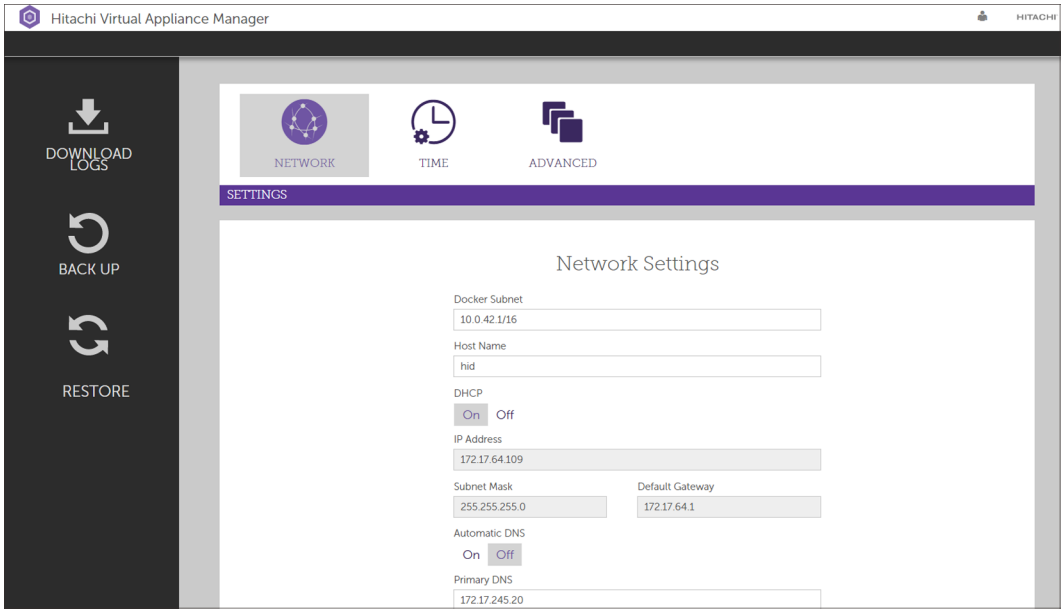
1. From the installation media, deploy the Storage Advisor OVF to the ESXi host.
2. Start the Storage Advisor virtual machine.
3. In the vSphere® client, wait for the **System status** to change to `Online`.

   The status is just below the banner in the virtual machine console.

   ```
   ****************************************
   *****Hitachi Storage Advisor*****
   ****************************************
   System status: Online
   Please wait for system to be online before using any
   services.
   ```
4. Open a browser and enter `https://`*`ip-address`*`/vam` in the address bar.

   User name: `service`
   Password: `Chang3Me!`
5. Change your password.

   a. Click and select **Change password**.
   b. Enter your new password.
6. From the Virtual Appliance Manager menu, click **Network** to configure the network settings.



   a. (Optional) Enter the IP range in the **Docker Subnet** field in the format *`ip-address\range`*. This is the specified range used by Storage Advisor.

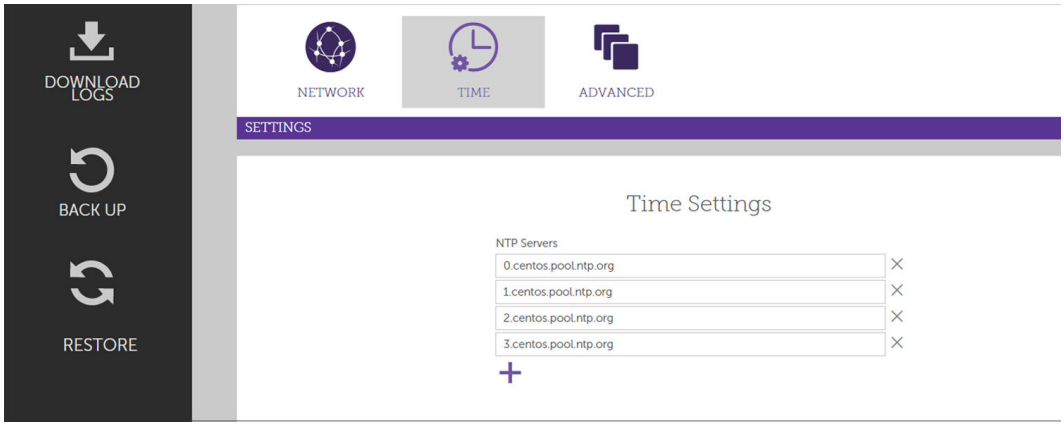
Note: If your data center is using the IP address scheme `172.17.*.*`, make sure you provide another IP range that is not currently used in your environment.

b. Set the host name for the virtual machine.
c. Set **DHCP** to `On`.
d. Enter the IP address of the Storage Advisor server.
e. Set **Automatic DNS** to `On` or `Off`.

   If you set this to `Off`, enter the IP address of at least one DNS server.
f. Click **Submit**.

7. (Optional) From the Virtual Appliance Manager menu, click **Time** and add Network Time Protocol (NTP) servers to the virtual machine.

   Adding NTP servers verifies that the Storage Advisor servers are synchronized with the storage system environment.



a. Click **+** to add a field for an NTP Server.
b. Enter the host name of the NTP server.
c. Click **Submit**.

Next steps

- Change the root password.
- Log in to Storage Advisor and onboard a storage system.
- Get a digitally signed SSL certificate from a trusted certificate authority (CA) by sending the CA a certificate signing request (CSR). After you obtain the signed certificate, you can import it to the server. By default, the Storage Advisor installation package comes with a self-signed certificate that you can use to initially log in to Storage Advisor.

Installing Hitachi Storage Advisor in a static environment

If you do not have a DHCP server, use the command line interface to indicate the static IP address of the Storage Advisor server.

Before you begin

Procedure

1. From the installation media, deploy the Storage Advisor OVF to the ESXi host.
2. Start the Storage Advisor virtual machine.
3. In the vSphere® client, wait for the **System status** to change to `Online`.

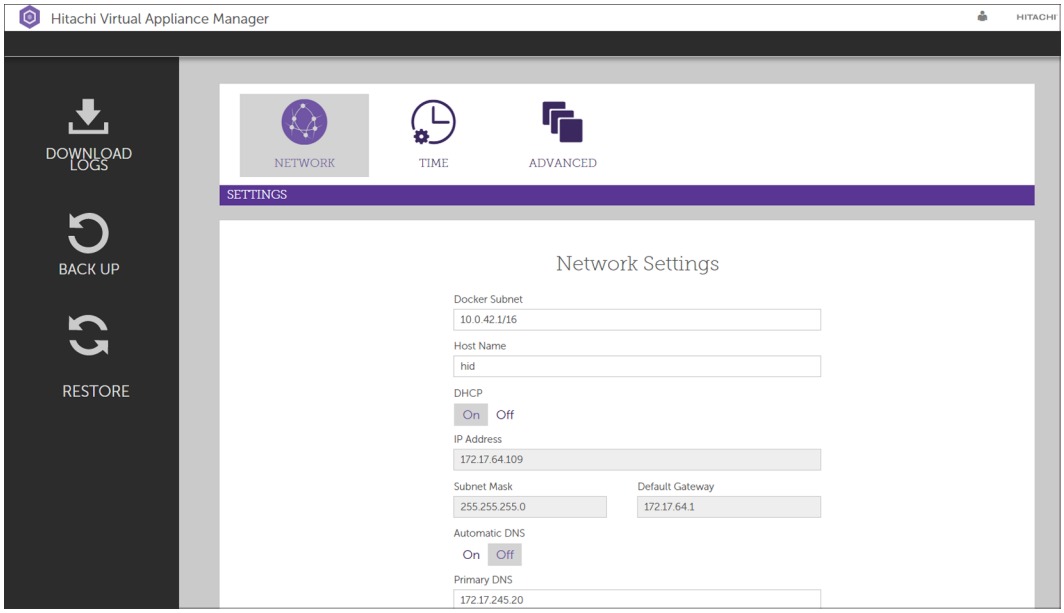
   The status is just below the banner in the virtual machine console.

   ```
   ****************************************
   *****Hitachi Storage Advisor*****
   ****************************************
   System status: Online
   Please wait for system to be online before using any
   services.
   ```
4. Press **Alt**+**F2**.
5. Log in with the service account.

   User name: `service`
   Password: `Chang3Me!`
6. Enter the command `ip-change`.
   The Change IP Address Utility opens.
7. Enter your settings at the prompts.
8. Reboot the VM to ensure that it has the IP address.
9. Open a browser and enter `https://`*`ip-address`*`/vam` in the address bar.

   User name: `service`
   Password: `Chang3Me!`
10. Change your password.

    a. Click and select **Change password**.
    b. Enter your new password.
11. From the Virtual Appliance Manager menu, click **Network** to configure the network settings.



a. (Optional) Enter the IP range in the **Docker Subnet** field in the format *ip-address\range*. This is the specified range used by Storage Advisor.

Note: If your data center is using the IP address scheme `172.17.*.*`, make sure you provide another IP range that is not currently used in your environment.

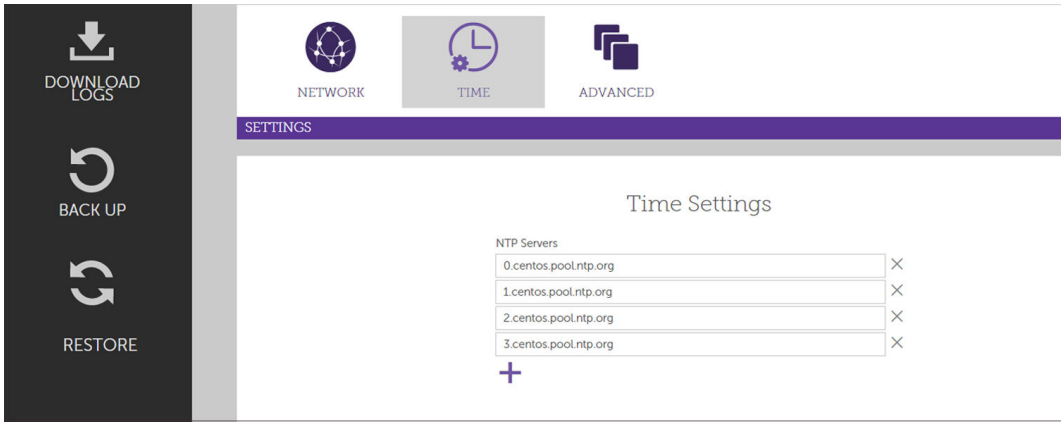
---

b. Set the host name for the virtual machine.
c. Set **DHCP** to `Off`.
d. Enter the IP address of the Storage Advisor server.
e. Set **Automatic DNS** to `On` or `Off`.

   If you set this to `Off`, enter the IP address of at least one DNS server.
f. Click **Submit**.

12. (Optional) From the Virtual Appliance Manager menu, click **Time** and add Network Time Protocol (NTP) servers to the virtual machine.

Adding NTP servers verifies that the Storage Advisor servers are synchronized with the storage system environment.



a. Click **+** to add a field for an NTP Server.
b. Enter the host name of the NTP server.
c. Click **Submit**.

Next steps

- Change the root password.
- Log in to Storage Advisor and onboard a storage system.
- Get a digitally signed SSL certificate from a trusted certificate authority (CA) by sending the CA a certificate signing request (CSR). After you obtain the signed certificate, you can import it to the server. By default, the Storage Advisor installation package comes with a self-signed certificate that you can use to initially log in to Storage Advisor.

Changing the root password immediately after installation

Change the root password immediately after installing Storage Advisor.

Procedure

1. Either open an SSH connection to the VM or open the VMware console and press `Alt+F2` to reach the console.
2. Login as root account using the default password:
   `3kO$Pe9dJyjy29HAi2mS`
3. Run the command `passwd root` in the terminal.
4. Enter the new password when prompted.

Logging in to Storage Advisor

Log in and verify that the installation is successful by accessing the Storage Advisor web interface from a browser.

Procedure

1. Open a web browser.

2. Enter the URL for Storage Advisor in the address bar:
   `https://ip-address:port-number`

   where:
   - *ip-address* is the IP address of the Storage Advisor server.
   - *port-number* is the port number of the Storage Advisor server. The default port number is 443.
3. In the login window, log in to Storage Advisor.

   User name: `sysadmin`
   Password: `sysadmin`

Logging in when Storage Advisor is not available

For the Virtual Storage Platform F400, F600, F800, Virtual Storage Platform G200, G400, G600, G800, and Virtual Storage Platform G1000 storage systems, if Storage Advisor is not available and you have an administrator login account with the required permissions, you can log in directly to Device Manager - Storage Navigator.

Before you begin

- You are managing VSP Fx00 models, VSP Gx00 models, VSP G1000, VSP G1500, or VSP F1500 storage systems.
- You must have an administrator login account with the required permissions. For information about creating user accounts in Hitachi Device Manager - Storage Navigator, see the *System Administrator Guide* for your storage system.

Procedure

1. Start a web browser.
2. Enter the URL:
   - For VSP G1000, VSP G1500, or VSP F1500 storage systems, enter: `https://IP-address-or-host-name-of-the-SVP/sanproject/emergency.do`
   - For VSP G200 storage systems, enter: `https://IP-address-or-host-name-of-the-SVP/dev/storage/8320004XXXXX/emergency.do` (where the model number is '8320004' and '4XXXXX' indicates the system serial number)
   - For VSP G400, G600 storage systems and VSP F400, F600 storage systems, enter: `https://IP-address-or-host-name-of-the-SVP/dev/storage/8340004XXXXX/emergency.do` (where the model number is '8340004' and '4XXXXX' indicates the system serial number)
   - For VSP G800 and VSP F800 storage systems, enter: `https://IP-address-or-host-name-of-the-SVP/dev/storage/8360004XXXXX/emergency.do` (where the model number is '8360004' and '4XXXXX' indicates the system serial number)

3. 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.
4. Enter the user ID and password for the account.
5. Click **Log In**.
6. If the Security Information dialog box appears, click **Yes**.
7. 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. Denying the request might reduce processing speed.

Result

You are successfully logged in to Device Manager - Storage Navigator.

Note: If the login process fails three times by using 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.

Generating and installing a signed SSL certificate

By default, a self-signed certificate is used by the server. SSL certificates are used to verify the user's identity and to enhance security on the server. You can get a digitally signed SSL certificate from a trusted certificate authority (CA) by sending a certificate signing request (CSR). After you obtain the signed certificate, you can import it to the server.

The following is a sample procedure for generating and installing a signed SSL certificate. The process of obtaining a certificate may be different within each organization.

Procedure

1. Open the virtual machine console and log in with the service account.
2. Start the `openssl` program:

   ```
   openssl req –nodes –x509 -newkey rsa:2048 -sha1 -keyout /etc/nginx/certificates/server.key -out /etc/nginx/certificates/server.crt
   ```

   The system returns the message `Generating a 2048 bit RSA private key.`
3. Provide the information as prompted.

- **Country Name** (two-letter code)
- **State or Province Name** (two-letter code)
- **Locality name** (City)
- **Organization Name** (Company)
- **Organizational Unit Name** (Section or department)
- **Common Name** (Your name or the server host name)
- **Email Address**

4. When you receive the CRT file, send it to a certificate authority to obtain an SSL certificate.

   If you need help with this step, consult with your Hitachi Data Systems representative or authorized service provider.
5. Open a browser and enter the Virtual Appliance Manager URL in the address bar.
   For example, `https://ip-address/vam`
6. Click **Advanced**.
7. Click the **Certificate Settings** tab.
8. Import the certificate into the server.
   a. Open the signed certificate (received from the certificate authority) in a text editor.
   b. Open the private key file (generated in step 2) in a text editor.
   c. Copy the certificate file contents into the **Certificate** text box.
   d. Copy the private key file contents into the **Private Key** text box.
   e. Click **Submit**.

Using Device Manager - Storage Navigator

To configure the storage system using Hitachi Device Manager - Storage Navigator, set up a client computer, and then log in to Hitachi Device Manager - Storage Navigator.

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:

- Ensuring that management clients can access and use Device Manager - Storage Navigator.
- Configuring the server if you use a physical or virtual server running Windows as a management client.

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 management clients (Device Manager - Storage Navigator) can access the same SVP 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 customer support to use other combinations or versions. To see the latest platform listed in the applicable product documents, visit our web site from the following URL: https://knowledge.hds.com/Documents.

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

Software requirements

Operating system[1]	Architecture	Browser	Java Runtime Environment (JRE)	Adobe Flash Player[2]
Windows 7 SP1	32 bit or 64 bit	Internet Explorer 11.0[3]	JRE 7.0 Update 67	14.0
Windows 8.1	32 bit or 64 bit	Internet Explorer 11.0[3]	JRE 7.0 Update 67	14.0
		Google Chrome 48.0 or later	JRE 8.0 Update 71	20.0

Operating system[1]	Architecture	Browser	Java Runtime Environment (JRE)	Adobe Flash Player[2]
Windows 8.1	64 bit	Internet Explorer 11.0[3]	JRE 7.0	20.0
	64 bit	Internet Explorer 11.0[3]	JRE 7.0	21.0
	64 bit	Google Chrome	JRE 7.0 or later	Installed as a plug-in of Web browser
Windows 10	64 bit	Internet Explorer 11.0[3]	JRE 7.0	20.0
	64 bit	Internet Explorer 11.0[3]	JRE 7.0	21.0
	64 bit		JRE 7.0 or later	Installed as a plug-in of Web browser
Windows Server 2008 R2 (SP1)	64 bit	Internet Explorer 11.0[3]	JRE 7.0 Update 67	14.0
Windows Server 2012 SP1	64 bit	Internet Explorer 10.0[3]	JRE 7.0 Update 67	14.0
Windows Server 2012 R2 SP1	64 bit	Internet Explorer 11.0[3]	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.
3. Only the latest version of Internet Explorer active on each OS is supported, according to Microsoft support policy.

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 customer support to use other combinations or versions. To see the latest platform listed in the applicable product documents, visit our web site from the following URL: https://knowledge.hds.com/Documents.

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

Item	Requirement
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-TX 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.

Configuring Internet Explorer for Device Manager - Storage Navigator

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

Before you begin

- 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.

Before you begin

- 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 or Storage Advisor 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 or Storage Advisor to configure the storage system.

Procedure

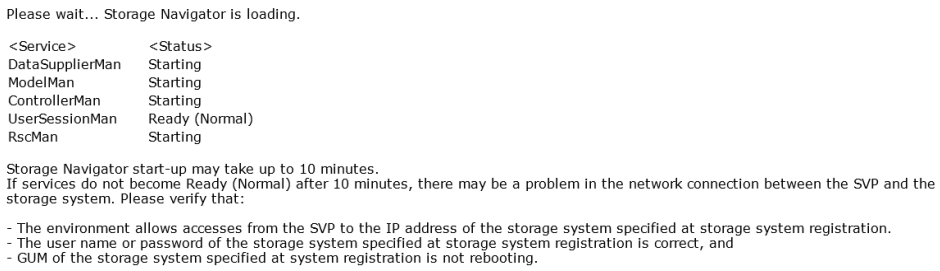
1. In your web browser, specify the following URL:

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

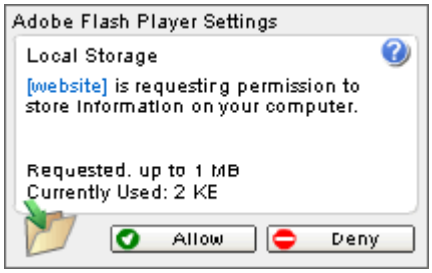
   If you changed the port number of the protocol HTTP from the initial value (443), specify the following URL:

   `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.



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 computers on page 49.
   - If multiple storage systems are connected, a window which allows selection of the storage system is displayed. Select the storage system you want to connect.
3. When the Storage Device List window opens, select the storage system. The Device Manager - Storage Navigator login window appears.
4. Type the user ID and password.
5. Click **Login**.
6. If the **Security Information** dialog box appears, click **Yes**.
7. 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.



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. 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. When you use a web browser for a long period of time, memory is heavily used. We recommend closing or logging out of Device Manager - Storage Navigator after you are finished using it.

Changing your password

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

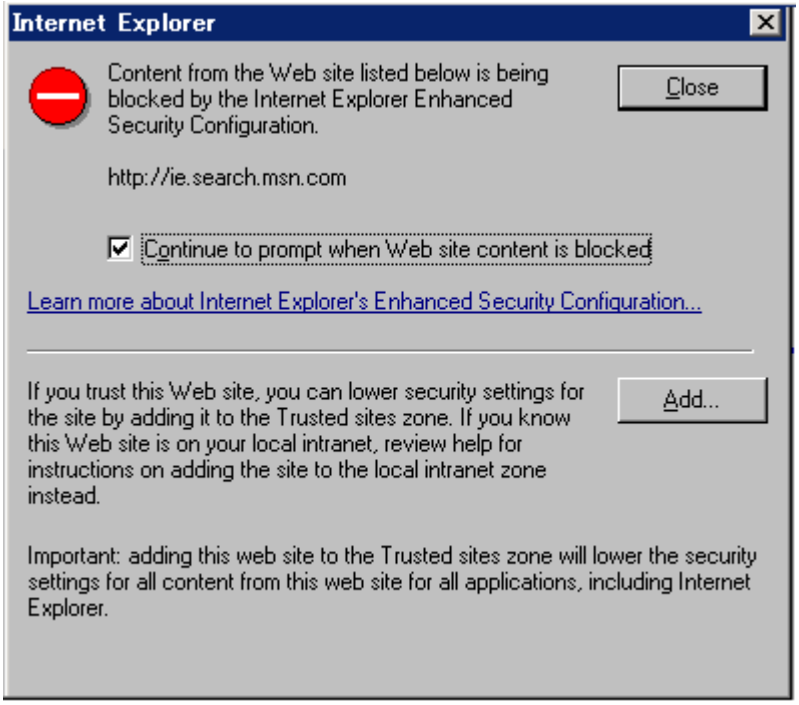
Procedure

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 computers

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

The message below may appear differently depending on the Windows version you are using.



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.

Onboarding and configuring a storage system

Onboarding a storage system is the process of associating it with Storage Advisor. After the storage system is onboarded, manage it from the Storage Advisor dashboard.

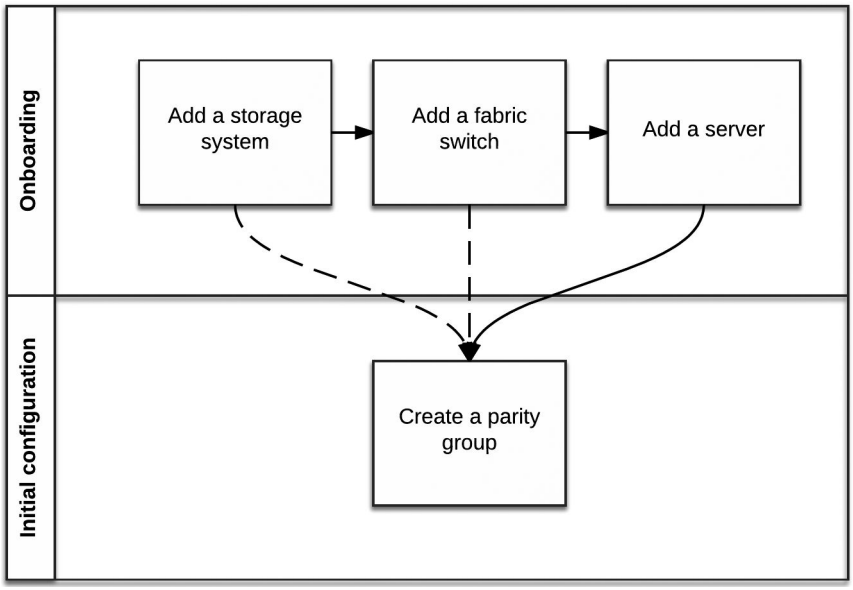
If the storage system includes NAS modules, the file storage is automatically added with the block storage.

Storage Advisor requires access to all resources groups on the storage system so that the workflows function correctly. Verify that the service processor user name used to onboard a storage system in Storage Advisor has access to all custom resource groups and meta resource groups

Overview

Onboarding a storage system in Storage Advisor is more than adding a storage system to a list. At least one fabric switch and server must be added for the storage system to be able to provision volumes to the server.

In the following workflow, the recommended path is marked by the solid arrows. The dashed arrows indicate the optional paths. Before a storage system is available for use in the network, all of the tasks in the workflow must be complete.



Adding the first storage system

You must onboard a storage system the first time you start Storage Advisor.

Before you begin

Storage Advisor requires access to all resources groups on the storage system so that the workflows function correctly. Verify that the service processor (SVP) user name used to onboard a storage system in Storage Advisor has access to all custom resource groups and meta resource groups.

If a storage array includes block storage and NAS modules, the file storage is automatically added with the block storage. Then file pools and other file resources can be created in the Storage Advisor web interface or by using the API.

You can add up to eight VSP Gx00 or VSP Fx00 storage systems at once by specifying an SVP IP address that has multiple storage systems. Storage systems with different credentials cannot be added in the same operation.

Procedure

1. On the Storage Advisor dashboard, click the plus sign (**+**) to add a storage system.
2. Enter values for the following parameters on the **Add Storage System** page.
   - **SVP IP Address:** Enter the IP address of the external service processor for the storage system you want to discover.
   - **User name and password:** Log in as a user that has administrator privileges on this storage system. For example, you can log in as the user `maintenance`.
3. Click **Submit**.
4. (Optional) Onboard other storage systems.

Result

The Jobs tab is updated with the job called `Create Storage System`. If multiple storage systems are being added, there will be a job for each one.

Wait a while for the storage system to be added. Refresh the Jobs tab to verify that storage system is onboarded.

Next steps

- Verify the storage system initial settings.
- Create parity groups.



Note: Parity groups are created by a service representative. Parity groups for a Hitachi Virtual Storage Platform G1000 storage system are created outside of Storage Advisor.

Adding a fabric switch

You can add a fabric switch after onboarding a storage system. Add, update, and delete fabric switches in the Storage Advisor interface.

After a fabric switch is added, you can choose to auto-create zones during volume provisioning. A fabric switch is required for any operations that use auto-select, such as host group creation and auto-selection of ports while attaching volumes to servers.

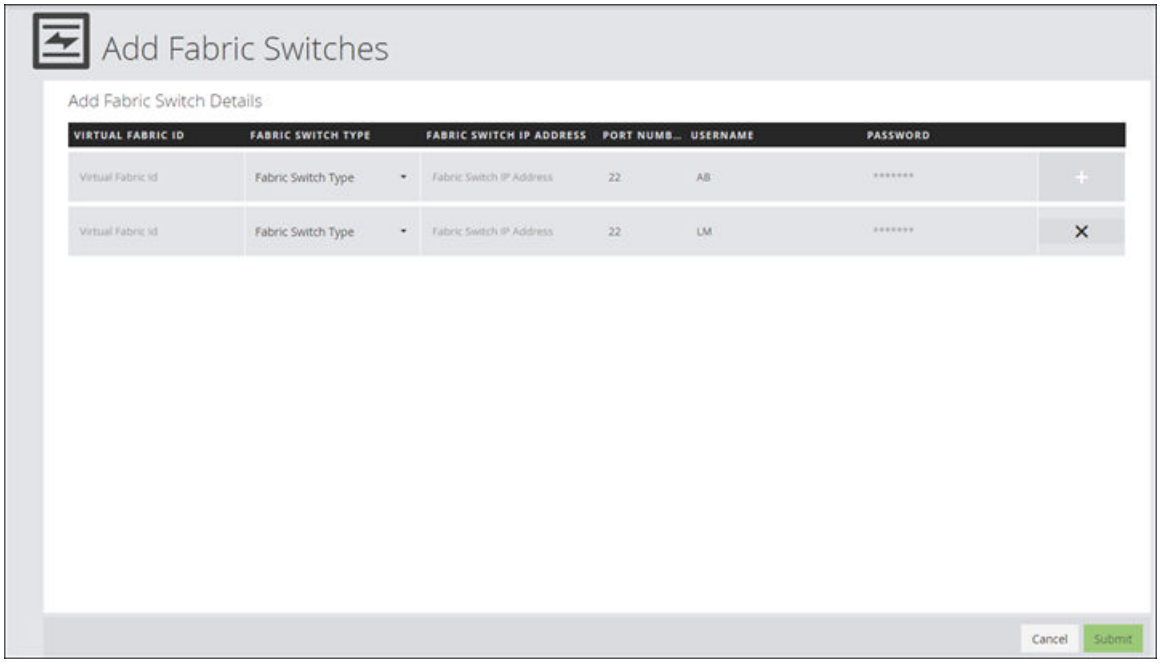
Before you begin

- Verify that servers and ports are connected according to the manufacturer's instructions.
- Verify that there is an active zone set with at least one dummy zone available.
- The Storage Advisor server is connected to the same IP network and has access to SNMP broadcast of Fibre Channel switches.

- Verify the required information about the fabric switch: Virtual Fabric ID (required only for Cisco switches), Fabric Switch Type, Fabric Switch IP Address, Port Number, Username, and Password.
- Verify that you have the Admin role for the fabric switch.

Procedure

1. On the Storage Advisor dashboard, select **Fabric Switches** to open the **Fabric Switches** page.
2. Click the plus sign (**+**) to open the **Add Fabric Switches** page.



3. Enter the following information from the configuration of the switch you are adding:
   - **Virtual Fabric ID**: For Cisco switches, the VSAN ID. Not applicable to Brocade switches.
   - **Fabric Switch Type**: Select **Brocade** or **Cisco**.
   - **Fabric Switch IP Address**
     To add or update a core switch, use the Management IP address of the switch or the Active CP IP address.
   - **Port Number**
   - **Username**
   - **Password**
4. Click **Submit**.

Result

A job is created to add the fabric switch.

Adding servers

Add servers so you can attach volumes. You can add multiple server parameters from a file, or add one server at a time.

There are two methods of adding servers:

- Manually add information for one server at a time.
- Import a CSV (comma-separated values) file with information for one server in each row.
  The CSV file must have the following headings, in the order specified: Name, Description, IPAddress, OSType, WWNs (comma separated list of WWNs). All fields are required except Description and IPAddress. Valid OSType values are as follows:
  - AIX
  - HP_UX
  - LINUX
  - NETWARE
  - OVMS
  - SOLARIS
  - TRU64
  - VMWARE
  - VMWARE_EX
  - WIN
  - WIN_EX

Procedure

1. On the Storage Advisor dashboard, click **Servers**. Then click the plus sign (**+**) to open the **Add Server** page.
2. On the **Add Server** page, do one of the following:
   - Click the upper plus sign (**+**) to browse for the CSV file or drag the file to the plus sign. The values from the file will populate the page.
   - Click the plus sign (**+**) in the table to add a row and enter a **Name**, **Description** (optional), **IP Address** (optional), **OS Type**, and **WWN**. You can add more servers by clicking the plus sign.
3. Click **Submit** to add the servers.

Result

A job is started to add the servers.

Next steps

Create volumes and attach them to the server.

Creating parity groups

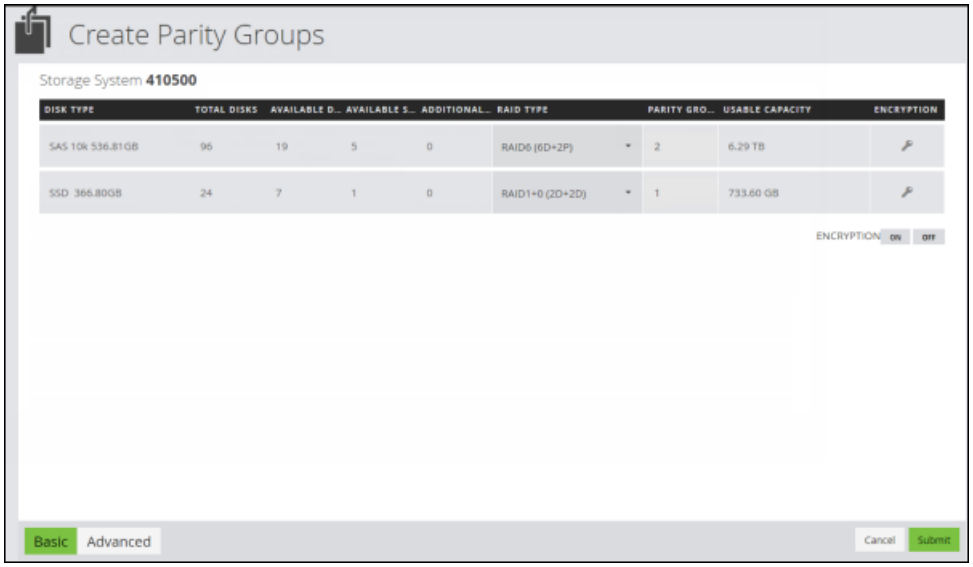
Note: Parity groups for VSP G1000 storage systems are created outside Storage Advisor by an authorized service representative.

Before you begin

- Complete the initial setup of any discovered supported storage system.
- Register the storage system for which you will create a parity group.
- Verify the target storage system name.
- Verify the total capacity that you expect to use. Plan to use all of the available disks in the system when you create parity groups.

Procedure

1. On the Storage Advisor dashboard, select **Storage Systems** in the resource side panel to see the inventory of registered storage systems.
2. Click a storage system to create and configure the parity groups for it.
3. Click **Parity Groups** to see the inventory of all parity groups in the storage system.
4. Click the plus sign (**+**). In the **Create Parity Groups** window, review the list of unused disk types in the storage system. This information is grouped by disk type, disk speed, and disk capacity, and includes the following details:
   - Number of available disks.
   - Available spares detected for each disk type, disk speed, and capacity.
   - Number of new or additional spares to reserve. This calculation is based on the total spares needed based on recommended best practices, and the number of existing spares in the system.
   - The recommended RAID configuration for the disk type.
   - The number of parity groups that can be created.
   - The total usable capacity that is available based on the number of parity groups and the RAID configuration.



5. Choose one of the following options:
   - Accept the recommended RAID configuration, which uses the full capacity of the installed drives.

- Change the RAID configuration or create fewer parity groups. If you make changes, you might not use the full capacity of the installed drives.

6. (Optional) Click Encryption **ON** if you want to use encryption.

   Prerequisites for enabling encryption:
   - The storage system must have an Encryption Disk Board.
   - Encryption License Key must be installed.
   - The Key Management Server must be configured on the SVP.

   Note: Encryption cannot be disabled in Storage Advisor.

7. Click **Submit**.

Result

A job is started to create the parity group for the storage system. This job includes the following tasks:
- Identifies the appropriate number and position for the spare disk.
- Assigns a spare disk.
- Creates the required number of parity groups for the requested RAID layout.
- Creates and quick formats the necessary volumes on the parity group so that it is ready for pool creation.
- The job may create sub-jobs when multiple parity groups are being created. Each sub-job will show the status of the parity groups being created.

Note: If you are creating parity groups for the entire array, it may take several hours before the storage system is configured.

Next steps

- Create a pool.
- Create and attach volumes.

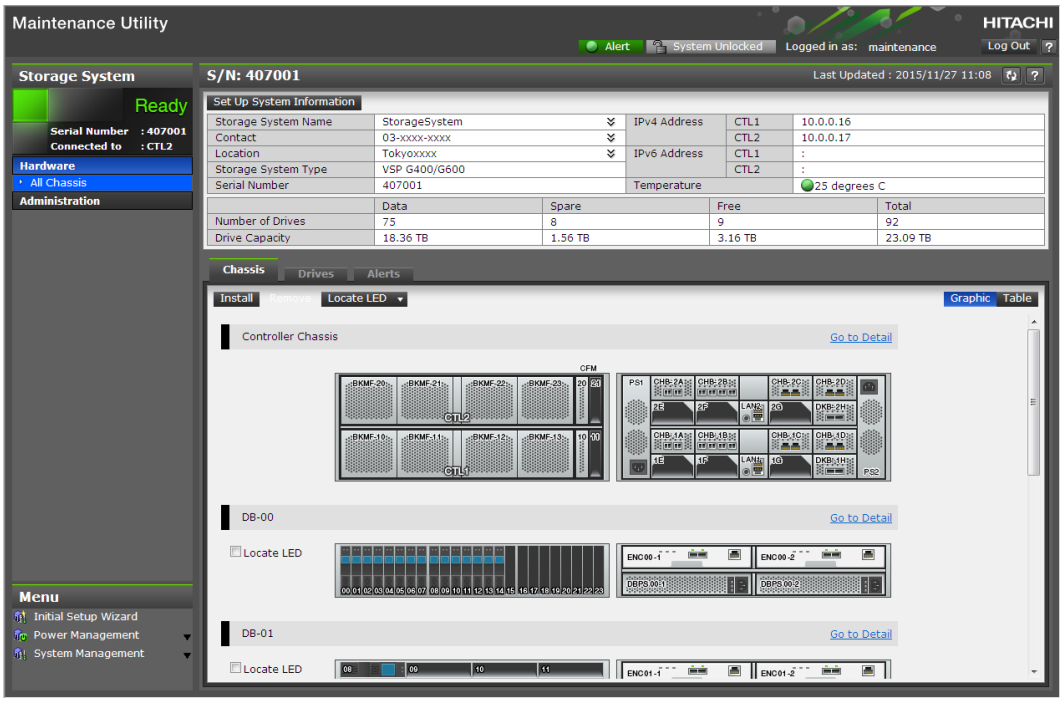
Note: For further information, access Help from within the Storage Advisor web interface.

Using the maintenance utility

To configure the storage system using the maintenance utility, start the maintenance utility from Hitachi Command Suite or Hitachi Device Manager - Storage Navigator.

Note:

- Click ? in the window to see the help menu for the description of the Maintenance Utility.
- To display the Help, the settings for enlarging and reducing the display might not be reflected in the help window depending on the type or version of browser.



Starting from Hitachi Command Suite

Procedure

1. Start Hitachi Command Suite.
2. In the **Hitachi Command Suite** main window, click the **Resources** tab, and then click **Storage Systems** from the tree view.
3. Expand the tree, and then right-click a storage system and click **Other Functions**.
4. In Hitachi Device Manager - Storage Navigator, click the **Maintenance Utility** menu, and then click **Hardware** to start the maintenance utility.

Starting from Hitachi Device Manager - Storage Navigator

Procedure

1. Launch a web browser from the console PC connected to the SVP, and then start Device Manager - Storage Navigator.
2. Enter the following URL in the address field of your browser, and then press the Enter key: `http://[IP address of SVP]/module/sn2/0/index.do`
3. In the **Storage Device List** window, click the picture of the registered storage system.
4. Log in to Device Manager - Storage Navigator.
5. On the **Maintenance Utility** menu, click **Hardware**.
6. Select the pull-down menu for the part that needs to be replaced (see the following table).

Pull-down menu	Parts to be replaced
Cache Memory replacement/installation for CTL1...	Cache memory installed on controller 1.
Cache Memory replacement/installation for CTL2...	Cache memory installed on controller 2.
Other hardware maintenance...	Component other than a controller, fan, and LAN blade.

Accessing a storage system without management software

You can use the administrator account created during the initial setup to use HDvM - SN temporarily 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.

Before you begin

- You must have an administrator login account with the Storage Administrator (initial configuration) role. For information about creating user accounts, see Creating user accounts on page 148 in this manual, and the *Hardware Reference Guide* for your system model.
- Adobe Flash Player must be configured on the client to use HDvM - SN.

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

Procedure

1. Start a web browser.
2. Enter the following URL:
   - For the VSP G200 storage system, enter:

`https://IP-address-or-host-name-of-the-SVP/dev/storage/8320004XXXXX/emergency.do` (where the model number is '8320004' and '4*XXXXX*' indicates the system serial number)

- For VSP G400, G600 and VSP F400, F600 storage systems, enter:

`https://IP-address-or-host-name-of-the-SVP/dev/storage/8340004XXXXX/emergency.do` (where the model number is '8340004' and '4*XXXXX*' indicates the system serial number)

- For VSP G800 and VSP F800 storage systems, enter:

`https://IP-address-or-host-name-of-the-SVP/dev/storage/8360004XXXXX/emergency.do` (where the model number is '8360004' and '4*XXXXX*' indicates the system serial number)

3. 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.
4. Enter a user ID and password for the account.
5. Click **Log In**.
6. If the Security Information dialog box appears, click **Yes**.
7. 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 Adobe 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.

Related tasks

- System management architecture on page 18

3

System configuration

This chapter provides instructions to manage the system configuration.

- System administration tasks at a glance
- System administration using Hitachi Storage Advisor
- System administration using Device Manager - Storage Navigator
- System administration using the maintenance utility
- System administration using NAS Manager
- Miscellaneous system administration considerations

System administration tasks at a glance

The following table summarizes key system administration tasks. The tool used to perform these tasks depends on whether the storage system contains NAS modules.

Table 1 System administration tasks at a glance

Task	Block-only storage systems (no NAS modules installed)	Block and file storage systems (NAS modules installed)
• Set IPv4 and IPv6 network settings and set HTTP blocking	Maintenance utility See Changing network settings on page 117	IP addresses cannot be added, deleted, or modified in the NAS Manager. To change these addresses, use the maintenance utility.
• Set system clock (date and time)	Maintenance utility See Changing the date and time on page 116	NAS Manager See Changing the system date and time of the NAS modules on page 121
• Configure audit log settings	Maintenance utility See Audit log settings on page 240	NAS Manager See the *File Services Administration Guide* (MK-92HNAS006) and the *Server and Cluster Administration Guide* (MK-92HNAS010)
• Configure alert notifications	Maintenance utility See Alert notifications on page 217	NAS Manager See the *Server and Cluster Administration Guide* (MK-92HNAS010)
• Changing link aggregation	N/A	NAS Manager See the *Network Administration Guide* (MK-92HNAS008)
• Change administrator password • Edit the login message • Select the SSL cipher suite • Update certificate files • Force the system lock to release	Maintenance utility See System configuration on page 61	NAS Manager See the *Network Administration Guide* (MK-92HNAS008)
• User administration - add, manage, and delete storage system users • Manage user groups	Device Manager - Storage Navigator See User administration for Device Manager - Storage Navigator on page 146	NAS Manager See User Administration for NAS Manager on page 176
• Registration	Device Manager - Storage Navigator to register the	NAS Manager to register the service. See the *Server and Cluster Administration Guide* (MK-92HNAS010)

Task	Block-only storage systems (no NAS modules installed)	Block and file storage systems (NAS modules installed)
	service processor host name. See Registering the primary SVP host name on page 120	
• Change storage system information	Device Manager - Storage Navigator See Setting storage system information on page 113	N/A
• Manage SSL certificates: create keypairs, obtain, update, and return certificates, verify and release passphrases	Device Manager - Storage Navigator See Managing HCS certificates on page 204	N/A
• Manage HCS certificates	Device Manager - Storage Navigator See Managing HCS certificates on page 204	N/A
• Manage HDvM - SN configuration files	Device Manager - Storage Navigator See Backing up HDvM - SN configuration files on page 114	NAS Manager See the *Server and Cluster Administration Guide* (MK-92HNAS010)
• Manage authorization and authentication servers	Device Manager - Storage Navigator See Using an authentication server and authorization server on page 162	N/A
• Create LDAP, RADIUS, and Kerberos configuration files	Device Manager - Storage Navigator See Authentication server protocols on page 163	NAS Manager See the *Server and Cluster Administration Guide* (MK-92HNAS010)
• Installing licenses • Enabling and disabling licenses • Removing licenses	Maintenance utility See License keys on page 229	NAS Manager See License keys on page 229

System administration using Hitachi Storage Advisor

Configure block storage

Use Storage Advisor to configure the block storage.

Enabling or disabling port security

Before a host storage domain (HSD) can be created on a port, port security must be enabled. By default, security is disabled on supported storage systems. If port security is disabled Storage Advisor will not select the port for HSD creation. If you select a port that has security disabled, you are limited to the default host group. If the user manually selects the port with security disabled, the host group will be created.

Procedure

1. On the Storage Advisor dashboard, click **Storage Systems** to see the inventory of storage systems and capacity information.
2. Click a storage system to see its configuration of pools, ports, volumes, and parity groups.
3. Click **Ports** to see the configured storage ports for the storage system.
4. Select one or more ports and click **Enable/Disable Security** to open the **Update Storage Port** page.
5. For a VSP G1000 storage system, you can update port attributes by selecting one of the following:
   - **Target**: Fibre target port
   - **Initiator**: MCU initiator port
   - **RCU Target**: RCU target port
   - **External**: External initiator port
6. Click **Enable Security** or **Disable Security** and then click **OK**.
   A job is started to update the port security.

Modfying port attributes in Storage Navigator

You can open the Ports inventory page in Hitachi Storage Navigator by clicking the icon () to launch Storage Navigator and view the Ports Ports/ Host Groups/iSCSI tab. From there, you can view and modify port attributes.

For more information, refer to the *System Administrator Guide*

Note: Any changes you make in Storage Navigator may not be reflected in Storage Advisor for a few minutes.

Adding a fabric switch

You can add a fabric switch after onboarding a storage system. Add, update, and delete fabric switches in the Storage Advisor interface.

After a fabric switch is added, you can choose to auto-create zones during volume provisioning. A fabric switch is required for any operations that use

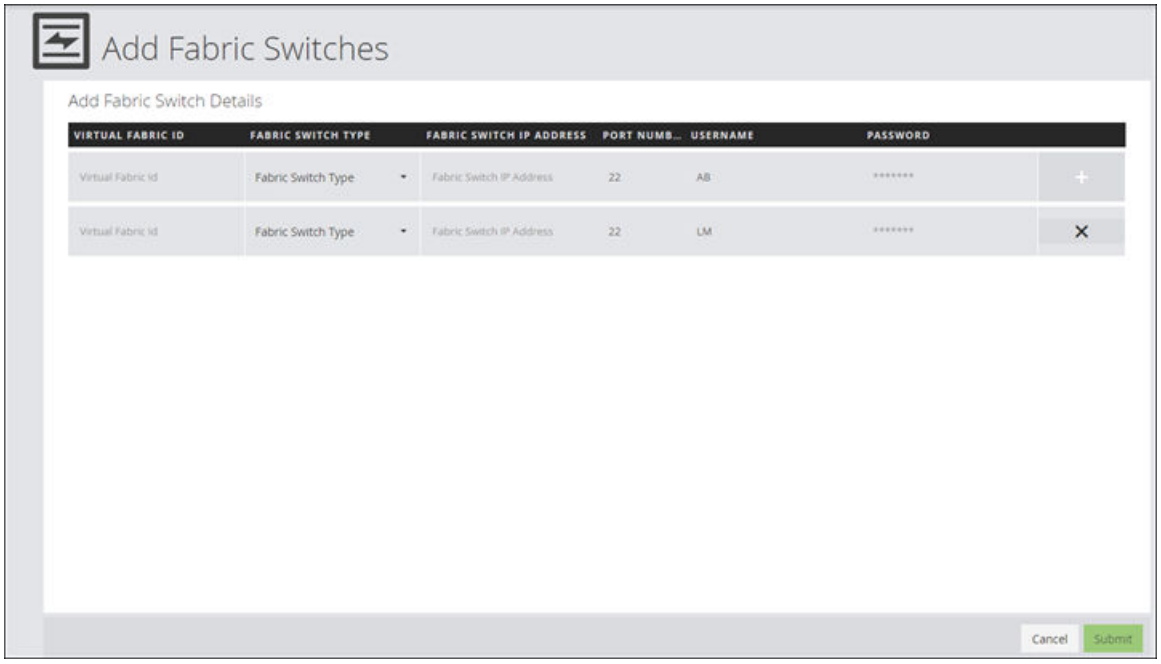
auto-select, such as host group creation and auto-selection of ports while attaching volumes to servers.

Before you begin

- Verify that servers and ports are connected according to the manufacturer's instructions.
- Verify that there is an active zone set with at least one dummy zone available.
- The Storage Advisor server is connected to the same IP network and has access to SNMP broadcast of Fibre Channel switches.
- Verify the required information about the fabric switch: Virtual Fabric ID (required only for Cisco switches), Fabric Switch Type, Fabric Switch IP Address, Port Number, Username, and Password.
- Verify that you have the Admin role for the fabric switch.

Procedure

1. On the Storage Advisor dashboard, select **Fabric Switches** to open the **Fabric Switches** page.
2. Click the plus sign (**+**) to open the **Add Fabric Switches** page.



3. Enter the following information from the configuration of the switch you are adding:
   - **Virtual Fabric ID**: For Cisco switches, the VSAN ID. Not applicable to Brocade switches.
   - **Fabric Switch Type**: Select **Brocade** or **Cisco**.
   - **Fabric Switch IP Address**
     To add or update a core switch, use the Management IP address of the switch or the Active CP IP address.

- **Port Number**
- **Username**
- **Password**

4. Click **Submit**.

Result

A job is created to add the fabric switch.

Supported fabric switch models

Storage Advisor supports a variety of Brocade® and Cisco® fabric switches.

System requirements for Brocade switches

Model	Fiber OS version	Type
300	7.0 7.1 7.2	71
5300	7.0 7.1 7.2	64
6505	7.0 7.1 7.2	118
6510	7.0 7.1 7.2	109
6520	7.0 7.1 7.2	133
7800	7.0 7.1 7.2	83
DCX 8510-4	7.0 7.1 7.2	121
DCX 8510-8 with firmware v6.4	7.0 7.1 7.2	120

System requirements for Cisco switches

Storage Advisor supports the Cisco MDS 9000 Series of switches.

Cisco MDS NX-OS Release 6.2(9) or later is required.

Creating parity groups

Parity groups are the basic units of storage capacity. Creating parity groups converts the raw disk capacity in your storage system into usable capacity.

Storage Advisor parity group concepts

Storage Advisor provides a simple one-click method of parity group creation that is based on best practices applicable to the disks in the storage system.

An advanced method of parity group creation is also available. You can choose to use the advanced method if there is not a need to rely on best practices.

Note: Parity groups on VSP G1000 storage systems cannot be created in Storage Advisor. They are created by an authorized service representative. They can be initialized in Storage Advisor. Encryption can be enabled in Device Manager - Storage Navigator.

Creating parity groups in Storage Advisor also creates LDEVs that can be consumed for pool creation.

Encryption can be enabled during parity group creation if prerequisites are met, including a storage system with an Encryption Disk Board.

Normal practice is to use all available disk capacity when creating parity groups to ensure that all of the storage system capacity is usable. There can be exceptions to this practice; for example:

- If the entire capacity of the storage system is not needed.
- If there is a need to create fewer parity groups in order to reserve more disks as spares.

Viewing parity groups

Access the Parity Groups page by clicking Storage Systems on the dashboard and then clicking a storage system tile. Click the Parity Groups tile.

A summary of parity groups includes disk type, number of parity groups, capacity, and available spares, all sorted by disk type.

- You can click Manage Spare Disks to open the **Disk Management** page and set free disks as spare disks, or spares as free disks.

  Note: Not available for VSP G1000.

- Click any parity group tile to view its details.
- Click the plus sign (+) to open the **Create Parity Groups** page.

When you open the **Create Parity Groups** page, the basic method is selected by default. Encryption can be enabled using either method.

- Basic option: Creating a parity group using the basic option requires no input, but you can change the RAID type or the number of parity groups. Storage Advisor applies recommended best practices for creating these parity groups.
- Advanced option: The advanced option allows the user to fully configure the RAID layout of the parity group by selecting the specific disks to assign for parity group creation.

Enabling Parity Group encryption in Hitachi Storage Navigator

You can open the Parity Groups inventory page in Hitachi Storage Navigator by clicking the icon () to launch Storage Navigator in order to enable parity group encryption.

For more information, refer to the *System Administrator Guide*

Note: Any changes you make in Storage Navigator may not be reflected in Storage Advisor for a few minutes.

Creating parity groups, basic method

The following procedure describes the basic option for creating a parity group and enabling encryption.

Note: Parity group creation on VSP G1000 storage systems is performed outside Storage Advisor by an authorized service representative. Encryption can be enabled (if prerequisites are met) in Device Manager - Storage Navigator.

Before you begin

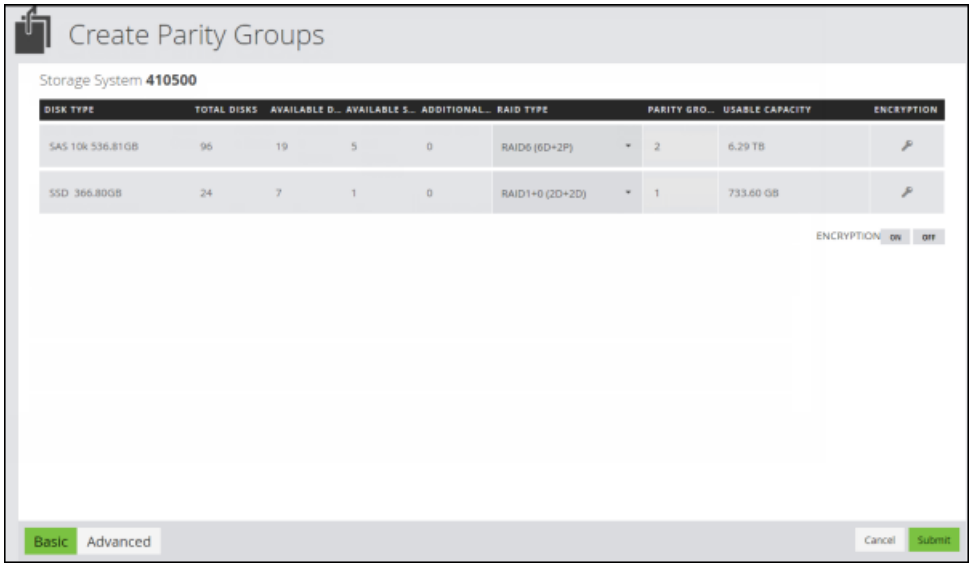
- Register the storage system.
- Identify the target storage system name.
- Identify the total capacity that you expect to use. Plan to use all of the available disks in the system when you create parity groups.

Procedure

1. On the Storage Advisor dashboard, select **Storage Systems** in the resource side panel to see the inventory of registered storage systems.
2. Click a storage system to create and configure the parity groups for it.
3. Click **Parity Groups** to see the inventory of all parity groups in the storage system.
4. Click the plus sign (**+**). In the **Create Parity Groups** window, review the list of unused disk types in the storage system. This information is

grouped by disk type, disk speed, and disk capacity, and includes the following details:

- Number of available disks.
- Available spares detected for each disk type, disk speed, and capacity.
- Number of new or additional spares to reserve. This calculation is based on the total spares needed based on recommended best practices, and the number of existing spares in the system.
- The recommended RAID configuration for the disk type.
- The number of parity groups that can be created.
- The total usable capacity that is available based on the number of parity groups and the RAID configuration.



5. Decide if the recommended RAID configuration for each disk type is acceptable. Choose one of the following options:
   - Accept the recommended RAID configuration, which uses the full capacity of the installed drives.
   - Change the recommended RAID configuration or create fewer parity groups. Storage Advisor shows the number of parity groups that can be created for the new RAID configuration and the corresponding usable capacity.
6. (Optional) Click Encryption **ON** if you want to use encryption.

   Prerequisites for enabling encryption:
   - The storage system must have an Encryption Disk Board.
   - Encryption License Key must be installed.
   - The Key Management Server must be configured on the SVP.

   Note: Encryption cannot be disabled in Storage Advisor.
7. Click **Submit**.

Result

A job is started to create the parity group for the storage system. This job includes the following tasks:

- Identifies the appropriate number and position for the spare disk.
- Assigns a spare disk.
- Creates the required number of parity groups for the requested RAID layout.
- Creates and quick formats the necessary volumes on the parity group so that it is ready for pool creation.
- The job may create sub-jobs when multiple parity groups are being created. Each sub-job will show the status of the parity groups being created.

Next steps

- Check the status of the parity group creation job by clicking Jobs.



Note: Parity group creation may take a long time.

Creating parity groups or hot spares, advanced method

The advanced option enables users to configure parity groups that are not based on the provided best practices.

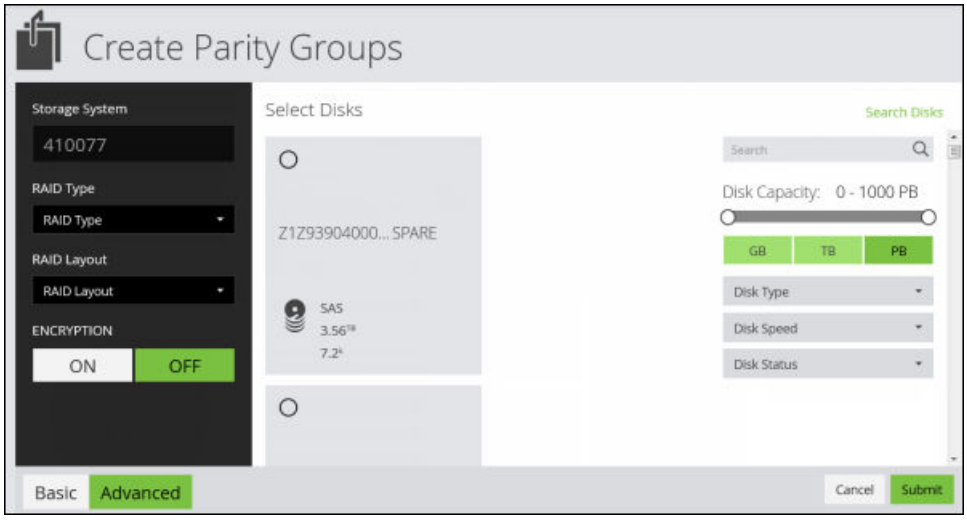
The advanced option allows you to fully configure the RAID layout of the parity group by selecting the specific disks and hot spares to assign for parity group creation.



Note: Parity groups on VSP G1000 storage systems cannot be created in Storage Advisor. They are created by an authorized service representative. They can be initialized in Storage Advisor. Encryption can be enabled in Device Manager - Storage Navigator.

Procedure

1. On the dashboard, click **Storage Systems** and click a storage system tile.
2. Click **Parity Groups** to open the **Parity Groups** page and click the plus sign to open the **Create Parity Groups** page.
3. Click **Advanced**.



4. Select a **RAID Type** and a **RAID Layout**.

RAID Type	RAID Layout
RAID5	3D+1P, 4D+1P, 6D+1P, 7D+1P
RAID6	6D+2P, 12D+2P, 14D+2P
RAID1+0	2D+2D

5. (Optional) Click Encryption **ON** if you want to use encryption.
   Prerequisites for enabling encryption:
   - The storage system must have an Encryption Disk Board.
   - Encryption License Key must be installed.
   - The Key Management Server must be configured on the SVP.

   Note: Encryption cannot be disabled in Storage Advisor.

6. Choose available disks. Select enough disks to match the RAID Layout.
7. Click **Submit**.

Result

A job is started to create the parity group for the storage system.

Next steps

- Check the status of the job by clicking Jobs.

  Note: Parity group creation may take time.

- Create a pool.

Managing free and spare disks

You can set free disks to spare and spare to free.

Note: Disk management is not available for VSP G1000 storage systems.

If you choose to use the basic method to create parity groups, Storage Advisor will automatically review the available spare disks and allocate more spare disks if needed.

If you choose to create parity groups using the advanced method, you should review the number of spare disks in the parity groups inventory summary. If you want to assign more or fewer spare disks, use disk management.

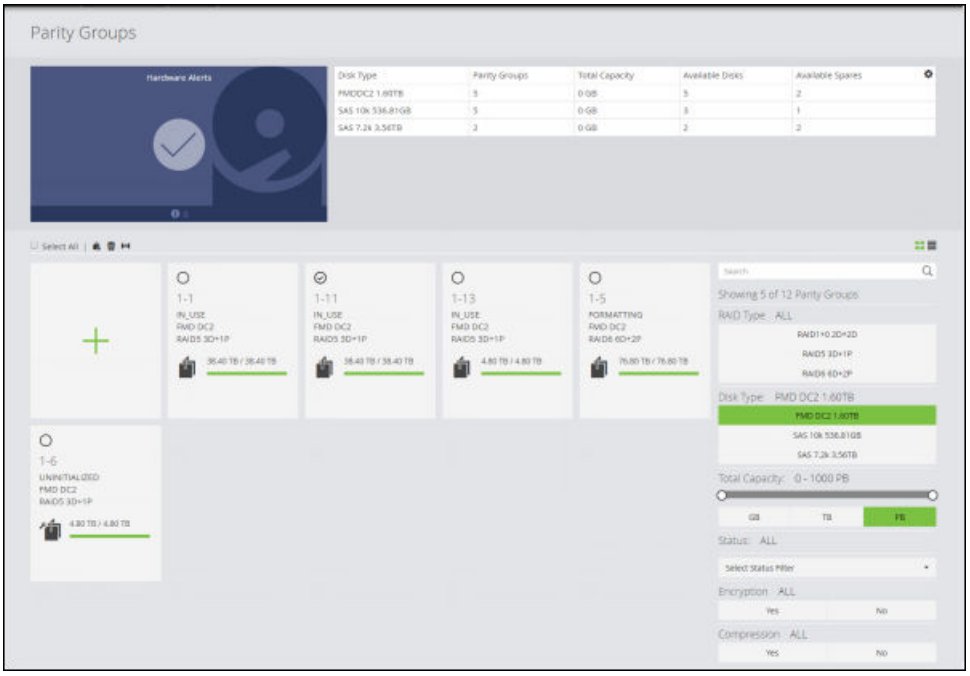
Procedure

1. On the dashboard, click **Storage Systems**.
2. Click a storage system tile and click **Parity Groups**.
3. Click **Manage Spare Disk** to open the **Disk Management** page and view disks not being used in any parity group.
4. Click **Disks to Set to Free** or **Disks to Set to Spare** and select one or more disks. Selecting Disks to Set to Spare will reserve the disks as a spare disks and they cannot be used for parity group creation. Selecting Disks to Set to Free will unallocate the spare disks and return then to the pool of available disks.
5. Click **Submit**.

Parity groups inventory

After parity groups are created, they are displayed for each storage system.

To view parity groups for a storage system, click Storage Systems on the dashboard and click a storage system tile to view the associated parity groups, pools, volumes, and ports. Click Parity Groups to open the Parity Groups page.



You can perform the following actions on this page:

- If there are hardware alerts related to the parity groups, you can click the Hardware Alerts tile to view details for different types of components on the Monitoring page for the storage system.
- To assign free and spare disks, click Manage Spare Disks to open the Disk Management page.

Note: Disk management is not available for VSP G1000 storage systems.

- Select one or more parity groups and do one of the following:
  - To initialize parity groups, click Initialize Parity Groups.
    You can create and initialize pool volumes on a parity group if pool volumes have not been created. You can also format any pool volumes that are in blocked state. You can initialize parity groups in the following conditions:
  - – When the parity group either does not have any pool volumes or at least one of the pool volumes is in Blocked state. In this case, you will notice that the parity group status is Uninitialized.
    – When the pool volumes on the parity group do not account for the entire parity group capacity and there are unused partitions on the parity group. In this case you will notice that the parity group status is Available but the available capacity is much less than the total capacity. This is supported only when the parity group status is Available or Uninitialized.

- To delete the parity group, click Delete. When you delete a parity group, it is removed from the storage system and the disks used to create the parity group are no longer in use. You can delete the parity group if you want to reconfigure the storage system with some other RAID configuration or simply decommission the array.

  Note: The following parity groups cannot be deleted:
  - Parity groups on VSP G1000, VSP G1500, or VSP F1500 storage systems
  - Parity groups that contain NAS boot volumes.

- To enable compression on parity groups, click Enable Compression on Parity Groups. Compression can be enabled for parity groups on FMD DC2 disks in Available state.
  After compression is enabled, the status of the parity group is AVAILABLE_PHYSICAL.

  Note: Parity groups that contain NAS boot volumes cannot be compressed.

- Click the plus sign (+) to create a new parity group.

  Note: Parity groups on a VSP G1000 storage system are created outside Storage Advisor by an authorized service representative.

- Use the filters to view the status of parity groups. Click a filter to apply it and click it again to remove it.
  - AVAILABLE: Parity group is not being used for any storage pools. It is available for pool creation.
  - AVAILABLE_PHYSICAL: Parity group is not being used for any storage pools. Compression is enabled on the parity group and physical capacity of the parity group is available for pool creation. Not applicable to parity groups that are not enabled for compression.
  - FORMATTED: At least one of the pool volumes in the parity group is being formatted. The full format takes longer than a quick format because the service processor fully scans the hard drive.
  - QUICK_FORMATTING: At least one of the pool volumes in the parity group is being formatted using the quick format method. To make the formatting process quick, the drive is not fully checked, the files are still there, and the volume could be re-built to gain access to the files again.
  - IN_USE: Parity group is being used by a storage pool.
  - UNINITIALIZED: The parity group either has no volumes or at least one of the pool volumes is in Blocked status, or one or more partitions is uninitialized and has a size greater than 16,787,456 blocks.

- UNSUPPORTED_ATTACHED: At least one of the pool volumes has a path to a storage port.
- UNSUPPORTED_INACCESSIBLE_RESOURCE_GROUP: Parity group and at least one of its pool volumes are in different resource groups and user does not have access to one of the resource groups.

Note: If the storage system includes NAS modules, a parity group is reserved for NAS firmware. Physical volumes are created on the parity group and provisioned to NAS modules outside of Storage Advisor by an authorized service provider. The parity group displays in the parity group inventory with the status UNSUPPORTED_ATTACHED.

External parity groups inventory

External parity groups are parity groups in a storage system that is connected to a storage system that has been onboarded in Storage Advisor.

You can display a list of external parity groups in a storage system that has been registered with Device Manager - Storage Navigator.

You can access the External Parity Groups page by clicking the External Parity Groups tile on the detail page for a storage system. If the storage system has no external parity groups, the tile does not display.

External parity groups are not available for deletion, initialization, or compression.

If external parity groups have been used to create a pool (outsideStorage Advisor), you can use their capacity to create volumes in Storage Advisor.

Enabling accelerated compression in Storage Advisor

Accelerated compression can be enabled for parity groups on FMD DC2 drives that are part of VSP Gx00 models, VSP Fx00 models and VSP G1000 storage systems. It enable users to realize more virtual capacity than the actual usable capacity.

Note: Accelerated compression is not compatible with encryption. If a parity group is encrypted when created, the data cannot be compressed.

Storage Advisor only uses the physical capacity of the FMD DC2 parity groups for which write is assured.

Accelerated compression is enabled in the Advanced tab of the Create Parity Groups page.

When you create pools, you can select capacity from compression-enabled parity groups by selecting the AVAILABLE_PHYSICAL status.

After creating a pool with capacity from a parity group that is enabled for accelerated compression, you can view the following in the detail page for the pool:

- **Expansion Rate:** The ratio of the total capacity of FMD DC2 pool volumes with respect to the total capacity of FMD DC2 pool volumes assured for writing.
- **Compression rate:** The ratio of data size compression.
- **Savings %:** Displays the percentage of the capacity reduced by data compression with respect to the used capacity before the data compression. This will not display a value until data is compressed.

If the savings percentage for a pool is not high enough, you can provision additional pool volumes to the pool from the parity groups using FMD DC2 drives.

Accelerated compression is enabled in the Parity Groups inventory page.

Creating a pool

Use the basic option to take advantage of tiers that are based on best practices.

If you want more flexibility and do not need to take advantage of best practices, you can use the advanced option to select specific parity groups.

You cannot create pools on external parity groups. They must be created outside Storage Advisor.

Note: The following types of pools are identical:

Thin = HDP (Dynamic Provisioning), which is functionality that allocates virtual volumes to a host and uses the physical capacity that is necessary according to the data write request.

Tiered = HDT (Dynamic Tiering), which is used with Dynamic Provisioning and places data in a hardware tier according to the I/O load. For example, a data area that has a high I/O load is placed in a high-speed hardware tier, and a data area that has a low I/O load is placed in a low-speed hardware tier.

Snap = HTI (Thin Image), which stores snapshot data in pools. A pool consists of multiple pool-VOLs. The pool-VOLs contain the snapshot data. A pool can contain up to 1,024 pool-VOLs.

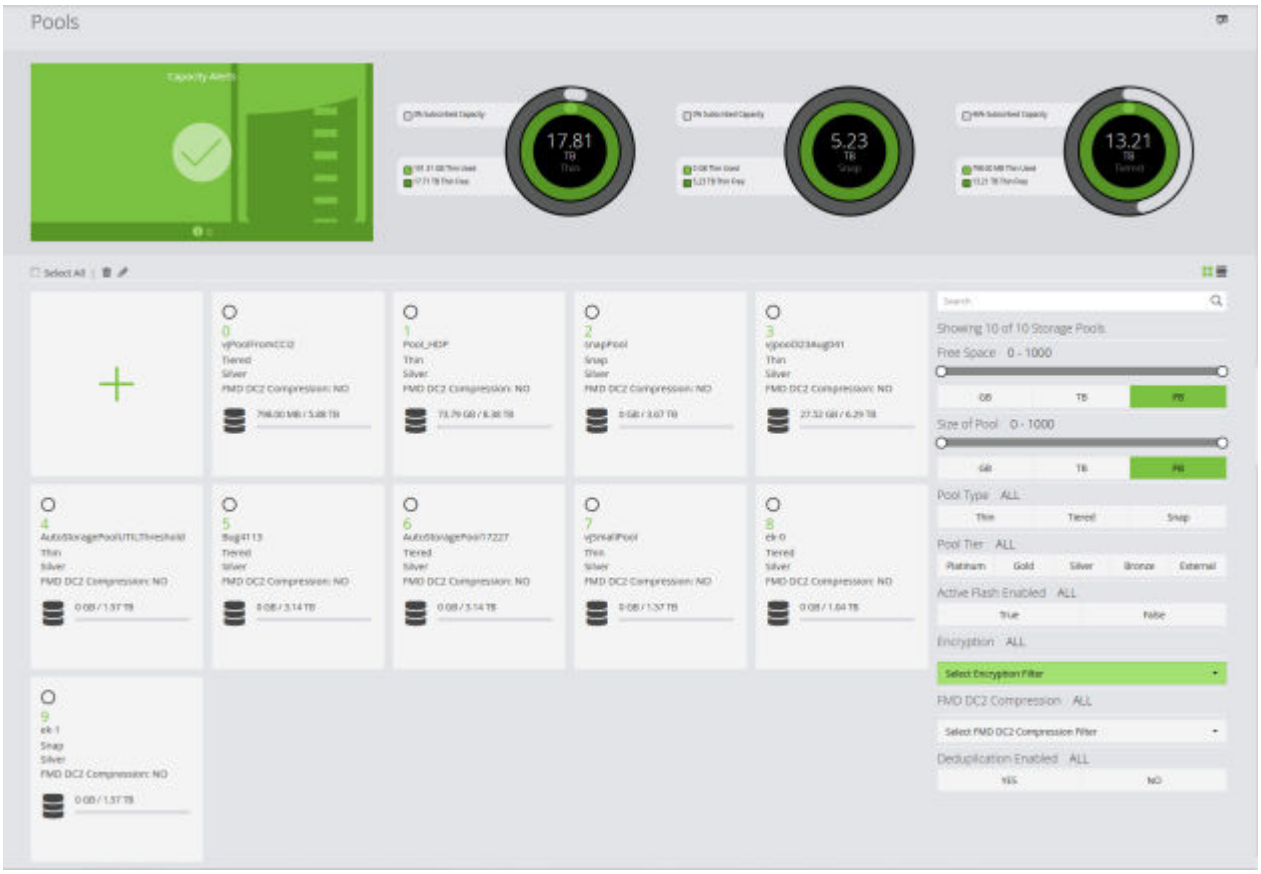
Pools inventory

Access the Pools page to add, update, and delete pools.

From the dashboard, click Storage Systems and then click a storage system tile to view parity groups, pools, volumes, and ports.

Click Pools to view the inventory of pools.

Note: If there are external pools (on external storage), they display in Pools inventory, but they cannot be added, updated, or deleted.



View pool details in either a tile view or a list view. Capacity utilization is represented by a color bar:

- Green Below 70%.
- Orange From 70% to 80%.
- Red Over 80%.

A key in a tile or row indicates that the pool is encrypted.

FMD DC2 Compression status indicates whether a pool is using a parity group that is enabled for accelerated compression.

The following actions are available on this page:

- Click Open the Pools page in Storage Navigator to open the Pools page of Storage Navigator in a separate browser window.
- Select a pool and click Edit to update it in the Update Storage Pool page.
- Select one or more pools and click Delete to delete the pools. Deleted pools are de-provisioned and removed from the storage system.
- Click the plus sign (+) to add a pool in the Create Pool page.

Opening the Pools inventory page in Hitachi Storage Navigator

You can open the Pools inventory page in Hitachi Storage Navigator by clicking the icon () to launch Storage Navigator and:

- Shrink or restore a HDP/HDT pool
- View the Tier properties of the HDT Pool
- Update the Monitoring Mode of the HDT pool (Manual Tier management)
- Start or stop the monitoring of the HDT pool (Manual Tier management)
- Start or stop tier relocation on the HDT pool (Manual Tier management)

For more information, refer to the *System Administrator Guide*

Note: Any changes you make in Storage Navigator may not be reflected in Storage Advisor for a few minutes.

Creating a pool, basic method

Use the basic method of pool creation to create pools based on best practices.

Before you begin

Create and configure parity groups on the storage system.

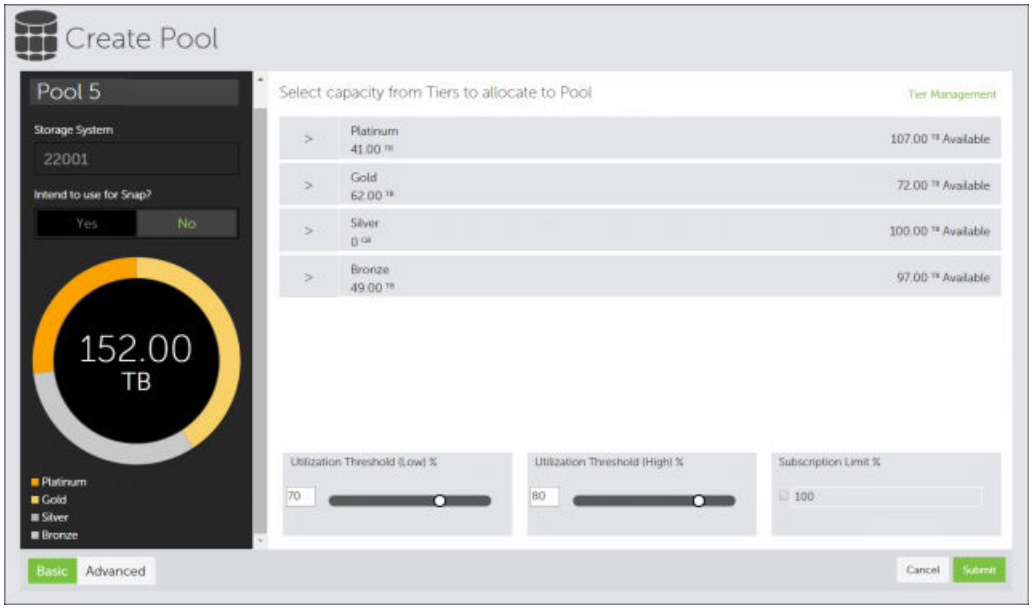
You need a minimum of four parity groups of the Bronze, Silver, or Gold tiers, or one parity group of the Platinum tier to create a pool using the basic method. Otherwise, you can use the advanced method of pool creation.

License requirements:

- For a Tiered pool: Dynamic Tiering
- For a Thin pool: Dynamic Provisioning
- For a Snap pool: Thin Image
- For active flash: active flash

Procedure

1. On the Storage Advisor dashboard, click **Storage Systems** to see the inventory of registered storage systems.
2. Click a storage system to create a pool for it.
3. Click **Pools**.
4. Click the plus sign (**+**) to open the **Create Pool** page.
   By default, the **Basic** option is selected.



5. Enter a **Pool Label**.

   Pool labels can contain only alphanumeric characters, hyphens, and underscores. Initial hyphens are not allowed.

6. In the **Select capacity from Tiers to Allocate to Pool** pane, you can choose storage from 1, 2, or a maximum of 3 tiers (**Platinum**, **Gold**, **Silver**, or **Bronze**).
   - If you select only one tier, you can use the **Intend to use for Snap?** toggle to decide whether to use Snap pools.
     - Click **Yes** to create Snap pools.

       Note: Use this option if you want to use data protection to create snapshots. You can also create a pool for snapshots later by returning to the Create Pool page.

     - Click **No** to create Thin pools.
   - If you select 2 or 3 tiers, the system creates Tiered pools.

Table 2 Tier Definitions

Pool Tier	Description
Platinum	SSD, FMD, and FMD DC2
Gold	SAS 15 k
Silver	SAS 10 k
Bronze	SAS 7.2 k

7. Click a selected tier to view the available storage capacity and select a capacity size.
8. Click **Tier Management** to see the disk type, capacity, and speed of each pool category.

9. Review the high and low pool utilization thresholds, for watermarks or warnings, and the subscription limit. The thresholds will serve as the Warning and Critical thresholds for monitoring capacity. Adjust the thresholds if needed. Select the **Subscription Limit %** checkbox to set the limit to Unlimited.

   Note: Subscription Limit % is not applicable to Snap pools.

10. Click **Submit.**

Result

A job is started to allocate the storage capacity and create the pool.

Next steps

- Check the status of the pool creation job by clicking Jobs.
- Create a volume.

How Storage Advisor calculates pool sizes for the basic method of pool creation

Storage Advisor incorporates best practices to calculate the best pool sizes based on the media available in the storage system. When the basic pool creation option is used, pool size is determined as follows:

- Storage Advisor identifies all the parity groups of the same disk type, disk capacity, disk speed, RAID type and layout and determines the available capacity of their usable LDEVs. Only parity groups in the Available and Quick Formatting states are eligible for pool creating using the basic method.
- Storage Advisor then uses combinations of these parity groups where four or more parity groups of the Bronze, Silver, or Gold tiers can be added together, or there is a parity group of the Platinum tier, to compute various possible pool sizes that can be created for the combination of disk type, disk capacity, disk speed, RAID type and layout.

  Note: If your parity groups do not meet these requirements, you can only use the advanced method of pool creation.

- Based on the Storage System model, Storage Advisor determines the maximum pool size.
- Storage Advisor then displays the pools in increasing order of pool size.

Creating a pool, advanced method

You can use the advanced method of pool creation to select parity groups filtered by disk type, speed, layout, and RAID level. This method does not employ best practices.

Note: Mixing different disk types in a Thin pool is not recommended. If you choose to create such a pool, Storage Advisor identifies the tier in this pool as "mixed".

Before you begin

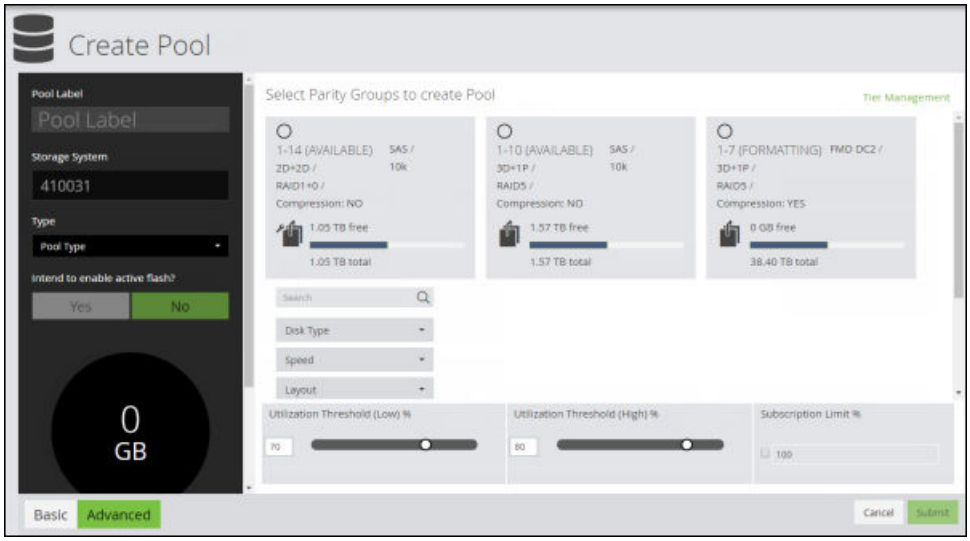
Create and configure parity groups on the storage system.

License requirements:

- For a Tiered pool: Dynamic Tiering
- For a Thin pool: Dynamic Provisioning
- For a Snap pool: Thin image
- For active flash: active flash

Procedure

1. On the Storage Advisor dashboard, click **Storage Systems** to see the inventory of registered storage systems.
2. Click a storage system to create a pool for it.
3. Click **Pools**.
4. Click the plus sign (**+**) to open the **Create Pool** page and click **Advanced**.



5. Enter a **Pool Label**.

   Pool labels can contain only alphanumeric characters, hyphens, and underscores. Initial hyphens are not allowed.
6. Click the **Type** list and choose one of the following; **Thin**, **Tiered**, or **Snap**.
7. Choose whether to enable active flash. Active flash enablement requires capacity from the Platinum tier.
8. Click **Tier Management** to see the definitions of disk type, capacity, and speed of each pool category.

9. Select one or more parity groups to use to create the pool. You can scroll through the parity groups to use search and filter functions.
   - For a Snap pool, select one or more parity groups with identical disk types.
   - For a Thin pool, select one or more parity groups with identical disk types.
   - For a Tiered pool, select one or more parity groups with two or three disk types.

   Storage Advisor shows the total size of the pool using the selected parity groups.
10. Set the utilization thresholds, or use the default threshold settings. The subscription limit can be set above 100%. Select the **Subscription Limit %** checkbox to set the limit to Unlimited.

    The thresholds are used as the Warning and Critical thresholds for Capacity Monitoring.
11. Click **Submit.**

Result

A job is started to allocate the storage capacity and create the pool.

Next steps

- Check the status of the pool-creation job by clicking Jobs.
- Create volumes.

Pool details

To access pool details, click Storage Systems. Then click a storage system to view all resources. Click Pools and then click a pool tile.



Note: A External pool cannot be edited or deleted.

On the pool details page, you can do the following:

- View the attributes of the pool.
- View a graph of utilization and thresholds.
- If the pool is based on a parity group using accelerate compression (FMD DC2 Compression), you can also view compression details, including expansion ratio and compression ratio.
- View volumes carved from the pool and perform operations on them. Operations available include deletion, updating, attaching and detaching to and from servers, protecting, unprotecting, and restoring. Click a volume in tile or list view to open the detail page for the volume.

  The Provisioning Status can be any of the following:
  - Attached: the volume is attached to a server.
  - Unattached: the volume is not attached to a server.

    - Unmanaged: the volume has only a LUN path associated. For example, a volume may be attached to a server that is not known to Storage Advisor.
- If the volume uses compression or deduplication and compression, you can view the compression ratio and deduplication ratio.
- Delete the pool.
- Edit the pool configuration by clicking the pencil icon to open the **Update Storage Pool** page.
  Once a pool is created, you can edit the pool label or expand the pool. Basic and advanced options, similar to those for pool creation, are available for pool expansion. The basic option includes choices for a new/expanded pool size based on the current set of parity groups in the pool. You can choose to expand an existing tier in the pool or add a new tier to the pool. If you add a tier to a thin pool, it will be expanded and converted into a tiered pool. Using the advanced option enables you to add more parity groups to the pool and increase capacity.

  Note: To expand a Thin pool, you must add a parity group of the same RAID layout, the same disk type, the same RAID level, and the same disk speed.

  Click Submit to update the window and start a job that will update the pool.

Create and attach volumes to servers

You can create volumes and attach them to servers and then apply data protection in a single workflow by first selecting a server.

Creating volumes to attach to servers

Start the create-and-attach workflow by selecting a server and creating volumes.

When you create volumes in Storage Advisor you can:

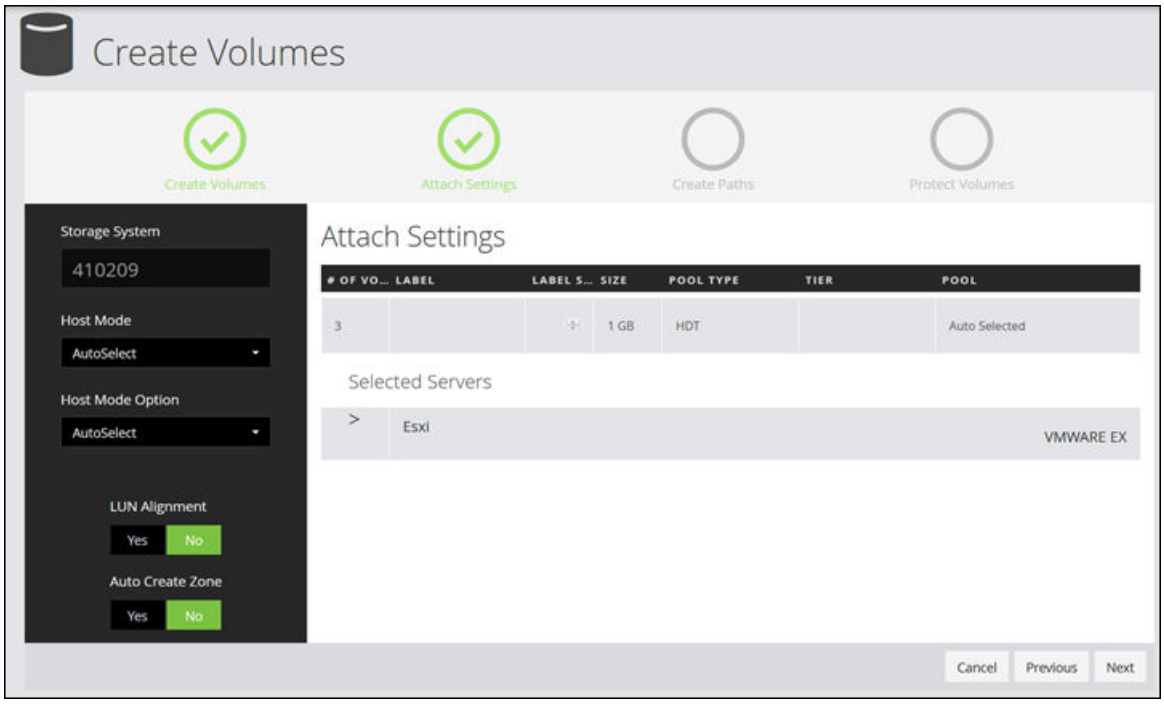
- Create multiple volumes of the same size or different sizes at the same time.
- Select the specific pool for volume creation or let Storage Advisor automatically select the best pool based on utilization.
- Specify a common label and starting label suffix for identical volumes that are the same size and have the same pool requirement.

Before you begin

- Create parity groups.
- Create pools.
- Add servers.

Procedure

1. On the Storage Advisor dashboard, click **Servers** to see the inventory of servers.
2. Do one of the following to open the **Create Volumes** page:
   - Select a server, click **Attach Volumes**, and select **Create, Attach, and Protect Volumes**.
   - Click a server tile to open the **Server <*ID*>** details page. Click the cylinder icon ( ) in the upper right area and select **Create and Attach Volumes**.



3. Configure volumes for the specified storage system.

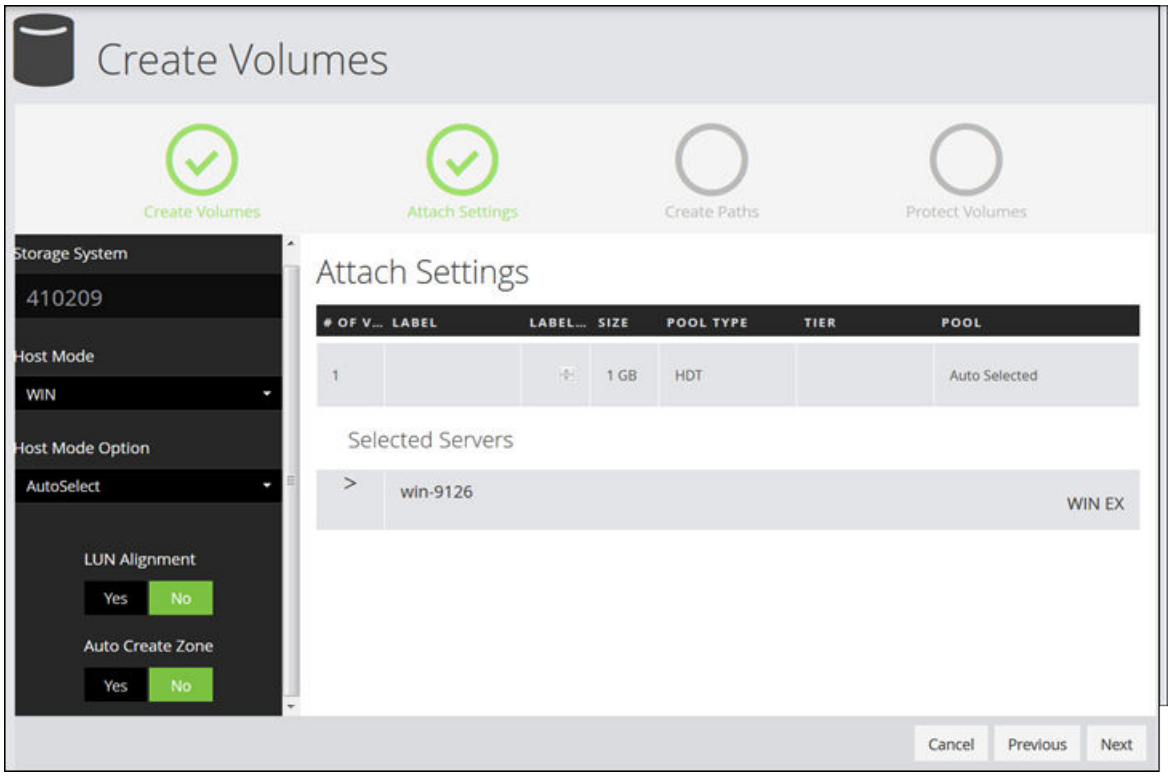
   You can switch to another storage system by using the drop-down Storage System list.

   a. Select the number of volumes.
   b. Enter the volume label and select a suffix for it.
   c. Select the size.
   d. Select the volume unit: **GB**, **TB**, or **PB**.
   e. Select the pool type: **Thin** or **Tiered**.
   f. For a Thin pool, select the tier: **Platinum**, **Gold**, **Silver**, or **Bronze**.

      If the storage system has available capacity from external storage, you can also select the **External** tier.
   g. (Optional) Select the pool from the list of available pools. The default selection is **Auto Selected**, which means that Storage Advisor selects the best pool for provisioning the volume based on utilization and tier requirements.
4. Click the plus sign if you want to create more volumes in another row.
5. Click **Next** to be directed to attach volumes to the selected servers.

Attaching newly-created volumes to servers

Storage Advisor provides options as part of the attachment of the new volumes to a single server or multiple servers.



Procedure

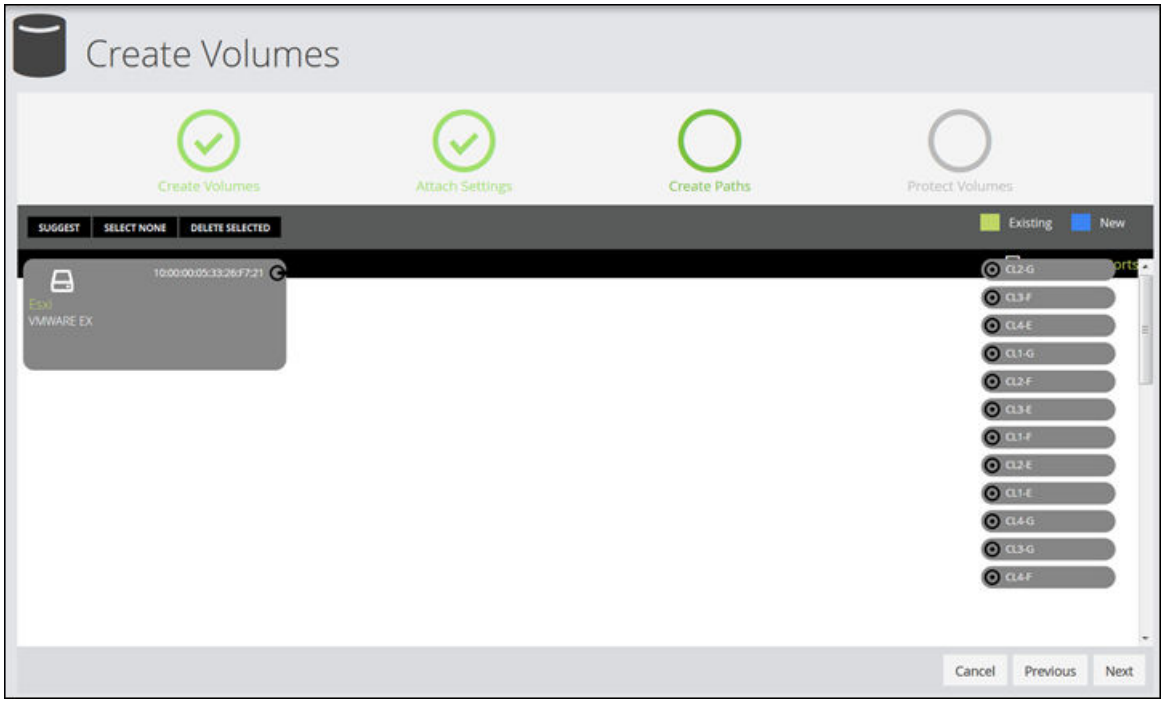
1. The **Host Mode** is set by default to the server operating system. You can make a selection if needed.

   The server OS Type is provided when the server is added to Storage Advisor.
2. By default, the **Host Mode Option** will depend on the **Host Mode** selection.

   Default values are set only for **VMWARE EX** and **WIN EX** host modes. The default for all other Host Modes is none.

   Storage Advisor identifies all host groups containing any of the server WWNs. If all of those host groups have the same host mode and host mode options, those settings are prepopulated with the same settings in the host groups.
3. Select the **LUN Alignment**.

   By default, Storage Advisor uses the LUN number that is common to the servers. If attachment is to only one server, this setting has no effect.
4. The **Auto Create Zone** is set to **No** by default. You can set it to **Yes** to automatically create zones.
5. Click **Next** to view options for creating and editing LUN paths.



6. In the **Create Paths** panel, you can view servers and their WWNs, along with ports on the storage system. The following options are available for managing LUN paths:
   - Existing paths are populated as follows: all existing host groups with one or more server WWN and the exact same host mode and host mode options selected on the Attach Settings panel are populated as paths.

     To prevent the volume from being added to an existing path, click the path to highlight it and click **Delete Selected**.
   - Click **Suggest** to populate automatically selected paths. By default, the least-used ports are selected.
   - To manually create a path, click a WWN and a port to connect them with a blue connector line. Click the connector again and then click **Delete Selected** to delete the connection.
7. When you are satisfied with the paths, click **Next** to view options for protecting volumes.

Managing storage systems

Access the storage system details page for an overview of registered storage systems. If you need to configure the storage system, you will need to access the service processor with Device Manager - Storage Navigator.

Storage system inventory

From the dashboard, click Storage Systems to access the Storage Systems page for an overview of registered storage systems.



The Storage Systems page includes a summary section identical to the summary on the dashboard. This includes monitoring tiles, capacity summary and data protection summary.

You can search for a specific storage system by searching for its serial number in the search box. You can also use various filters to find a specific storage systems.

From the storage systems page you can view and manage individual storage systems.

View storage system details in either a tile view or a list view. Capacity utilization is represented by a color bar:

- Green: Below 70%.
- Orange: From 70% to 80%.
- Red: Over 80%.

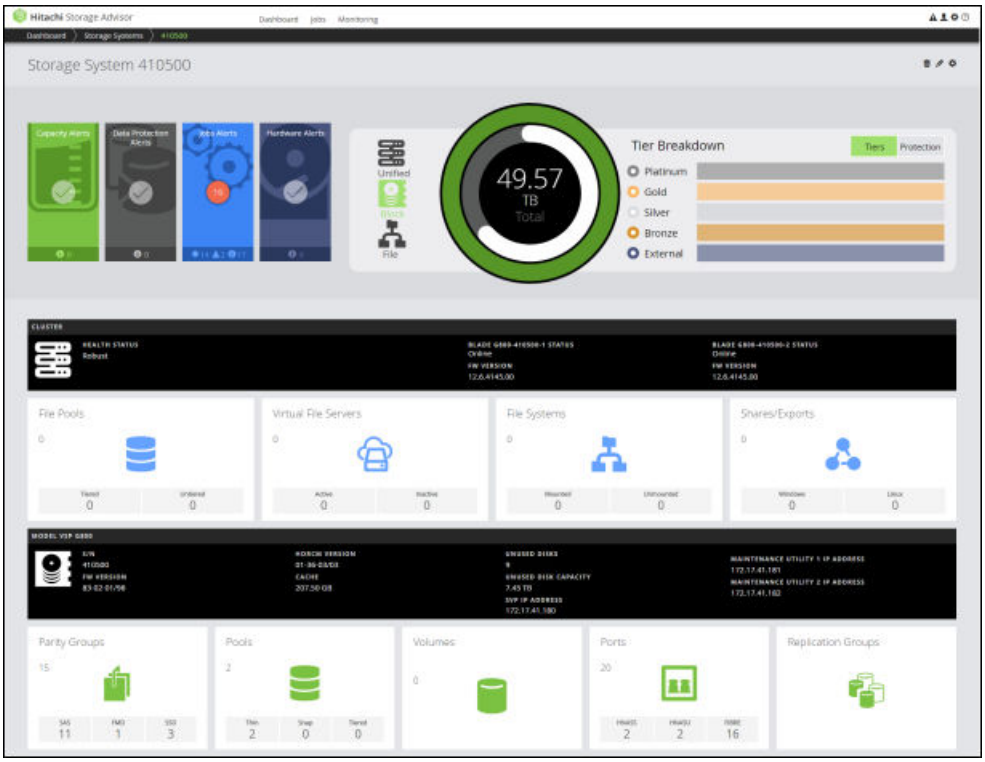
The following actions are available:

- Click a storage system to view details in the Storage System <*serial number*> page, where you can also access and manage the associated parity groups, pools, volumes, and ports.
- To delete a storage system, select it and click Delete .
- To edit the user name and password for a storage system, select it and click Edit to open the Update Storage System <*serial number*> page.

Storage system details

View details about a storage system and access resources.

On the dashboard, click Storage Systems and then click a Storage System <serial number> tile.



On a storage system detail page, you can do the following:

- Click Delete to delete the storage system. This action is available only to users with the SystemAdministrator role.
- Click Edit to update the storage system user name and password. This action is available only to users with the SystemAdministrator role.
- Click Settings in the upper-right corner to launch either of the following:
  - Device Manager - Storage Navigator to perform any advanced storage management operations that are not available in Storage Advisor.
  - If the storage system includes optional NAS modules, you can launch NAS Manager to perform operations that are not available in Storage Advisor.
- Review the information gauge regarding available capacity in storage system.
- Use the Alerts tiles to access alerts related to the storage system.
- Click Review Tiered Categories to open the Tier Management page to view and edit tier categories.
-

Field	Description
Model	Model name of the storage system.
S/N	Storage system serial number.
FW Version	Firmware version.
HORCM Version	01-33-03/06

Field	Description
	A data replication component residing on the server.
Cache Capacity	Total cache capacity configured on the storage system.
Unused Disks	Disks that are not assigned as hot spares or used to create parity groups.
Unused Disk Capacity	Total unused capacity of all disks.
SVP IP Address	Address of the service processor on the storage system.
Maintenance Utility IP Addresses 1 and 2	Configured automatically when the storage system is onboarded.

- View attributes about the storage system, including information that Storage Advisor discovered about the system, such as model, serial number, and SVP IP address.
- If you notice that the number of unused disks and unused disk capacity is too high, it implies that you have additional raw capacity in the system that can be converted into usable capacity by creating parity groups. Click Create Parity Groups to configure unused disks into parity groups.
- View the total and unused disk capacity for the different pool tiers.
- Click Review Tiered Categories to open the Tier Management page, where you can view the tier definitions and edit their names.
- Click a tile in the lower portion of the page to display the details for parity groups, pools, volumes, or ports for the storage system.

Using Device Manager - Storage Navigator for advanced storage configuration

Device Manager - Storage Navigator is the element manager for a supported storage system block module. 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 Storage System details page for advanced configuration options while performing management operations such as remote replication, volume migration, and resource group management with Storage Advisor.

Note: If you use Device Manager - Storage Navigator to manage resource groups, make sure that the user who adds storage systems in Storage Advisor has access to all custom resource groups and meta resource groups.

Use the Device Manager - Storage Navigator online help to obtain procedure information for advanced storage configuration tasks.

Accessing Device Manager - Storage Navigator

Launch Device Manager - Storage Navigator or from the Settings menu available in the Storage System details page. In the login dialog, use the user account assigned to you by your security administrator. The tasks that you can do on the system depend on the user role assigned to the user groups to which you belong.

In the login dialog, use the user account assigned to you by your security administrator. The tasks that you can do on the system depend on the user role assigned to the user groups to which you belong. Security administrators with view and modify privileges are responsible for setting up user accounts in Device Manager - Storage Navigator.

Refer to the Roles table for roles that are available for use in Device Manager - Storage Navigator and the permissions that each role provides to the users.

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
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

Role	Capabilities
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 service representatives.
Support Personnel (User)	• Viewing storage system status • Installing OS security patches • Updating operating systems • Performing basic maintenance

Using NAS Manager for advanced file storage configuration

NAS Manager is the element manager for NAS modules. It is a factory-installed application running on the NAS modules. You can access NAS Manager from the Storage System details page for advanced configuration options while performing management operations such as data protection, server settings and network configuration.

Use the NAS Manager online help to obtain procedure information for advanced file storage configuration tasks.

Accessing NAS Manager

Launch NAS Manager from the Settings menu available in the Storage System details page. In the login dialog, use the user account assigned to you by your administrator. The tasks that you can do on the system depend on your user role.

Refer to the Administrator types and responsibilities list for roles that are available for use in NAS Manager and the permissions that each role provides to the users.

Administrator types and responsibilities

This section describes the types of NAS storage system administrators and defines their expected roles in managing the system and the associated storage subsystems.

- **Global Administrators** can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server+Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access.
- **Storage Administrators** manage storage devices, as specified in the administrator profile created by the Global Administrator.
  Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users.
- **Server Administrators** manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices.
  Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules.
- **Server+Storage Administrators** manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator.
  Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components.

All administrators can connect to the NAS storage system through NAS Manager, the browser-based management utility provided by the system management unit (SMU). Additionally, Global Administrators can connect to the SMU command line interface (CLI).

Note: Server Administrators, Storage Administrators, and Server+Storage Administrators are not able to access all of the NAS Manager pages that a Global Administrator can access.

Tier management

The Tier Management page displays the tier definitions. You can edit the tier names (Platinum, Gold, Silver, Bronze, and External).

Access the Tier Management page in one of these ways:

- Click **Settings** and select **Tier Management**.
- In the detail page for a storage system, click **Tier Management**.

Updating a storage system

Update the user name and password for a storage system. This action requires the SystemAdministrator role be assigned to the user.

Procedure

1. Access the **Update Storage System <*serial number*>** page one of these ways:
   - On the **Storage Systems** page, select a storage system and click **Edit**.
   - On the **Storage System <*serial number*>** page, click **Edit**.
2. Edit the **Username** or **Password** and click **Submit**.

Managing servers

Storage Advisor supports provisioning storage to a group of server WWNs by allowing logical servers to be managed by Storage Advisor. Once servers are onboarded in Storage Advisor, storage volumes can be provisioned to the servers by creating Host Storage Domains and optionally creating zones to provide a path between the storage volume and server.

Adding servers

Add servers so you can attach volumes. You can add multiple server parameters from a file, or add one server at a time.

There are two methods of adding servers:

- Manually add information for one server at a time.
- Import a CSV (comma-separated values) file with information for one server in each row.

  The CSV file must have the following headings, in the order specified: Name, Description, IPAddress, OSType, WWNs (comma separated list of WWNs). All fields are required except Description and IPAddress. Valid OSType values are as follows:
  - AIX
  - HP_UX
  - LINUX
  - NETWARE
  - OVMS
  - SOLARIS

- TRU64
- VMWARE
- VMWARE_EX
- WIN
- WIN_EX

Procedure

1. On the Storage Advisor dashboard, click **Servers**. Then click the plus sign (**+**) to open the **Add Server** page.
2. On the **Add Server** page, do one of the following:
   - Click the upper plus sign (**+**) to browse for the CSV file or drag the file to the plus sign. The values from the file will populate the page.
   - Click the plus sign (**+**) in the table to add a row and enter a **Name**, **Description** (optional), **IP Address** (optional), **OS Type**, and **WWN**. You can add more servers by clicking the plus sign.
3. Click **Submit** to add the servers.

Result

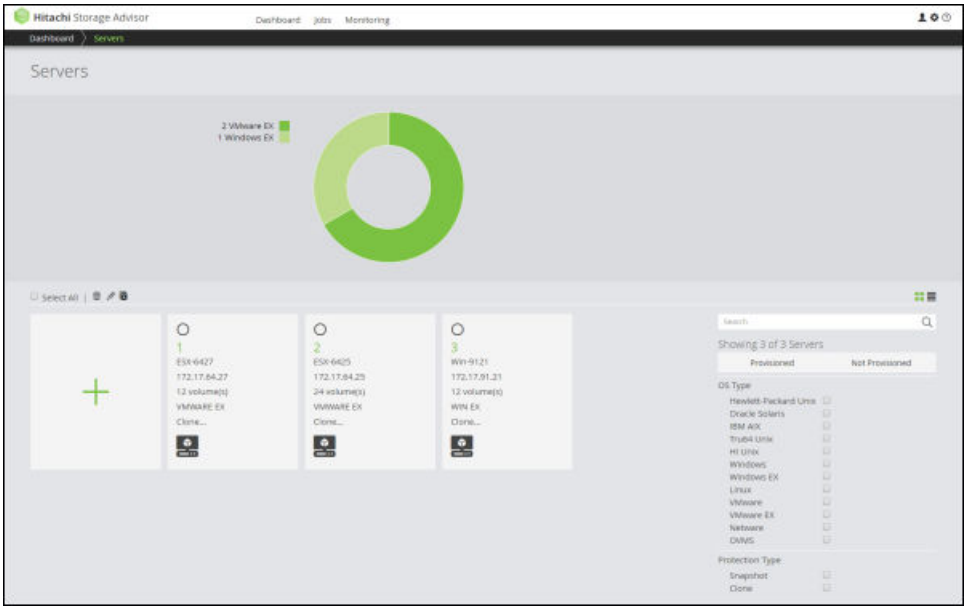
A job is started to add the servers.

Next steps

Create volumes and attach them to the server.

Server inventory

The Servers page displays all servers and includes a graphic summary based on operating systems.



To find the server you are looking for, you can either search by server ID or narrow down the list of servers using filters available.

You can click server tiles on this page to access details of individual servers and manage their volumes.

The following actions are available on this page:

- To add a server, click the plus sign (+) to open the Add Servers page.
- You can select one or more servers and perform the following actions:
  - Click Delete to delete the server.
  - Click Edit to update server parameters.
  - Click Create and Attach Volumes to use the provided workflow to create new volumes, attach them to the server, and optionally, protect the volumes.
  - Click Attach Existing Volumes to attach existing volumes to the server.

Server details

The Server details page provides you all the details about the server as well as a list of volumes, if any, attached to the server.

This page also shows path details for every volume attached to the server, including the storage ports and server WWNs used to create HSDs as well as the host mode options set up on the HSD.

You can perform server actions such as removing the server, editing the server or provisioning volumes to server by attaching existing volumes or creating and attaching new volumes.

You can perform volume operations such protecting or detaching volumes.

On the dashboard, click Servers to open the Servers inventory page. Then click a server tile to open the Server <*ID*> detail page for the selected server.

You can perform the following actions at the server level:

- Click Delete to remove the server.
- Click Edit to update server parameters.
- Click the cylinder icon ( ) and select one of the following:
  - Attach Existing Volumes to attach volumes to the server.
  - Create and Attach Volumes to create volumes and attach them to the server.

The following actions are available for volumes:

- If there is a Data Protection Failed alert, you can click it to see failed data protection jobs on the Data Protection Monitoring page.
- Click Edit to rename a volume on the Update Volume page. If the volume is unprotected, you can also update the size.
- Click Detach Volumes to detach volumes from the server.
  Before confirming, you can choose whether to remove SAN zones.

- Click Protect Volumes to protect volumes using Storage Advisor data protection technologies.
- Click Unprotect Volumes to remove data protection applied to volumes.
- Click Restore Volumes to restore from a backup.

Updating a server

You can change the parameters for an existing server.

Before you begin

Detach all volumes from the server. If you want to remove a WWN, detach all volumes using the WWN.

Procedure

1. From the dashboard, click **Servers** to open the inventory of servers.
2. Click server you want to update to open the server details page.
3. Click the pencil icon to open the **Update Server** page.
4. Edit the parameters and click **Submit**.

Managing volumes

A volume is a single accessible storage area, created in a pool within a parity group on a storage system. Create a volume and manage its properties with Storage Advisor

About capacity saving

Capacity saving reduces the used capacity of volumes.

Hitachi Storage Advisor allows you to use capacity saving when you create or update a volume.

A capacity saving volume is a dynamically provisioned volume (DP-Vol) that is capable of compression or both deduplication and compression.

When you create a capacity saving volume, HSA first creates a deduplication system data volume. This volume is used internally by the storage system, does not contain user data, and cannot be accessed by hosts.

Storage Advisor offers the following capacity saving options:

- Compression
  Compression allows you to reduce the used capacity of your volume.
- Deduplication and compression
  Deduplication identifies duplicate data blocks in order to remove redundancy and is done in addition to data compression.
- No
  No data compression or deduplication is done.

Creating volumes

Create volumes for a registered storage system so you can attach them to a server.

When you create volumes in Storage Advisor you can:

- Create multiple volumes of the same size or different sizes at the same time.
- Select the specific pool for volume creation or let Storage Advisor automatically select the best pool based on utilization.
- Specify a common label and starting label suffix for identical volumes that are the same size and have the same pool requirement.
- Set up compression, or deduplication and compression for the volume.

Before you begin

- Create parity groups.
- Create pools.
- Add servers (optional).

Procedure

1. On the Storage Advisor dashboard, click **Storage Systems** to see the inventory of storage systems and capacity information.
2. Click a storage system to see its configuration of servers, pools, ports, volumes, and parity groups.
3. Click **Volumes** to see the inventory of configured volumes for the storage system.
4. Click the plus sign (**+**) to open the **Create Volumes** page.
5. Configure volumes for the specified storage system.
   a. Enter the volume label (required) and select a suffix for it.
   b. Select the number of volumes.
   c. Select the size.
   d. Select the volume unit: **GB**, **TB**, or **PB**.
   e. Select the pool type: **Tiered** or **Thin**.
   f. For a Thin pool, select the **Tier**.

      If the storage system has available capacity from external storage, you can also select the **External** tier.
   g. If you select Thin pools, you can select **Compression**, **Deduplication and Compression**, or **No** from the **Capacity Saving** drop down list.
   h. (Optional) Select the pool from the list of available pools. The default selection is **Auto Selected**, which means that Storage Advisor selects the best pool for provisioning the volume based on utilization and tier requirements.
6. Click the plus sign to move the configured volume to the lower portion of the **Create Volumes** page.

   A blank row appears at the top of the page where you can create more volumes.

7. Click **Submit**.

Result

A job is started to create the volumes and add them to the volume inventory for the storage system.

Next steps

- Check the status of the volume-creation job by clicking Jobs.
- Attach volumes to a server.

Attaching existing volumes to a server

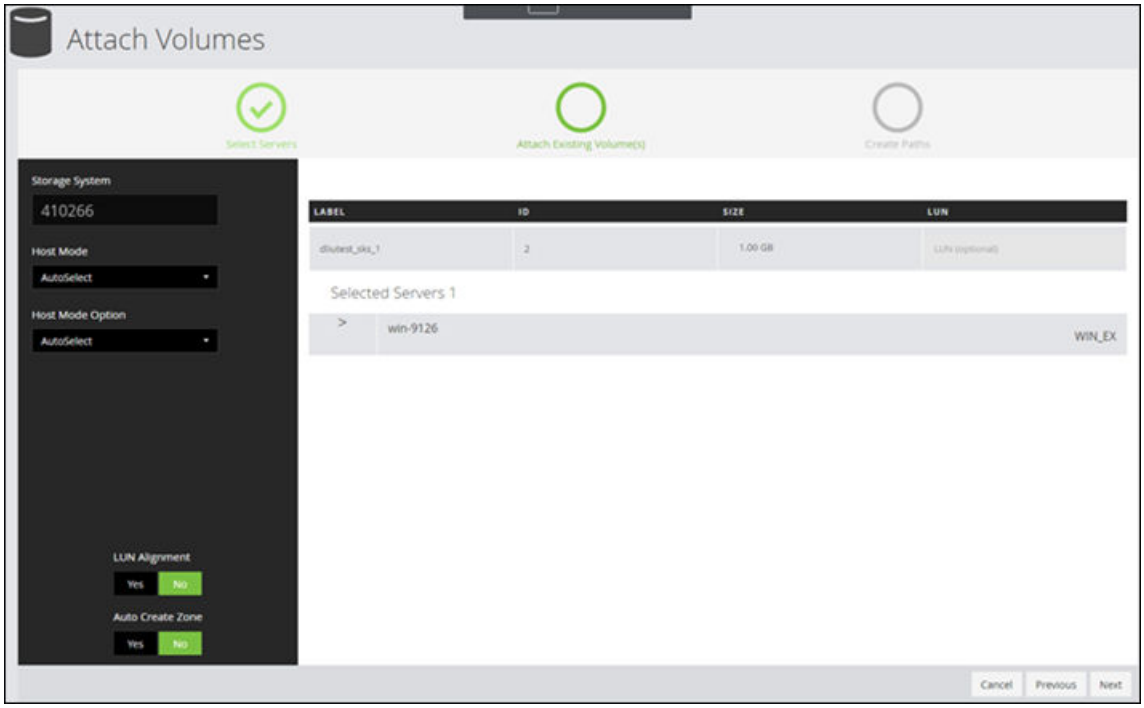
If there are volumes that have not been attached to servers, you can use this procedure to attach them.

Before you begin

- Enable security on ports.
- Add servers.
- Create volumes.

Procedure

1. To select volumes and servers, do one of the following:
   - On the **Volumes** inventory page for a storage system, select one or more volumes and click **Attach Volumes** to select servers on the **Attach Volumes** page.
   - On the **Servers** inventory page, select one or more servers and click **Attach Volumes** to select volumes on the **Attach Volumes** page.
   - On the detail page for a pool, select one or more volumes and click **Attach Volumes** to select servers on the **Attach Volumes** page.
2. Click **Next** to view options for attaching existing volumes.



3. The **Host Mode** is set by default to the server operating system. You can make a selection if needed.

   The server OS Type is provided when the server is added to Storage Advisor.

4. By default, the **Host Mode Option** will depend on the **Host Mode** selection.

   Default values are set only for **VMWARE EX** and **WIN EX** host modes. The default for all other Host Modes is none.

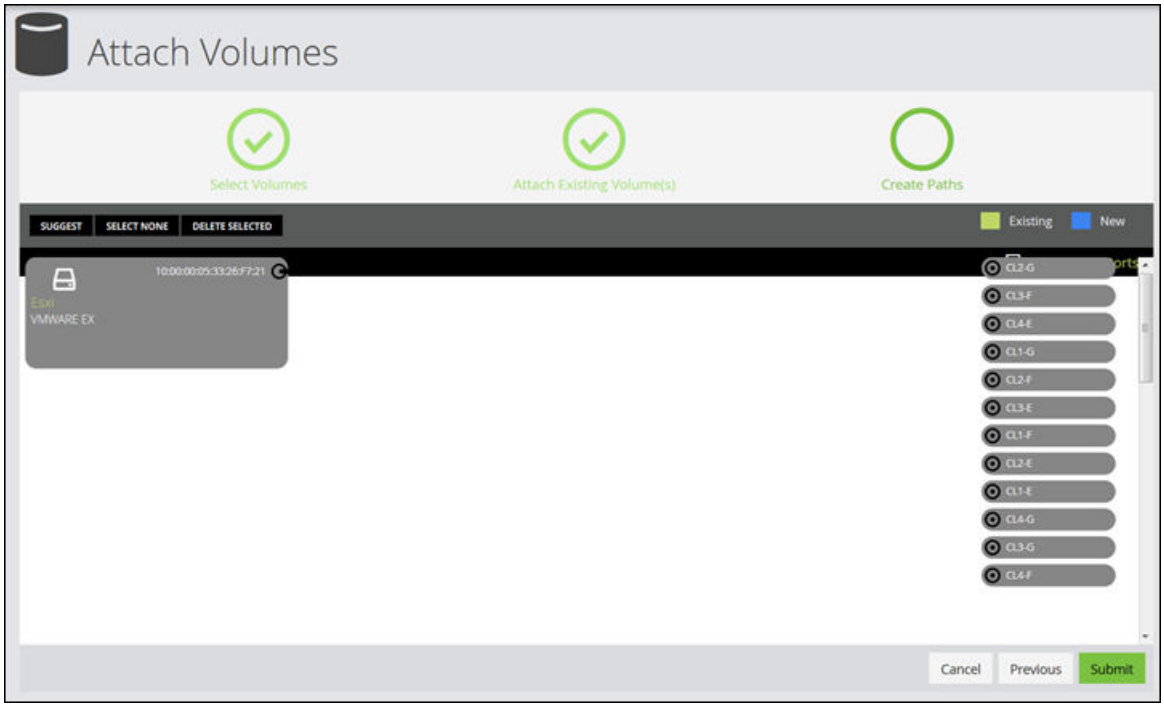
   Storage Advisor identifies all host groups containing any of the server WWNs. If all of those host groups have the same host mode and host mode options, those settings are prepopulated with the same settings in the host groups.

5. Select the **LUN Alignment**.

   By default, Storage Advisor uses the LUN number that is common to the servers. If attachment is to only one server, this setting has no effect.

6. The **Auto Create Zone** is set to **No** by default. You can set it to **Yes** to automatically create zones.

7. Click **Next** to view options for creating and editing LUN paths.



8. In the **Create Paths** panel, you can view servers and their WWNs, along with ports on the storage system. The following options are available for managing LUN paths:
   - Existing paths are populated as follows: all existing host groups with one or more server WWN and the exact same host mode and host mode options selected on the Attach Settings panel are populated as paths.

     To prevent the volume from being added to an existing path, click the path to highlight it and click **Delete Selected**.
   - Click **Suggest** to populate automatically selected paths. By default, the least-used ports are selected.
   - To manually create a path, click a WWN and a port to connect them with a blue connector line. Click the connector again and then click **Delete Selected** to delete the connection.
9. When you are satisfied with the paths, click **Submit**.

Update a volume

You can expand an unprotected volume and rename any volume.

Procedure

1. Navigate to details for a single volume in one of these ways:
   - From the dashboard, click **Storage Systems** and then click a storage system tile to view its resources. Click **Volumes** and then click the volume tile for the volume you want to update.

- From the dashboard, click **Servers** and then click a server tile to view its volumes. Click a volume tile for the volume you want to expand.

2. On the Volume <*ID*> page click **Edit** to open the **Update Volume** page.



Note: To reset a volume to the default settings, click **Reset**.

3. You can rename the volume, and if it is unprotected, you can change the size by clicking the right, left, up, and down arrows next to the volume size.
4. Toggle **Compression** and **Deduplication** to enable the desired capacity saving type.

Capacity saving type	Toggle compression	Toggle deduplication
Deduplication and compression	ON	ON
Compression only	ON	OFF
Disable capacity saving	OFF	OFF

5. Click **Submit**

Result

A job is started to update the volume.

Volumes inventory

The Volumes page enables you to filter, sort, and edit volumes for a single storage system, and to select volumes for data protection.

Access the inventory of volumes for a storage system to gain insight into volume size, data protection and utilization. You can also create volumes, attach existing volumes and perform data protection operations.

View volume details in either a tile view or a list view. Capacity utilization is represented by a color bar:

- Green: Below 70%.
- Orange: From 70% to 80%.
- Red: Over 80%.



Note: Volumes labeled HSA-reserved are created automatically when file pools are created and no operations can be performed on them in Storage Advisor.

The following actions are available on this page:

- If there are Data Protection Alerts, click the tile to view the alerts in the Monitoring tab.
- Click the plus sign (+) to add volumes on the Create Volumes page.
- Click a volume to view details and attach, update or delete the volume.

- Select a volume and click Edit to update the volume by editing the name. If the volume is unprotected you can also expand the capacity.
- Select one or more volumes to perform one of the following actions:
  - To delete volumes, click Delete. When you delete a volume, it is de-provisioned and removed from the storage system.
  - To attach existing volumes to one or more servers on the Attach Volumes page, click Attach Volumes.
  - To apply data protection on the Protect Volumes page, click Protect Volumes.
  - To suspend data protection, click Suspend.
  - To resume data protection following suspension, click Resume.
  - To unprotect a volume, select it and click Unprotect.

    Note: A volume in an "External" replication group cannot be unprotected.

  - To restore a secondary volume to the primary volume, click Restore to open the Restore Volume page.

Opening the Volume inventory page in Hitachi Storage Navigator

You can open the Volume inventory page in Hitachi Storage Navigator by clicking the icon ( ) to launch Storage Navigator and:

- Create a Command Device from a volume
- Restore a blocked volume
- Migrate a volume from one pool to another

For more information, refer to the *System Administrator Guide*

Note: Any changes you make in Storage Navigator may not be reflected in Storage Advisor for a few minutes.

Configure file storage

To configure file storage, begin by creating file pools and virtual file servers. You need both to create file systems.

Then create file systems and use them to create shares and exports that you can use to offer storage to users.

Managing file pools

Storage Advisor employs the following best practices in file pool creation:

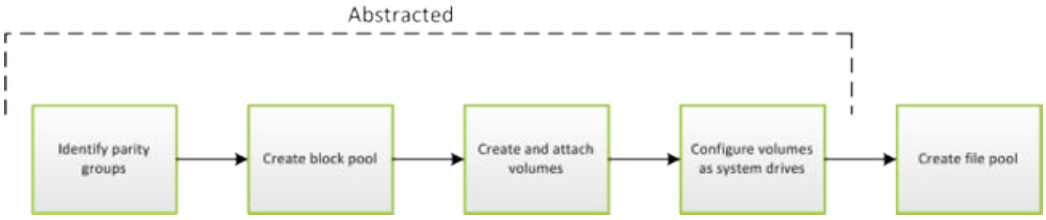
- For creation of the related block pool, use of RAID6 with a minimum of four parity groups for SAS or one parity group for SSD, FMD, or FMD DC2.

Note: This best practice is highly recommended. If capacity is chosen from non-conforming parity groups during file pool creation, a warning displays.

- Creation of a Thin pool that comprises each selected tier (either one or two).
- Minimum disk requirements for file pool creation:
  - 24 disks for SAS 10K, 15K
  - 48 disks for SAS 7.2K
  - 8 disks for FMD, FMD DC2, SSD

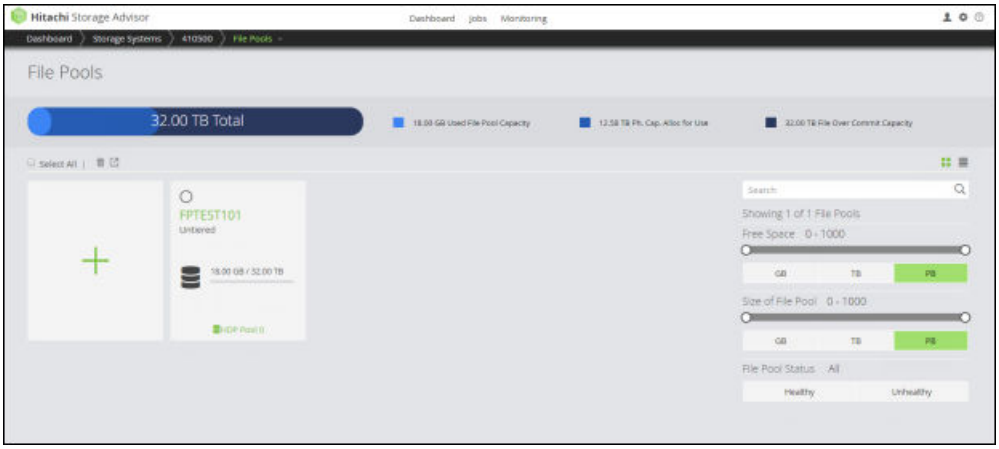
When a user creates a file pool in Storage Advisor, the system automatically performs the following operations:

1. Identifies parity groups.
2. Creates a block pool.
3. Creates volumes and attaches them to NAS modules.
4. Configures volumes as system drives.
5. Creates a file pool.



File pool inventory

Access the File Pools page from the detail page for a storage system.



Use this page to view file pool information in a tile or list view, and to delete or expand existing pools, as well as to create new pools.

The colored bars display used capacity, physical capacity allocated for use on the underlying block storage, and the file over-commit capacity. The over-commit capacity reflects the amount by which the file pool is over-subscribed.

Each tile or list row shows whether the file pool is tiered, it's File Pool Label, and capacity utilization.

The following actions are available:
- Create a new file pool by clicking the plus (+) sign to open the Create File Pool page.
- Delete one or more file pools by selecting them and clicking Delete.
- Add capacity by selecting a file pool and clicking Expand to open the Expand File Pool page.
- Open the File Pool detail page for the file pool by clicking a File Pool Label.
- Click a HDP Pool [ID] link in a tile to open the detail page for the underlying block storage pool.

Creating file pools

Create file pools to create file systems.

Before you begin

The minimum disk requirements are:
- 24 disks for SAS 10K, 15K
- 48 disks for SAS 7.2K
- 8 disks for FMD, FMD DC2, SSD

Onboard a storage system and create parity groups.

Note: Parity groups are created by a service representative.

Procedure

1. On the **File Pools** page, click the plus (**+**) sign to open the **Create File Pool** page.
2. Enter a label for the file pool.
3. In the **Select Capacity for New File Pool** pane, choose storage from one or two tiers. For a tiered pool, select Platinum and one other tier.

   Note: Best practices suggest that file over-commit capacity should be an estimated 200%. Best practices also include using RAID 6, with a minimum of four parity groups for SAS drives or one parity group for SSD, FMD, or FMD DC2 drives. If another RAID layout is selected, a warning displays.

The information gauge displays the total capacity, with the physical block capacity and estimated over-commit capacity also detailed.

The **Estimated Max Potential:** in IOPS displays after each type of capacity is selected.

Table 3 Tier Definitions

Pool Tier	Description
Platinum	SSD, FMD, FMD DC2
Gold	SAS 15 k
Silver	SAS 10 k
Bronze	SAS 7.2 k

4. (Optional) Adjust the Utilization Thresholds.
5. Click **Submit**.
   A job is added to create the file pool.

File pool details

Access the File Pool details page by clicking a **File Pool Label** in the File Pools page.

Use this page to view details about a file pool and to manage file systems in the pool.

You can search for a specific file system by searching for its File System Label in the search box. You can also use the Free Space and File Systems Size filters to find specific file systems, or filter by virtual file server.

View file system information in either a tile view or a list view, including capacity utilization and whether or not the file system is mounted.

Capacity utilization is represented by a color bar in each tile.

The following actions are available:

- Delete the file pool by clicking Delete.
- Expand the file pool by clicking Expand to open the Expand File Pool page.
- View details of an underlying block pool by clicking an HDP pool link in the file pool tile.
- Add a file system by clicking the plus (+) sign to open the Create File System page.
- Delete one or more file systems by selecting them and clicking Delete.
- Edit a file system by selecting it and clicking Edit to open the Update File System page where you can change the label or expand the file system.
- Select a file system and mount or unmount it.

Expanding a file pool

File pool capacity may need to be expanded when the used capacity approaches the capacity of the underlying block pool.

You can also relabel a file pool or change utilization thresholds.

To access the Expand File Pool page do one of the following:
- In the File Pools page, select a file pool and click Expand.
- In any file pool detail page, click Expand.

Procedure

1. To expand the file pool, select capacity from one of the tiers.
   An untiered file pool cannot be expanded into a tiered file pool.
2. If you want to change the file pool label, enter it in the **File Pool Label** field.
3. If you want to change utilization thresholds, use the sliders.
4. Click **Submit**.
   The job is added to the **Jobs** page.

Managing virtual file servers

Virtual file server inventory

Access the Virtual File Servers page from the dashboard or from the detail page for a storage system.

Use this page to view information about virtual file servers in a tile or list view. Use the filters to show only offline or online virtual file servers, or filter by blade number.

The following actions are available:
- Open the Create Virtual File Server page by clicking the plus (+) sign.
- Open the Virtual File Server detail page, where you can delete, edit, and enable or disable the virtual file server by clicking the virtual file server label in any tile or list row.
- Open the storage system detail page by clicking the Storage System [ID] link in any tile or list row.
- Delete one or more virtual file servers by selecting them and clicking Delete.
- Change the label for a virtual file server by selecting it and clicking Edit to access the Update Virtual File Server page.
- You can also Delete, Enable, or Disable by selecting a virtual file server and clicking the applicable icon.

Creating a virtual file server

Create virtual file servers so you can create file systems.

Before you begin

- Configure ports.
- Obtain the required IP address and subnet mask information for the virtual file server.

Procedure

1. On the **Virtual File Servers** page, click the plus sign (**+**) to open the **Create Virtual File Server** page.
2. Enter a label for the virtual file server.
3. Enter the IP address (ipv4 or ipv6) for the virtual file server.
4. Enter the subnet mask for the virtual file server.
5. Select the cluster node Gigabit Ethernet port to which the IP address for the virtual file server is assigned.
6. Click **Submit**.
   A job is added on the **Jobs** page to create the virtual file server.

Virtual file server details

Access the Virtual File Server detail page from the Virtual File Servers page.

Use this page to manage a virtual file server's file systems.

The following actions are available:

- Open the storage system detail page by clicking a Storage System [ID].
- Select a file system in either the list or tile view and do one of the following:
  - Delete the file system by clicking Delete.
  - Expand a file system or change the label on the Update File System page by clicking Edit.
  - Click Mount or Unmount to mount or unmount the file system.
  - Open the File System detail page by clicking a file system.
  - Open the detail page for the underlying file pool by clicking the File Pool link in a tile.

Managing file systems

File system inventory

Access the File Systems page from the detail page for a storage system. Use this page to view information about file systems in a list or tile view, and to manage file systems.

You can search for a specific file system by searching for its file system label in the search box. You can also use the Free Space and File Systems Size filters to find specific file systems, or filter by virtual file server.

View file system details in either a tile view or a list view, including capacity utilization and whether or not the file system is mounted.

Capacity utilization is represented by a color bar in each tile.

The following actions are available:

- View details of a file system by clicking the file system label in a tile or row to open the File System detail page.
- Add a file system by clicking the plus (+) sign to open the Create File System page.
- Delete one or more file systems by selecting them and clicking Delete.
- Edit a file system by selecting it and clicking Edit to open the Update File System page.
- Select a file system and Mount or Unmount it.
- View details of the underlying pool by clicking a File Pool label in a tile.
- View details of the related virtual file server by clicking the VFS label in a tile.

Creating file systems

Create file systems so that you can create shares on Windows and exports on Linux.

Before you begin

Create file pools and virtual file servers.

Procedure

1. Click the plus sign (**+**) on the **File Systems** page to open the **Create File System** page.
2. Select a virtual file server.
   a. Enter a label up to 255 alphanumeric characters.
   b. Select a format:
      - **4K**: This choice is best for small block random applications (Virtual Server / Virtual Desktops / Databases).
      - **32K**: This choice is best for large block sequential applications (Video, Media, Images) or when the file system is hosted on NL-SAS drives.
3. Enter capacity up to 1PB.
4. Select a pool and click **Submit**.
   A job is added to the **Jobs** page to create the file system.

File system details

Access the File System detail page from the File Systems page.

Use this page to create and manage shares and exports. You can also view information about a file system and access the associated file pool and virtual file server.

The following actions are available:

- Delete the file system by clicking Delete.
- Update label and capacity by clicking Edit to open the Update File System page.
- Mount or Unmount the file system by clicking Mount or Unmount.
- Access the file pool where the file system was created by clicking the File Pool [ID] link in the tile.
- Access the virtual file server where the file system was created by clicking the virtual file server label in the tile.
- Create a share or export by clicking the plus sign (+) to open the Create Shares/Exports page.
- Delete a share or export by selecting it and clicking Delete.
- Update a share or export by selecting it and clicking Edit to open the Update Share or Update Export page.

Updating a file system

Update a file system to re-label or expand it.

Procedure

1. On the **File Systems** page, select a file system and click **Edit** to open the **Update File System** page.
2. You can change the file system label, the capacity, or both.
   - To edit the label, enter changes in the label field.
   - To change the capacity, enter it and select a new unit of measure, if necessary.
3. Click **Submit**.
   The new job is added to the **Jobs** page.

Managing shares and exports

Shares enable file sharing in Windows and exports enable file sharing in Linux.

Shares and exports inventory

Access the inventory of shares and exports in the detail page for a storage system to view information about existing shares and exports in a tile or list view.

Use this page to add, edit, and delete shares and exports. You can also access related resources.

The following actions are available:

- To add a share or export, click the plus sign (+) to open the Create Shares/Exports page.
- To delete a share or export, select a tile and click Delete.
- To edit a share or export, select a tile and click Edit to open the Update Export page or the Update Share page.
- Click File System label in a tile to open the detail page for the file system where the share or export was created.
- Click VFS label in a tile to open the Virtual File Server detail page where the file system was created.

Creating shares and exports

Create shares and exports to offer storage capacity to users.

Procedure

1. Access the **Create Shares/Exports** page by clicking the plus sign (**+**) on the **Shares/Exports** page.
2. Enter a **File System Path** and a **Share/Export Label**.
3. Select a **File System**.
4. Create a share by selecting **Windows** or create an export by selecting **Linux**.
5. Click **Submit**.
   A job to create the share or export is added to the **Jobs** page.

Export details

Access the detail page for an export to review internal and external paths and to edit the export.

The following controls are available:

- Delete the export by clicking Delete.
- Edit the export by clicking Edit to open the Update Export page.
- Access the file system where the export was created by clicking File System.
- Access the virtual file server where the file system was created by clicking VFS.

Updating an export

You can update an export to change the file system path and access configuration.

Procedure

1. Access the **Update Export** page by clicking **Edit** in an Export detail page.

2. (Optional) Enter a new path in the **File System Path** field.
3. (Optional) In the **Access Configuration** field, enter IP addresses, host names, or the NIS netgroups of the clients who are allowed to access the NFS export (up to 5957 characters).

   If the system has been set up to work with a name server, you can enter the NIS netgroup to which the clients belong, or the client's computer name rather than its IP address (not case sensitive).

   You can also specify the required flavors of NFS security in a colon-separated list using the option (sec=<list>).

   The supported flavors are:
   - none - Connect as a null user
   - sys - The traditional security flavor used by NFS, users are not authenticated by the server
   - krb5 - Kerberos authentication
   - krb5i - Kerberos authentication with per-messaging integrity
   - krb5p - Kerberos authentication with per-message privacy

   For example: 10.1.*.*(sec=sys:krb5:krb5i)

   See the mount-point-access-configuration man page for further information.
4. Click **Submit** to save any changes.
   A job is added to the **Jobs** page to update the export.

Share details

Access the detail page for an share to review internal and external paths and to edit the export.

The following controls are available:
- Delete the share by clicking Delete.
- Edit the share clicking Edit to open the Update Share page.
- Access the file system where the export was created by clicking the File System label.
- Access the virtual file server where the file system was created by clicking the VFS label.
- Add an existing Account Domain user group to the share by clicking the plus sign (+) to open the Create Groups page.

Adding existing account domain groups to a share

You can add an existing account domain group to a share. This enables you to change users permissions when they access the share.

Before you begin

The account domain group and CIFS setup must already exist.

Procedure

1. On the detail page for a share, click the plus sign (**+**) to open the **Create Groups** page.
2. In the **Group Name** field, type in a user group name from the account domain.
3. Choose permissions; **Full Control**, **Change**, or **Read**.
4. Click **Submit**.
   A job is started to add the group to the share.

Updating a share

You can update a share to change the file system path, permissions, and access configuration.

Procedure

1. Access the **Update Share** page by clicking **Edit** in a Share detail page.
2. (Optional) Enter a new path in the **Modify File System Path** field.
3. (Optional) In the **Access Configuration** field, enter IP addresses of the clients who can access the share (up to 5,957 characters allowed in this field).

What to type	Means	Example
Blank or * Partial addresses using wildcards.	All clients can access the share.	10.168.*.* Clients with matching addresses can access the share.
Specific addresses	Only clients with the specified IP address can access the share.	10.168.20.2
Specific address range	Only clients with an IP address within the specified IP address range (10.168.20.0 to 10.168.20.255) can access the share.	10.168.20.0/16
Partial addresses using wildcards	Clients with matching addresses can access the share.	10.168.*.*
Permisssions		
What to type	**Permissions granted**	
(rw)	read-write	
(ro)	read only	

Note: The order in which you specify the entries is important. Take the following two lines:

- *(ro)
- 10.1.2.38(rw)

The first grants read-only access to all clients, whereas the second grants read/write access to the specified client. The second line is redundant, however, as the first line matches all clients. You must transpose the lines to grant write access to 10.1.2.38. Examples:

- 10.1.2.38(ro) grants read-only access to the client whose IP address is 10.1.2.38.
- 10.1.2.0/24(ro) grants read-only access to all clients with an IP address in the range 10.1.2.0 to 10.1.2.255
- 10.1.*.*(rw) grants read-write access to all the matching clients.

4. (Optional) Select the supplied **Everyone** group and select permissions.
5. Click **Submit** to save any changes.
   A job is added to the **Jobs** page to update the share.

System administration using Device Manager - Storage Navigator

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 Systems** 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.

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

Before you begin

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

Procedure

1. Copy the backup file to any folder in the SVP.
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 115

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.

Before you begin

- 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 114

System administration using the maintenance utility

Changing the date and time

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

Changing the controller clock settings

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

Before you begin

- 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.

Before you begin

- 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 an SVP.

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.

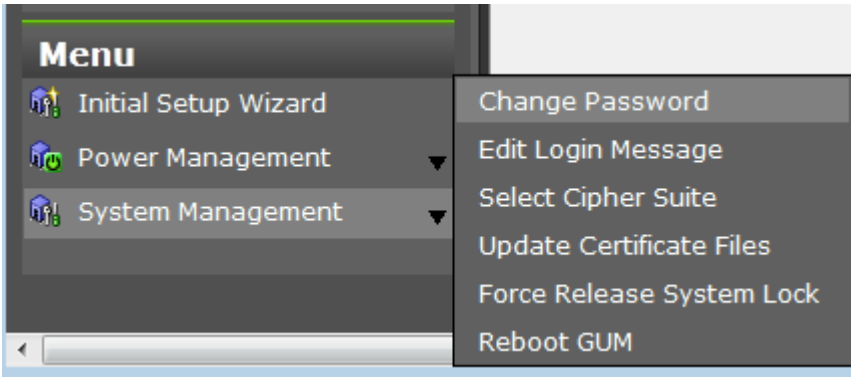
Changing the administrator password

Before you begin

- 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

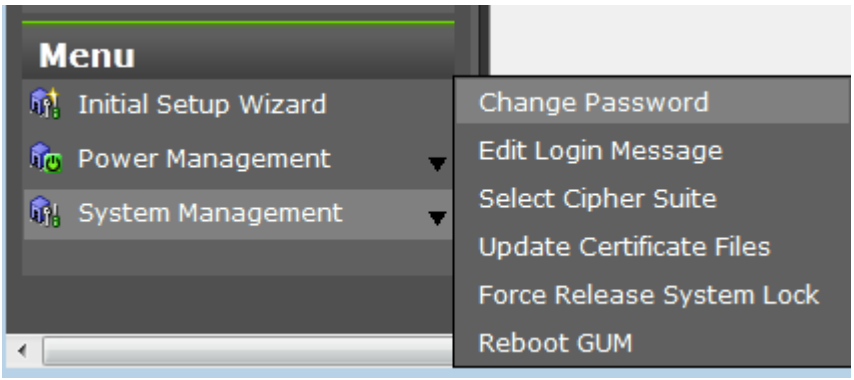
When users log in to the maintenance utility, they will see a login message. You can use the login banner message to inform users of specific system conditions, user requirements, or to provide other information that users may need to manage the system.

Before you begin

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.

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.

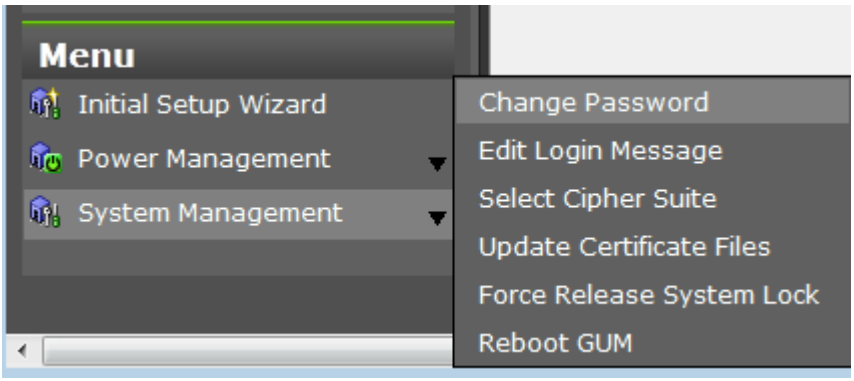
Caution: Before using this feature, ensure that releasing the system lock will not cause system problems due to processes that are currently running. Releasing the system lock can terminate a process before it completes and possibly leave the system in an unknown state. Check with any users that are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

Before you begin

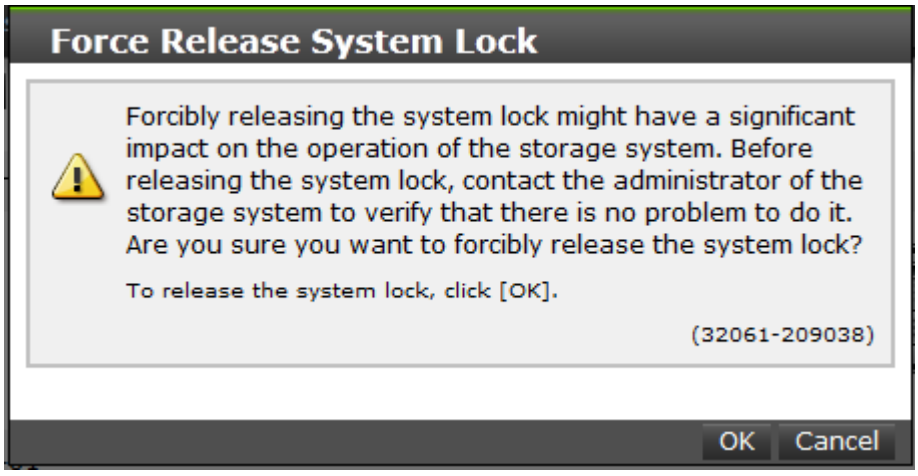
You must have the Storage Administrator (View & Modify) role to complete this procedure.

Procedure

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



2. Click **Force Release System Lock**.
3. A warning message is displayed. 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.



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`

System administration using NAS Manager

Changing the system date and time of the NAS modules

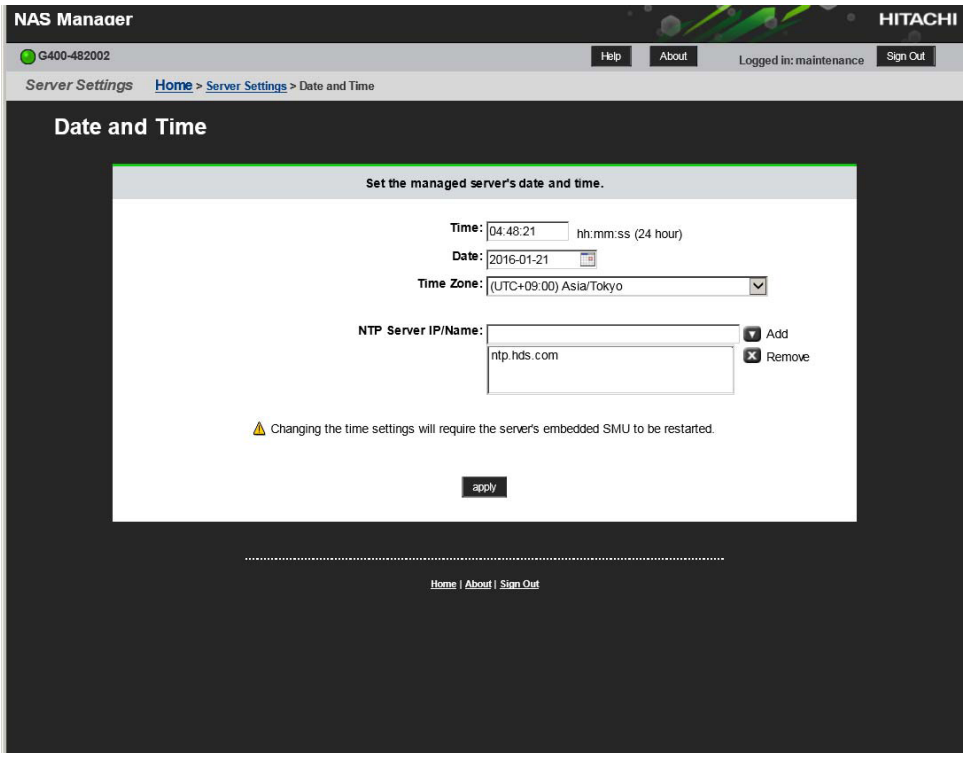
Use the following instructions to change the system date and time.

When the system date and time are set by NAS Manager, they are also reflected in the system date and time of the storage system.

Tip: See the *Hitachi NAS Platform Server and Cluster Administration Guide* for more details about changing the system date and time of the NAS modules.

Procedure

1. Log on to NAS Manager
2. Click **Server Settings**.
3. Click **Date and Time** in the **Server Settings** window.



4. In the **Date and Time** window, set date and time.

   When using NTP server:

   a. Select a time zone in **Time Zone** field.

   b. Enter the IP address or the name of the NTP server in **NTP Server IP/Name** field, and then click **add**.

      When using the Active Directory server, enter the IP address or the name of the NTP server.

   When setting without using the NTP server:

   a. Enter time in **Time** field.

   b. Enter date in **Date** field.

5. Confirm the settings and click **apply**.

Tip: You are not required to enter **Time** and **Date** because the settings are acquired from the NTP server.

6. Click **OK**.
   The window changes to the **Login** window a few minutes later.

Miscellaneous system administration considerations

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 2003, Windows Server 2008, Red Hat Enterprise Linux AS 5.0, Red Hat Enterprise Linux AS 4.0 on EM64T, or Red Hat Enterprise Linux AS 5.0 on EM64T
  You can set both an IPv4 address and an IPv6 address for the computer on which the report configuration tool is installed. 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 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 `raidinf` commands. Assign the storage administrator role (initial configuration) only to this user account.
  For information on user accounts, see Creating user accounts on page 148.
- The report configuration tool installation software
  The report configuration tool is available on the software installation media.

Installing the report configuration tool

Procedure

1. Insert the software installation media into a drive.
2. On the media, navigate to the `/program/Config_Report_CLI/Win32` folder and double-click `setup.exe` for Windows. Follow the instructions on the screen. If you are not using Windows, navigate to `/program/Config_Report_CLI/RIinstsh`.
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 on Windows. When necessary, specify the directory as the application path.

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.

The list of commands for creating reports is located in Raidinf command reference (obtaining configuration reports and tier relocation logs) on

page 249. Creating a configuration report on page 245 describes how to create a configuration report without using `raidinf` commands.

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.

For SVP firmware 83-03-01-*XX*/00 or later, some ports are automatically assigned unused port numbers.

You can change the automatically assigned port numbers:

- To check automatically assigned port numbers, see Viewing the port number used in SVP on page 125.
- To change an automatically assigned port number, see Reassigning an automatically assigned port number on page 128.
- To return a port to its automatically assigned port number, see Initializing and reassigning an automatically assigned port number on page 129.
- To change the range of port numbers used for automatic assignment, see Changing the range of an automatically assigned port number on page 130.
- To return the range of port number for automatic assignment to its original range, see Initializing the range of an automatically assigned port number on page 131.

Note: Perform this task only if an SVP port number is used by another application.

You need to verify the effects before you modify an SVP port number. See Effects of changing SVP port numbers on page 125.

The following table describes the port number key names and the initial value of the port number.

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
		Automatically assigned	83-03-01-*XX*/00 or later
DKCManPrivate	RMI	11099	83-01-24-*XX*/00 or later

Port number key name	Protocol	Initial port number	Corresponding SVP software version
SLP	SLP	427	83-01-24-*XX*/00 or later
SMIS_CIMOM	SMI-S	5989	83-01-20-*XX*/00 or later
		Automatically assigned	83-03-01-*XX*/00 or later
CommonJettyStart	HTTP	8080	83-01-24-*XX*/00 or later
CommonJettyStop	HTTP	8210	83-01-24-*XX*/00 or later
RestAPIServerStop	HTTP	9210	83-01-24-*XX*/00 or later
DeviceJettyStart	HTTP	8081	83-01-24-*XX*/00 or later
		Automatically assigned	83-03-01-*XX*/00 or later
DeviceJettyStop	HTTP	8211	83-01-24-*XX*/00 or later
		Automatically assigned	83-03-01-*XX*/00 or later

Viewing the port number used in SVP

You can view the port number used in SVP.

Procedure

1. Open the Windows command prompt as administrator on the SVP.
2. Move the current directory to the directory where the tool is located (for example: `C:\MAPP\wk\Supervisor`). Execute the following command: `C:MAPP\wk\Supervisor\MappIniSet\MappPortRefer.bat` *serial-number (optional)*

   Note: A space is required between `MappPortRefer.bat` and *serial-number.*

   If you omitted the serial number, information of every storage system that is registered in the **Storage Device List** window is displayed.

   For the port on which the port number information is not allocated, **Not Defined** is displayed and a completion message displays.
3. Press any key to acknowledge the message and close the message box.
4. 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	User reference 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 46.
	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 commands) 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 Raidinf command reference (obtaining configuration reports and tier relocation logs) on page 249.
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* (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. If the storage system is 83-03-01-*XX*/00 or later, check the port number which is used after registering the storage system. For detail, see Viewing the port number used in SVP on page 125.	*Hardware Reference Guide* for your storage system
CommonJettyStart	None	None
CommonJettyStop	None	None
RestAPIServerStop	None	None
DeviceJettyStart	None	None
DeviceJettyStop	None	None

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.

Before you begin

- 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 *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` *`port-number-key-name port-number`*

   Note:

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

- A space is required between *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.

To initialize the automatically assigned port number: See Initializing and reassigning an automatically assigned port number on page 129

Before you begin

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.

Reassigning an automatically assigned port number

You can reassign the port number that is automatically assigned to the storage system.

If the port number assigned to the storage system is used in another application, the port number is reassigned. Also, if you disabled the automatic assign, this deletes the unnecessary port number that is already assigned.

Caution:

- Stop the storage system service before reassigning. If you did not stop before reassigning, stop the storage system service in Storage Device List window, then start the service.
- The port for DeviceJettyStart and DeviceJettyStop that is assigned when starting the storage system service cannot be reassigned.
- If you disable the function which is using the port, this deletes the port number that is already assigned.

Procedure

1. Logout from Device Manager - Storage Navigator on the storage system that you want to reassign.
2. Stop the service of the storage system that you want to reassign.
3. Open the Windows command prompt as administrator on the SVP.
4. Move the current directory to the directory where the tool is located (for example, `C:\MAPP\wk\Supervisor)`. Execute the following command: `C:MAPP\wk\Supervisor\MappIniSet\MappPortManageRenum.bat` *serial-number (optional)*

   Note: A space is required between `MappPortManageRenum.bat` and *serial-number*.

   If you omitted the serial number, it is executed for the storage system of 83-03-01-*XX*/00 or later that is registered in the **Storage Device List** window.
5. A 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.
6. Press any key to acknowledge the message and close the message box.
7. Close the Windows command prompt.
8. Start the service of the storage system which is reassigned.

Initializing and reassigning an automatically assigned port number

You can initialize the port number that is automatically assigned to the storage system.

Caution:
- Stop the service of the storage system which has the status Ready in the Storage Device List window before initializing.
- If you did not stop before initializing, execute Reassigning an automatically assigned port number on page 128.

Procedure

1. Logout from Device Manager - Storage Navigator.

2. Stop the service of all the storage systems which have the status **Ready** in the **Storage Device List** window.
3. Open the Windows command prompt as administrator on the SVP.
4. Move the current directory to the directory where the tool is located (for example, `C:\MAPP\wk\Supervisor`). Execute the following command:
   `C:MAPP\wk\Supervisor\MappIniSet\MappPortManageInit.bat`
5. A 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.
6. Press any key to acknowledge the message and close the message box.
7. Reassign the port number.

   `C:MAPP\wk\Supervisor\MappIniSet\MappPortManageRenum.bat` *serial-number (optional)*

   Note: A space is required between `MappPortManageRenum.bat` and *serial-number*.

   If you omitted the serial number, the batch file is run for the storage system of 83-03-01-*XX*/00 or later which is registered in **Storage Device List** window.
8. A 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.
9. Press any key to acknowledge the message and close the message box.
10. Reassign the port number for all the registered storage systems by executing Steps 7 through 9.
11. Close the Windows command prompt.
12. Start the service of the storage system.

Changing the range of an automatically assigned port number

You can change the range of the port number that is automatically assigned to the storage system.

Procedure

1. Open the Windows command prompt as administrator on the SVP.
2. Move the current directory to the directory where the tool is located (for example, `C:\MAPP\wk\Supervisor`). Execute the following command:
   `C:MAPP\wk\Supervisor\MappIniSet\MappPortRangeSet.bat` *port-number-key-name port-number-range*

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

- A space is required between *port-number-key-name* and *port-number-range*.

The following table shows the port number key name and initial value of the port number range which can be changed. Port 0 is not assigned.

Port number key name	Initial value of port number range	Remark
PreRMIServer	51100 to 51355	None
SMIS_CIMOM	5989 to 6244	None
DeviceJettyStart	48081 to 48336	None
DeviceJettyStop	48411 to 48666	None
unavailable	1 to 1023	Port number that is not used in automatic assign

- The valid range of the port number is between 1 and 65535. Use a port number that is not used in another service.
- Port numbers between 1 and 1023 are reserved for the other applications. If you exclude a number between 1 and 1023 from the setting value of unavailable, the port numbers might not operate normally.
- The following can be used for the port number range:
  Numbers, space, symbols (, -) and rm
- You can specify multiple *port-number-key-name* and *port-number-range*.
  For example: `MappPortRangeSet.bat PreRMIServer 51200-55000 SMIS_CIMOM 5989-6244,8000`

3. Press any key to acknowledge the message and close the message box.
4. Close the Windows command prompt.

Initializing the range of an automatically assigned port number

You can initialize the range of the port number that is automatically assigned to the storage system.

Procedure

1. Open the Windows command prompt as administrator on the SVP.
2. Move the current directory to the directory where the tool is located (for example, `C:\MAPP\wk\Supervisor`). Execute the following command:
   `C:MAPP\wk\Supervisor\MappIniSet\MappPortRangeInit.bat`
3. A 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.
4. Press any key to acknowledge the message and close the message box.

5. Close the Windows command prompt.

Releasing HTTP communication blocking

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

Before you begin

- 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.

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 the HTTP communication port as needed.

Before you begin

- 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.

4

User Administration

This chapter describes various user roles, permissions, and groups available to manage your storage system.

- User administration for maintenance utility
- User administration for Device Manager - Storage Navigator
- User Administration for NAS Manager

User administration for maintenance utility

The maintenance utility allows you to set up and manage user accounts.

Required roles for operating Maintenance Utility

You can control the availability of using each operation window of Maintenance Utility for a user by registering the user in the user group and assigning them with the appropriate role.

The following table lists the required roles for using specific Maintenance Utility operation windows.

Maintenance Utility operation window	Required role name
Initial Setting Wizard	Storage Administrator (Initial Configuration)
Set Up System Information	Storage Administrator (Initial Configuration)
Firmware	Support Personnel or User Maintenance*
User Administration	Security Administrator (View & Modify)
Alert Notifications	Storage Administrator (Initial Configuration)
Set Up Date & Time	Storage Administrator (Initial Configuration)
Set Up Network Settings	Storage Administrator (Initial Configuration)
Licenses	Storage Administrator (Initial Configuration)
Audit Log Settings	Audit Log Administrator (View & Modify)
Turn on/off Locate LEDs	Support Personnel or User Maintenance*
Power on Storage System	Support Personnel or User Maintenance*
Power off Storage System	Support Personnel or User Maintenance*
Edit UPS Mode	Support Personnel or User Maintenance*
Edit Login Message	Storage Administrator (Initial Configuration)
Select Cipher Suite	Security Administrator (View & Modify)
Update Certificate Files	Security Administrator (View & Modify)
Force Release System Lock	Storage Administrator (Initial Configuration)
Reboot GUM	Support Personnel or User Maintenance
Change Password	No role is required.
Boot System Safe Mode	Support Personnel*
Alert Display	Support Personnel or User Maintenance*
Alert Display Related to FRU	Support Personnel or User Maintenance*

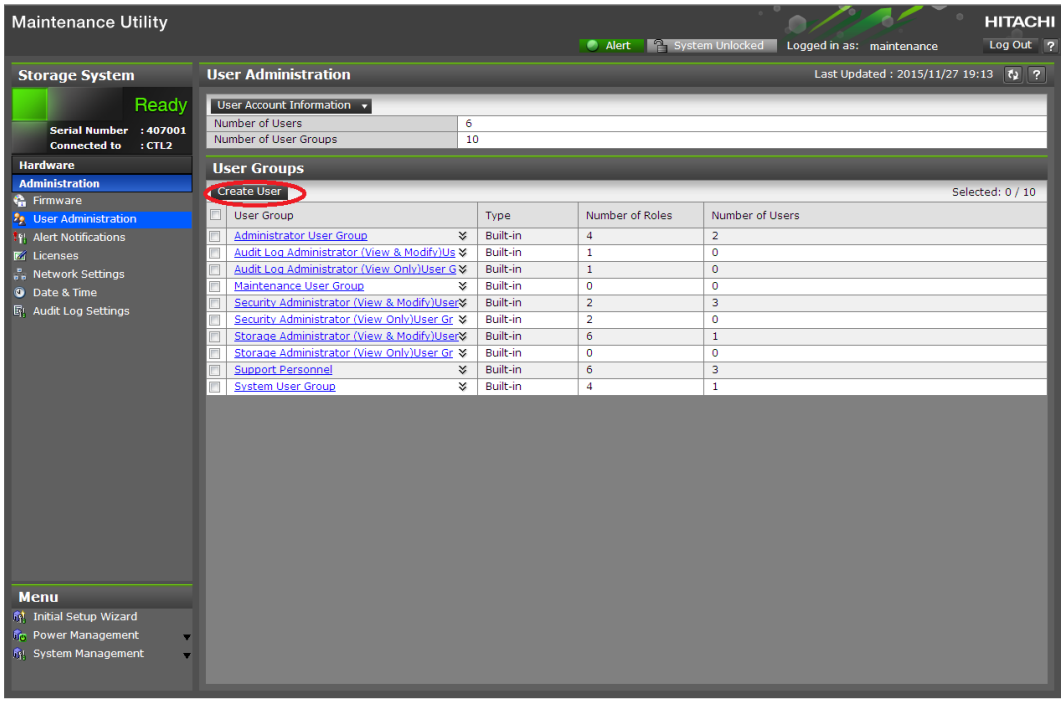
Maintenance Utility operation window	Required role name
Administration Menu	N/A
Power Management	N/A
System Management	N/A
Resetting GUM	N/A
* • Support Personnel: Operations performed by the service personnel • User Maintenance: Operations performed by the user	

Setting up user accounts

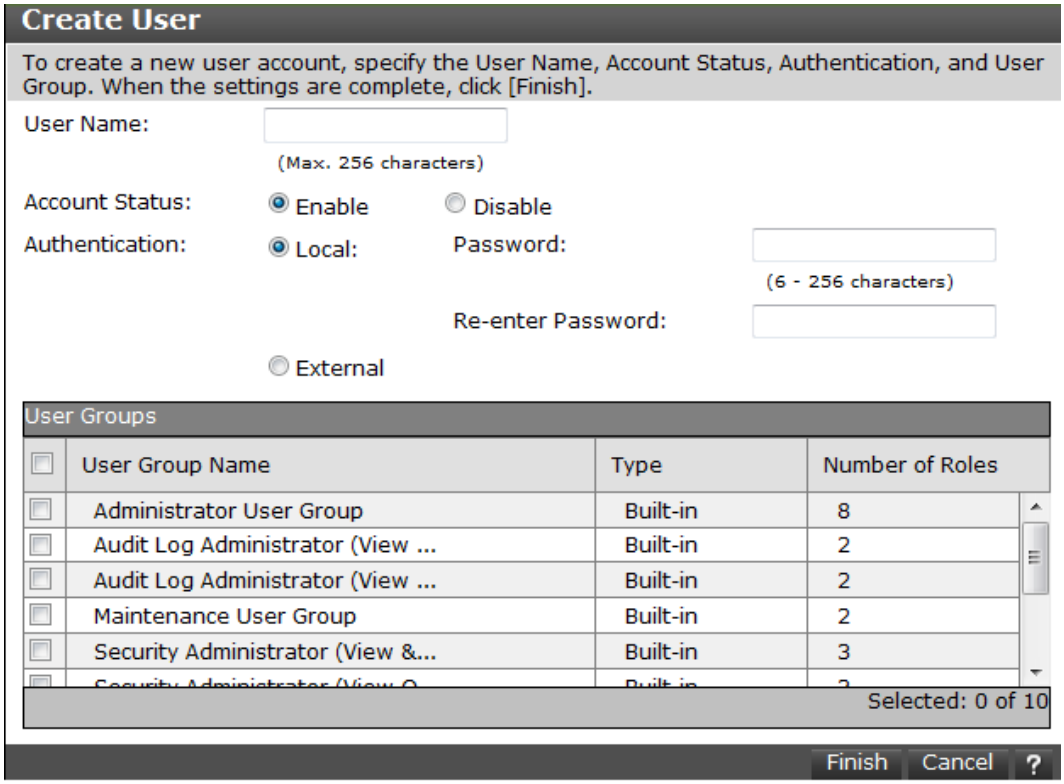
This procedure describes how to create a user account and register the account to a user group with appropriate roles. You can create up to 20 users, including the built-in user.

Procedure

1. In the Maintenance Utility window, click **Administration > User Administration**.
2. In the **User Groups** tab, click **Create User**.

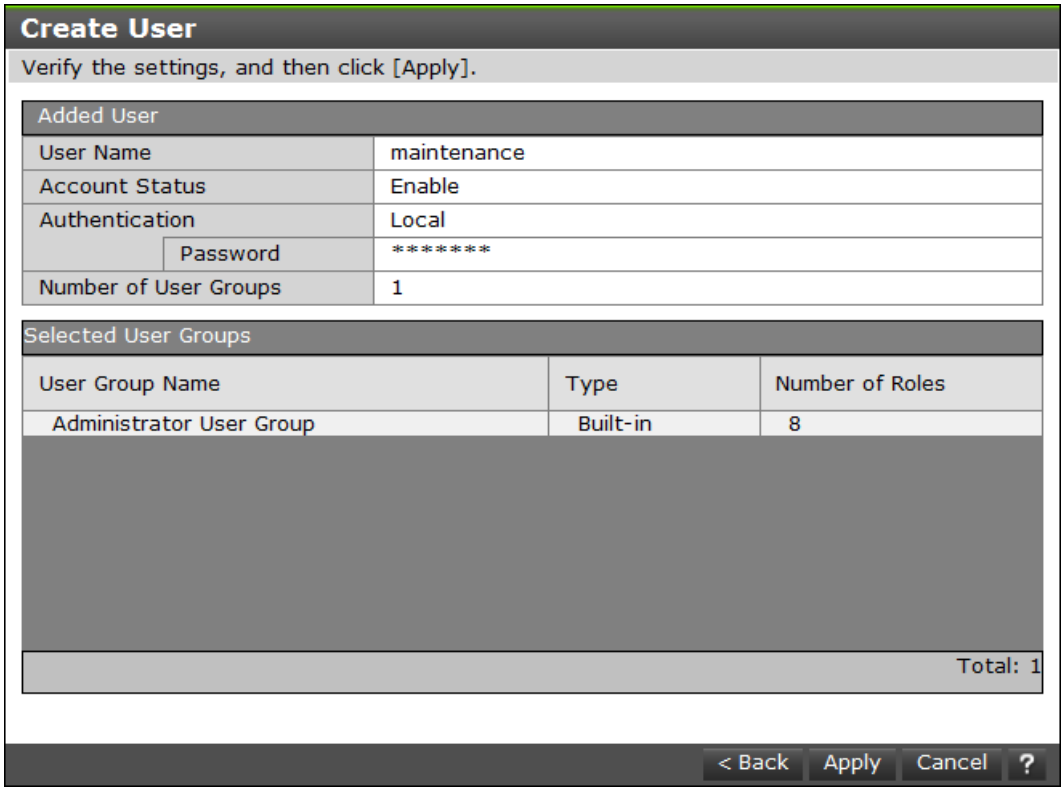


3. Create a new user account. Specify the User Name, Account Status, Authentication and User Group. Click **Finish**.



Item	Description
User Name	
Account Status	The following statuses are available: Enable = user can use the account. Disable = user cannot use the account or log in to the storage management software.
Authentication	The following methods are available: Local = does not use authentication server. Uses a dedicated password for storage management software. External = uses an authentication server.

4. Confirm the settings, and then click **Apply**.



5. When the completion message appears, click **Close**.

Disabling user accounts

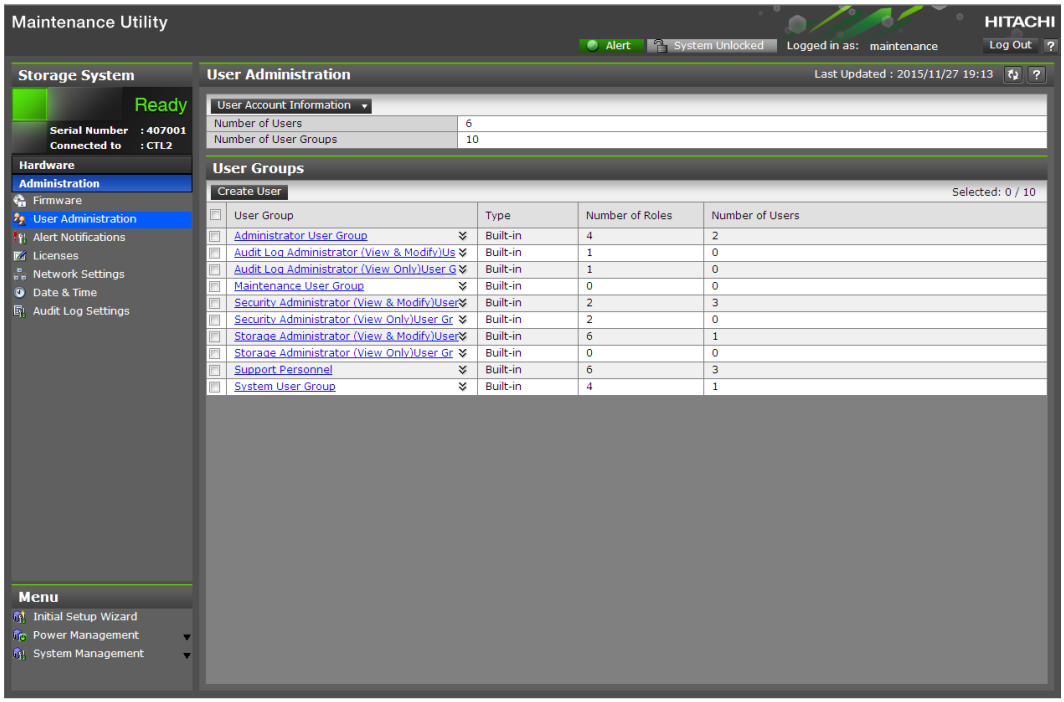
The following procedure describes how to disable user accounts.

Observe the following guideline:

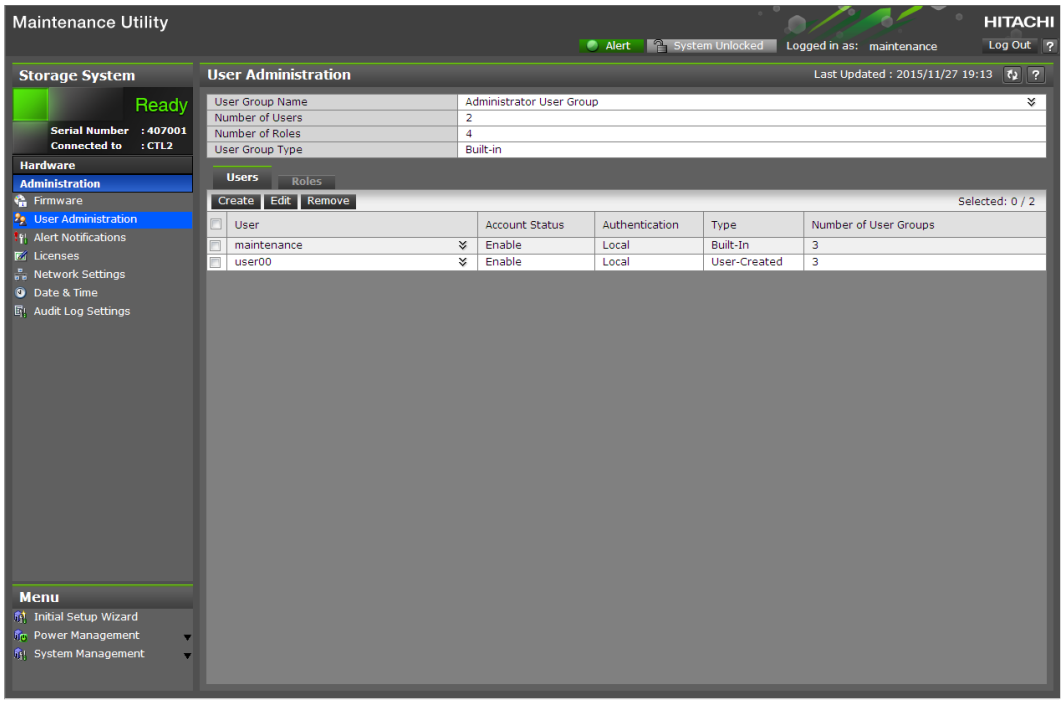
- Log into an account that is different from the user whose account that you want to disable (you cannot disable the current login user account).
- To disable the user account specified by the registered storage system in the **Storage Device List** window, click Stop Service for the registered storage system. After disabling the user account, click Edit to enable the user account.

Procedure

1. In the Maintenance Utility window, click **Administration > User Administration**.
2. In the **User Groups** tab, click the user group to which the user belongs.

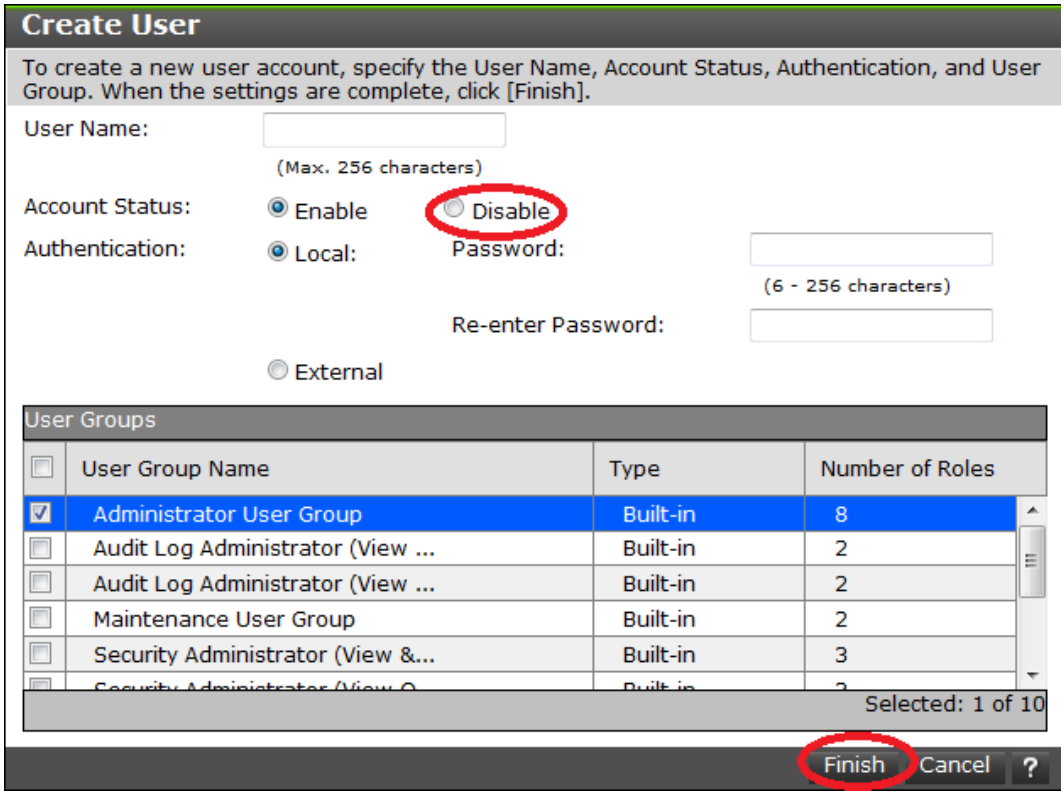


3. Click the **Users** tab, and then select the user that you want to disable.

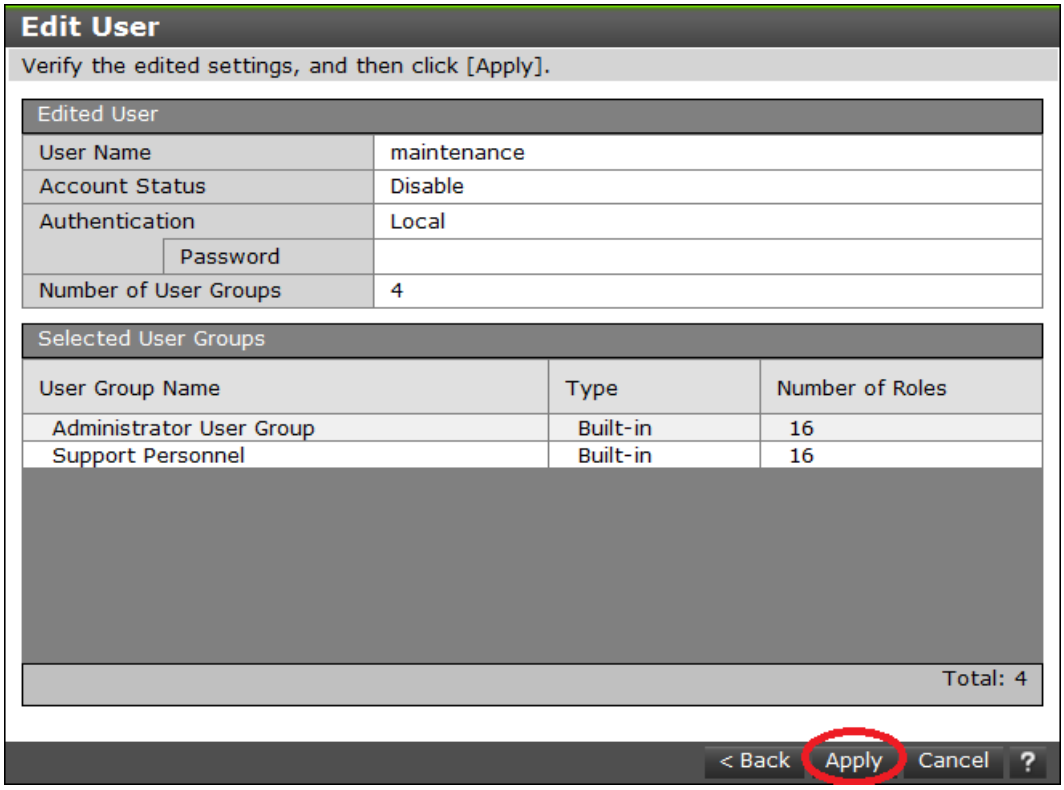


4. Click **Edit**.

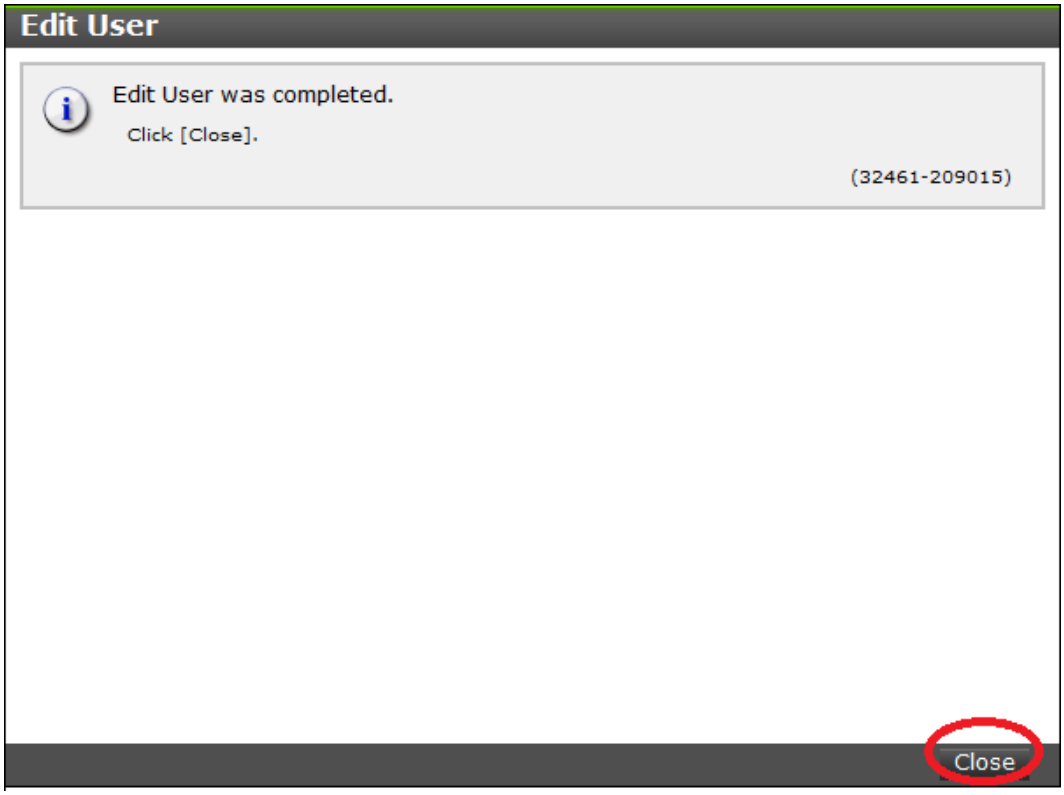
5. For **Account Status**, click **Disable**, and then click **Finish**.



6. Confirm the settings, and then click **Apply**.



7. When a completion message appears, click **Close**.



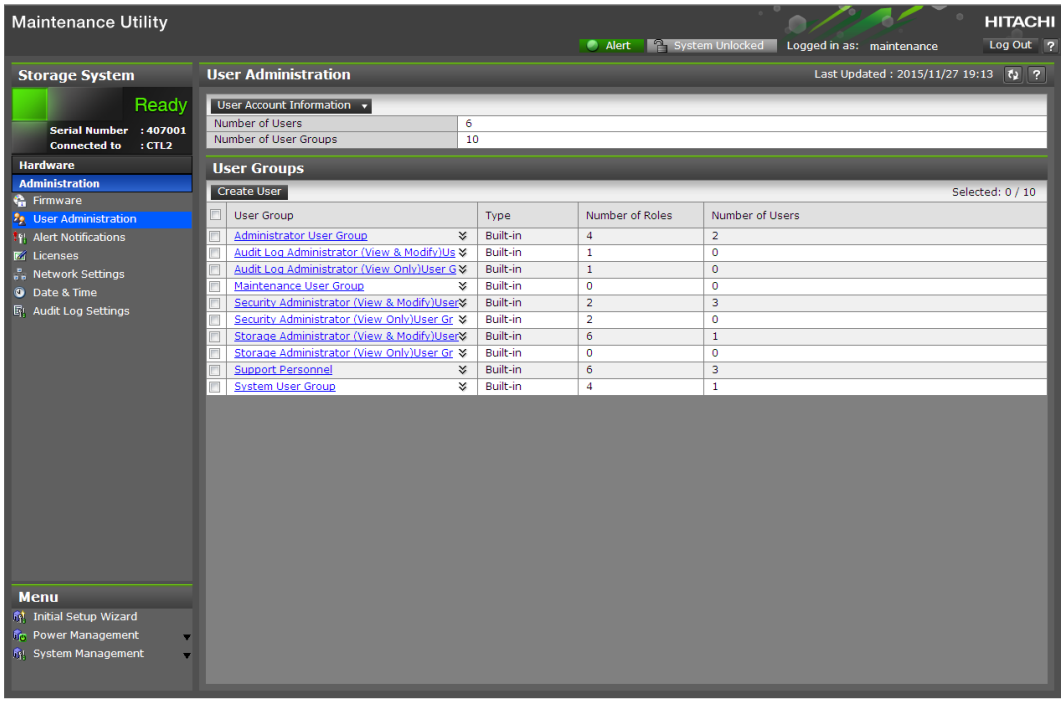
Removing user accounts

Security administrators can remove a user account when the account is no longer in use. Built-in user accounts cannot be deleted. If deleting the current login user account, you can continue the storage management software operation until you log out.

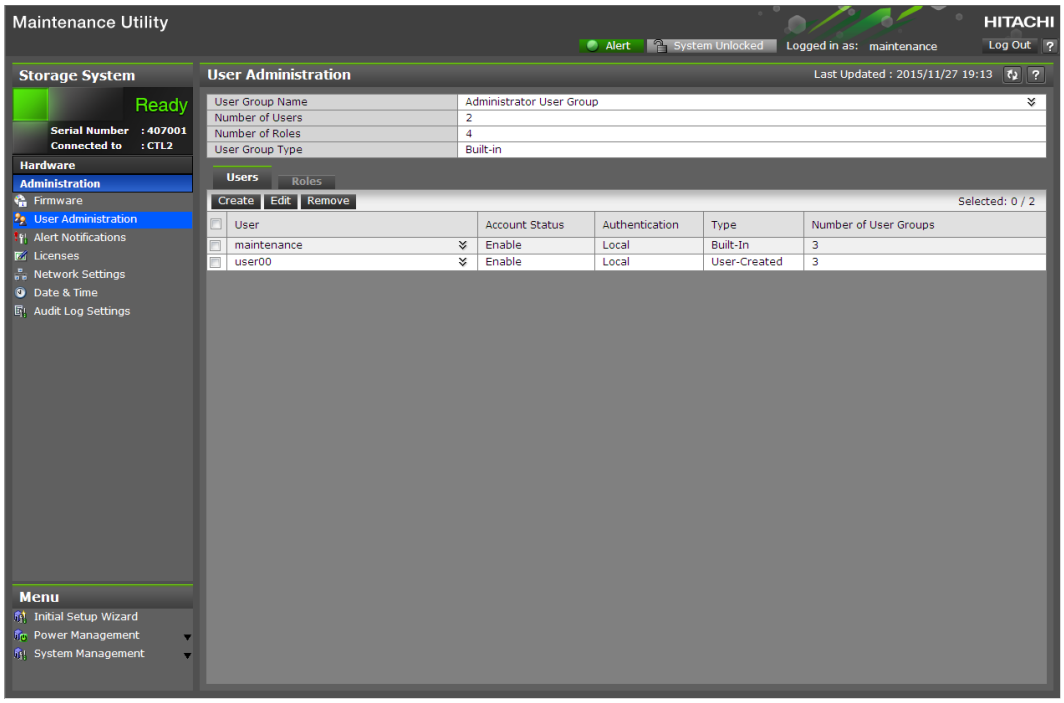
Note: To delete the user account specified by the registered storage system in the **Storage Device List** window, click **Stop Service** of the registered storage system. After deletion, click Edit to enable the user account.

Procedure

1. In the Maintenance Utility window, click **Administration > User Administration**.
2. In the **User Groups** tab, click the user group to which the user belongs.

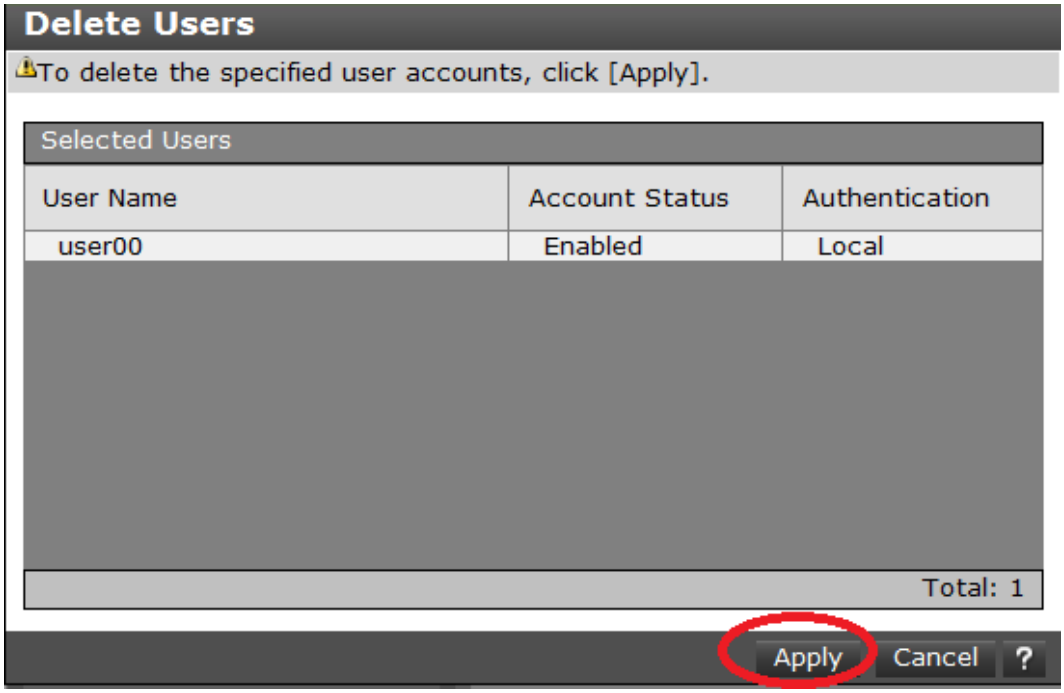


3. Click the **Users** tab, and then select the user you want to remove.

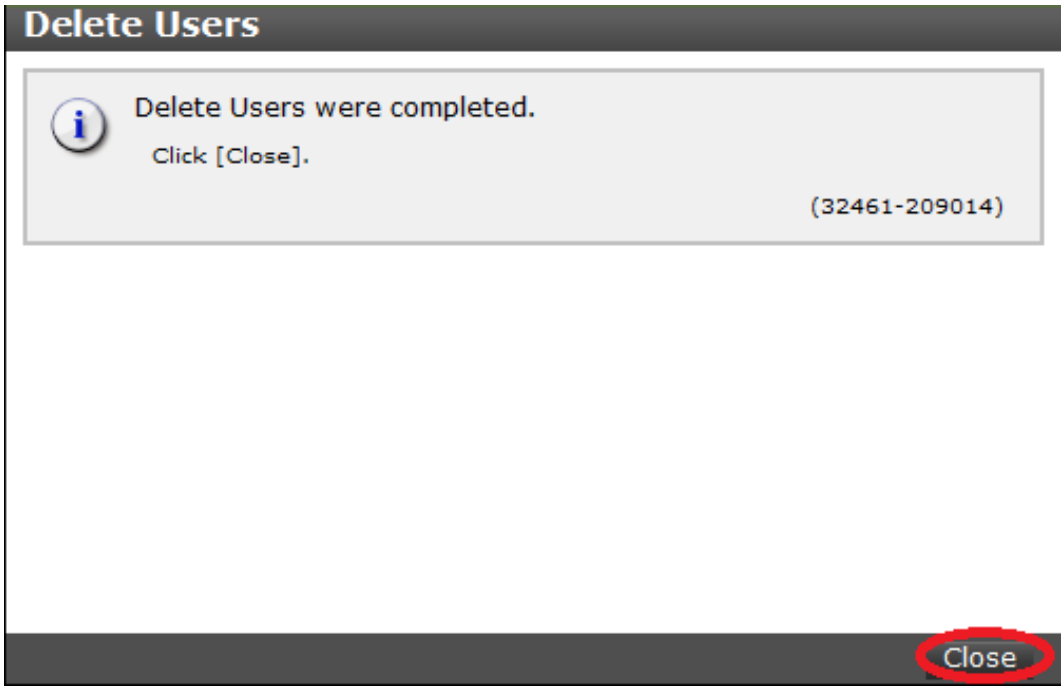


4. Click **Remove**.
The **Confirm** window opens.

5. In the **Confirm** window, confirm the settings, and then click **Apply**.



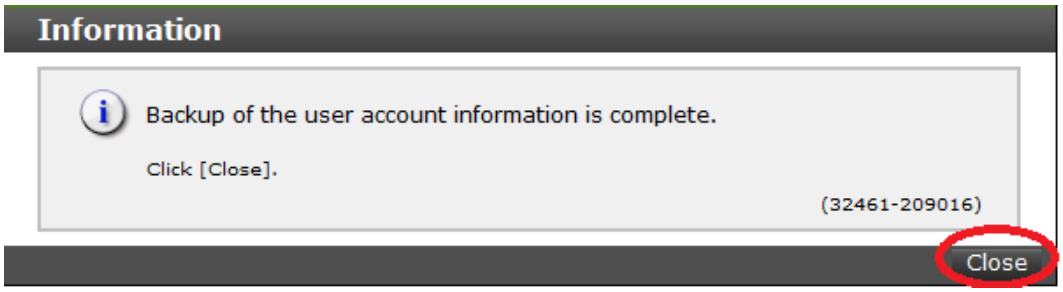
6. At the completion message, click **Close**.



Backing up user accounts

Procedure

1. Click **User Account Information > Backup**.
2. Specify a storage destination and a file name in the displayed window and download a file.
3. When the following message appears, click **Close**.

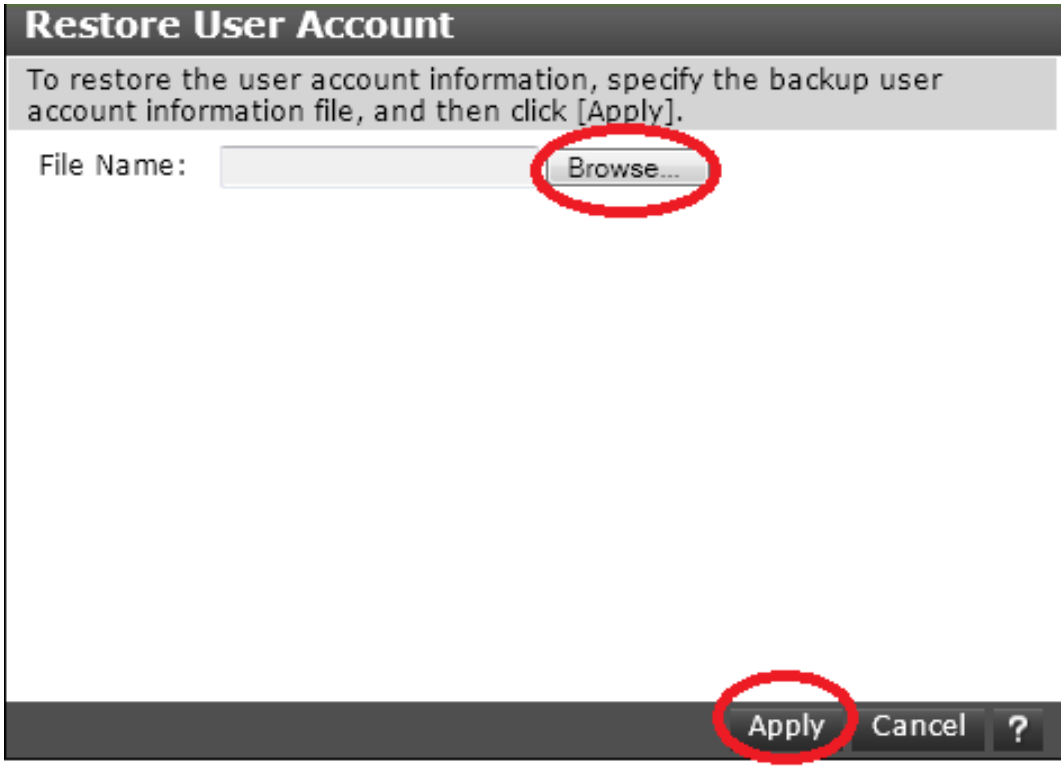


Restoring user account information

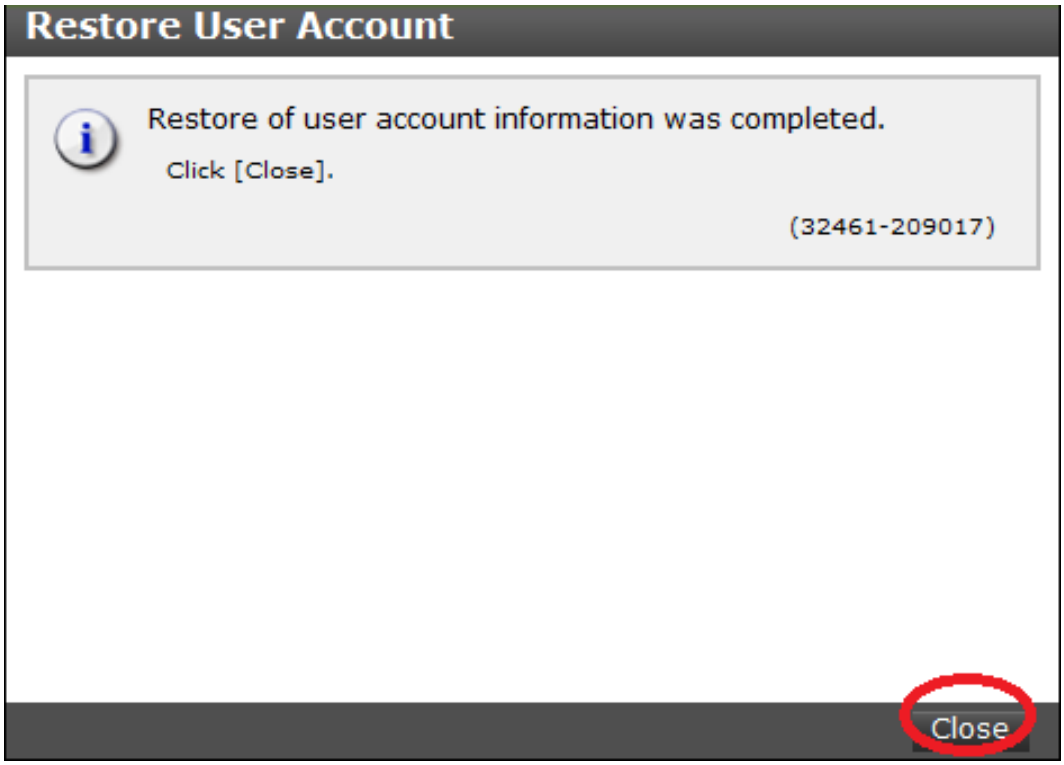
Procedure

1. Click **User Account Information > Restore**

   The **Restore User Account** window opens.
2. Specify file names to be restored, and then click **Apply**.



3. When a completion message appears, click **Close**.



User administration for Device Manager - Storage Navigator

This section describes various user roles, permissions and groups available to manage 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 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 user groups whose roles are other than Storage Administrator, All Resource Groups Assigned is automatically set to Yes. If you delete all the roles except 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 161

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 162 for information and instructions.
- Review Managing user groups on page 155 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 148.
- Change, disable, or delete user passwords and permissions. See Changing user passwords on page 151.

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 access the storage system temporarily 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, or when 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 148
- Changing user passwords on page 151
- Changing user permissions on page 152
- Enabling or Disabling user accounts on page 153
- Deleting user accounts on page 154

Creating user accounts

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

Before you begin

- 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 4 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 5 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] - . @ _
Password	6-63	• Alphanumeric characters • The following symbols:[1] , - . @ _
Note:		

Item	Length in characters	Characters that can be used
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.

   The user logging in to NAS Manager must belong to the built-in Administrator group.
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 and NAS Manager.
7. To use an authentication server, select **External**. To authenticate users with only Device Manager - Storage Navigator, or to log in to NAS Manager, 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.

Character restrictions for user names and passwords

Note the following restrictions for user names and passwords.

A user account created by using Device Manager - Storage Navigator can be used for maintenance utility, CCI, and NAS Manager. It can also be used by maintenance personnel for logins (the Support Personnel role is required).

The number of characters and types of characters that can be used vary between Device Manager - Storage Navigator, CCI, and NAS Manager. If a user uses all three programs, specify a user name and a password that satisfy the following conditions.

Item	Length in characters	Characters that can be used
User name	1-20	• Alphanumeric (ASCII code) characters • The following symbols[1, 3]: - . _
Password	6-63	• Alphanumeric (ASCII code) characters • The following symbols[1, 2]: - , . : @ _

Note:
1. If the host on which CCI is installed is running on UNIX, a slash (/) can be specified.
2. If the host on which CCI is installed is running on Windows, a back slash (\) can be specified.
3. Do not specify a user name consisting of periods (.) (..) only, or specify a user name beginning with a hyphen (-). If you specify such names, you cannot log in to NAS Manager.

Note: To use NAS Manager after installing NAS modules, users created with DKCMAIN firmware 83-03-2*x* or earlier, must change the password. If you do not change the password, you cannot log in to NAS Manager. Also, if a user name contains more than 20 characters, the user cannot log in to NAS Manager.

User name and password for Device Manager - Storage Navigator

Item	Length in characters	Characters that can be used
User name	1-256	• Alphanumeric (ASCII code) characters • The following symbols: # $ % & ' * + - . / = ? @ ^ _ ` { | } ~ You cannot use the # symbol when you enter a user name in a screen from the **Tool Panel** dialog box.
Password	6-256	• Alphanumeric (ASCII code) characters • All symbols You cannot use the quotation mark (") or backslash (\) symbols when you enter a password in a screen from the **Tool Panel** dialog box.

Note: If you cannot log in on a **Tool Panel** dialog box screen, check to see if you have used a number sign (#) in the user name, or used a quotation mark (") or a backslash (\) in the password.

User name and password for logging in to SVP

Item	Length in characters	Characters that can be used
User name	1-128	• Alphanumeric (ASCII code) characters

Item	Length in characters	Characters that can be used
		• The following symbols: ! # $ % & ' - . @ ^ _ ` { } ~
Password	6- 127	• Alphanumeric (ASCII code) characters • All symbols

User name and password for logging in to CCI

Item	Length in characters	Characters that can be used
User name	1-63	• Alphanumeric (ASCII code) characters • The following symbols*: - . @ _
Password	6- 63	• Alphanumeric (ASCII code) characters • The following symbols*: - , . @ _
*When you use a Windows computer for CCI, you can also specify a backslash (\). When you use a UNIX computer for CCI, you can also specify a slash (/).		

User name and password for logging in to NAS Manager

Item	Length in	Characters that can be used
User name	1-20	• Alphanumeric (ASCII code) characters • The following symbols*: - . _
Password	6-256	• Alphanumeric (ASCII code) characters • All symbols: - . _
* Do not specify a user name consisting of periods (.) (..) only, or specify a user name beginning with a hyphen (-). If you specify such names, you cannot log in to NAS Manager.		

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.

Before you begin

- 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.

Before you begin

- 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.

Adding a user

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 add or remove users.

   To add users to the selected groups:

   a. Click **Add Users**.
   b. In the **Add Users** window, select a user and click **Add**.

   To remove users from the selected groups:

   a. In the **Remove Users** window, select one or more users.
   b. Click **More Actions > Remove Users**.
3. Click **Finish**.
4. In the **Confirm** window, check the settings. If the **Task Name** field is empty, enter a task name.
5. Click **Apply**. The task is now registered. If you selected the **Go to tasks window for status** check box, the **Task** window opens to show the status of the task.

Enabling or Disabling user accounts

Security Administrators can disable a user account to prevent the user from logging in to Device Manager - Storage Navigator and NAS Manager temporarily. Security Administrators can also enable a user account to allow the user to log in to Device Manager - Storage Navigator and NAS Manager.

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.

To allow or prevent a user from logging in to Device Manager - Storage Navigator and NAS Manager, follow the steps below.

Before you begin

- Log into an account that is different from the user whose account that you want to enable or 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.
   - To allow the user to log in to Device Manager - Storage Navigator and NAS Manager, click **Enable**.
   - To prevent the user from logging in to Device Manager - Storage Navigator and NAS Manager, 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.

Before you begin

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.

Before you begin

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
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

Role	Capabilities
	• 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 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*.

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
Support Personnel	• Storage Administrator (Initial Configuration) • Storage Administrator (System Resource Management) • Storage Administrator (Provisioning)	All Resource Groups Assigned

Built-in group	Role	Resource group
	• Storage Administrator (Performance Management) • Storage Administrator (Local Copy) • Storage Administrator (Remote Copy) • Support Personnel	

Related tasks

- Checking if a role is available to a user group on page 158

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.

Before you begin

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.

Before you begin

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 156

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.

Before you begin

- 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.

Before you begin

- 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.

Before you begin

- 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.

Before you begin

- 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

This section explains how to delete a user group when it is no longer needed.

Before you begin

- 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.

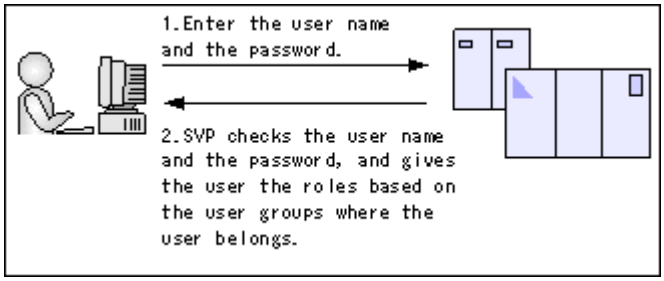
Procedure

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**.

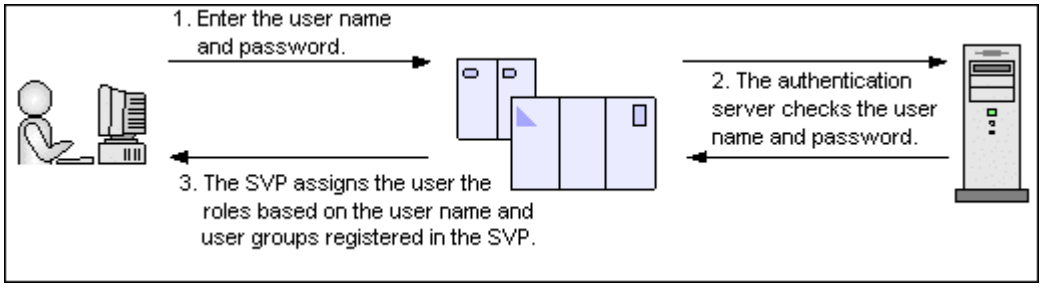
Using an authentication server and authorization server

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 the login workflow without an authentication server:

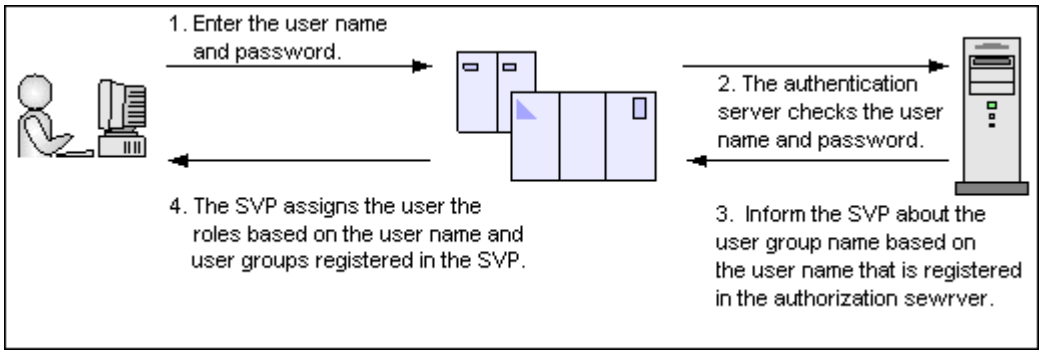


The following figure shows the login workflow with an authentication server:



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 the login workflow when an authentication server and an authorization server are used in combination:



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.

Before you begin

- 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. Create a configuration file. The items to specify depend on the protocol you use.
2. Log in to the SVP and store the following files in an easily accessible location.
   - Certificate (for secure communication)
   - Configuration file
3. Open the Windows command prompt on the SVP.
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. 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.

Caution: If you save the configuration file when using the Windows standard Notepad application, specify ANSI for the letter code. If you use an editor other than the memo pad and have the YTF-8 BOM setting, specify No BOM then save.

```
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

Attribute	Description	Required / Optional	Default value
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 times out. It must be between 1 and 30.[2]	Required	10
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	Required	None

Attribute	Description	Required / Optional	Default value
	• Flat model: An attribute name for a user entry's RDN sAMAccountName is used for Active Directory.		
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 searched with the information registered in the SRV records by specifying "true".	Optional	False

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.

Attribute	Description	Required / Optional	Default value
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.

Caution: If you save the configuration file when using the Windows standard Notepad application, specify ANSI for the letter code. If you use an editor other than the memo pad and have the YTF-8 BOM setting, specify No BOM then save.

```
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 6 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 7 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.

Caution: If you save the configuration file when using the Windows standard Notepad application, specify ANSI for the letter code. If you use an editor

other than the memo pad and have the YTF-8 BOM setting, specify No BOM then save.

```
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 8 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

Attribute	Description	Required / Optional	Default value
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
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 9 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

Attribute	Description	Required / Optional	Default value
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
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.

Attribute	Description	Required / Optional	Default value
• 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 162

Related tasks

- Connecting authentication and authorization servers on page 165

User Administration for NAS Manager

This section describes various user roles, permissions and groups available to manage your storage system. You use NAS Manager to create and manage SMU user accounts on your storage system.

Administrator types and responsibilities

This section describes the types of NAS storage system administrators and defines their expected roles in managing the system and the associated storage subsystems.

- **Global Administrators** can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server+Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access.
- **Storage Administrators** manage storage devices, as specified in the administrator profile created by the Global Administrator.

  Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users.
- **Server Administrators** manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices.

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

- **Server+Storage Administrators** manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator.
  Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components.

All administrators can connect to the NAS storage system through NAS Manager, the browser-based management utility provided by the system management unit (SMU). Additionally, Global Administrators can connect to the SMU command line interface (CLI).

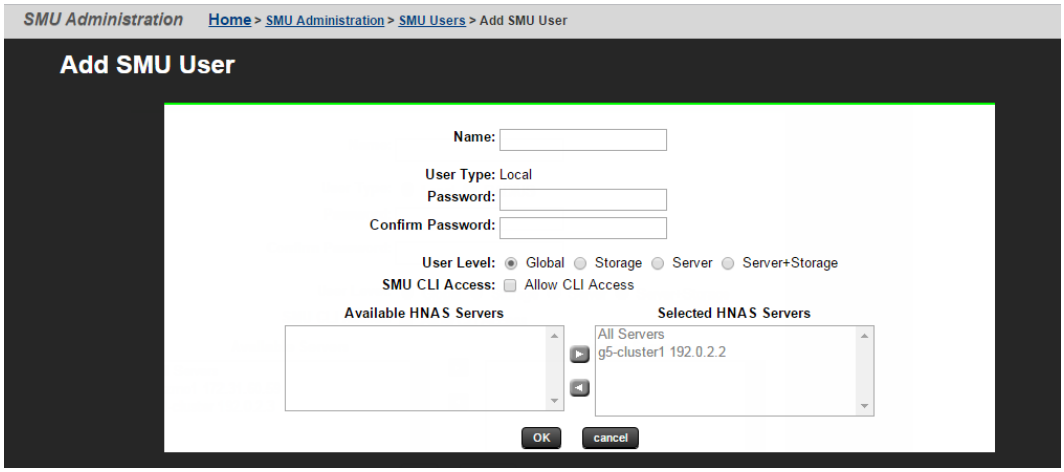
Note: Server Administrators, Storage Administrators, and Server+Storage Administrators are not able to access all of the NAS Manager pages that a Global Administrator can access.

Adding an SMU user (an administrator)

To add an SMU user (a NAS storage system administrator):

Procedure

1. Navigate to **Home > SMU Administration > SMU Users > SMU Users** to display the **SMU Users** page.
2. Click **add** to display the **Add SMU User** page:



Field/Item	Description
Name	The name of the new user account. This name will be requested when logging in to the SMU. The rules for user names are: • For Global administrators only, if the user will access the SMU through the CLI, the user name:

Field/Item	Description
	○ Must start with a letter or an underscore, and may consist of up to 31 alphanumeric characters and the underscore (_) and the hyphen (-). ○ Cannot match certain special purpose names: root, manager, postgres, nobody, or nfsnobody. ○ Cannot match certain special purpose user ID numbers: for example, those with uid less than 502. • For all types of administrators, if the user will access the SMU only through NAS Manager, the user name may consist of alphanumeric characters and/or the underscore (_), the hyphen (-), the equal sign (=), parentheses "(" or ")", brackets ([or]), the pound sign (#) and the exclamation point (!). • **Supervisor** is a reserved system user name. It is not available as a new user name. **Note:** If you are using RADIUS realms, and the global administrator will access the SMU using both NAS Manager and the CLI, use the underscore (_) to combine the user name and the realm: for example, `johnsmith_realm2`. If the global administrator will access the SMU using only NAS Manager, you can use the at sign (@) to combine the user name and the realm: for example, `johnsmith@realm3`.
User Type	The user type. User types are either **local** or **RADIUS**. • Local users are those whose passwords are locally defined and authenticated in the SMU. • RADIUS users are those whose passwords are defined and authenticated in an external RADIUS servers. The RADIUS administrator must add a user name and password to all RADIUS servers.
Password	Enter the password that will be used when this user account logs in. The password cannot exceed 256 characters. This field only applies when the User Type is selected to Local. It does not apply when the RADIUS User Type is selected.
Confirm Password	Confirm the password entered in the previous field by entering it in again. Only applies when the Local User type is selected.
User Level	Specify the level for the new administrator that you are creating. You can select any one of the following: • **Global Administrators** can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server+Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access. • **Storage Administrators** manage storage devices, as specified in the administrator profile created by the Global Administrator. Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users.

Field/Item	Description
	• **Server Administrators** manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices. Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules. • **Server+Storage Administrators** manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator. Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components. **Note:** Server Administrators, Storage Administrators, and Server+Storage Administrators are not able to access all of the NAS Manager pages that a Global Administrator can access.
SMU CLI Access (for Global Administrators only)	If the administrator is allowed to log in and access the SMU CLI of an external SMU, select the **SMU CLI Access** check box.
Available HNAS Servers	For Server administrators, Storage administrators, and Server+Storage administrators, lists the servers managed by the SMU to which the administrator has not yet been given management privileges. Not available for Global administrators, because Global administrators are allowed to manage all storage and all servers.
Selected HNAS Servers	For Server administrators, lists the servers that the administrator can manage. Note that a Server administrator cannot manage the storage attached to these servers. Not available for Global administrators, because Global administrators are allowed to manage all storage and all servers. For Storage administrators, lists servers that have attached storage that the administrator can manage. Note that a Storage administrator cannot manage these servers, only the storage attached to these servers. For Server+Storage administrators, lists servers that the administrator can manage. The Server+Storage administrator can also manage the storage attached to these servers.
OK	When the profile is complete and correct, click **OK** to save and enable the user profile, and then return to the **SMU Users** page.
cancel	Closes the page without saving the profile, and returns to the **SMU Users** page.

3. Enter the user name for the new administrator in the **Name** field.
4. Specify if the administrator login is authenticated locally (by the SMU) or by a RADIUS server by selecting the appropriate **User Type**.

Note: If you are authenticating this user through a RADIUS server, the **Password** and **Confirm Password** fields will not be available, and you should skip the next two steps, but you must enter the user passwords into the RADIUS server using the tools available for that server.

5. If the **User Type** is local, enter the password for the new administrator in the **Password** field.
6. If the **User Type** is local, confirm the password for the new administrator in the **Confirm Password** field.
7. Specify the initial login password for the user by filling in the **Password** and the **Confirm Password** fields.
8. Specify the user level for the new administrator that you are creating.

   You can select one of the following:
   - **Global Administrator**
   - **Storage Administrator**
   - **Server Administrator**
   - **Server+Storage**
9. For Global Administrators only, if the administrator is allowed to log in and access the SMU command line interface (CLI) of an external SMU, select the **SMU CLI Access** check box.
10. Using the **Available Servers** and the **Selected Servers** lists, specify the servers the administrator can access or the servers with the storage the administrator can manage.
    - To grant management privileges for a server or the storage attached to a server, move the server from the **Available Servers** list to the **Selected Servers** list.
    - To revoke management privileges for a server or the storage attached to a server, move the server from the **Selected Servers** list to the **Available Servers** list.
    - To move the server between the **Available Servers** and the **Selected Servers** lists, select the server, and use the arrow buttons between the lists.
11. Review the profile, and verify that it is correct.
    - If the profile is correct, click **OK** to save and enable the user profile, and then return to return to the **SMU Users** page.
    - To return to the **SMU Users** page without saving the profile, click **back**.

Changing the password for a currently logged in user

Note: If the user is authenticated through a RADIUS server, you cannot change their password using NAS Manager or the SMU CLI, you must change it using the tools/utilities for the RADIUS server.

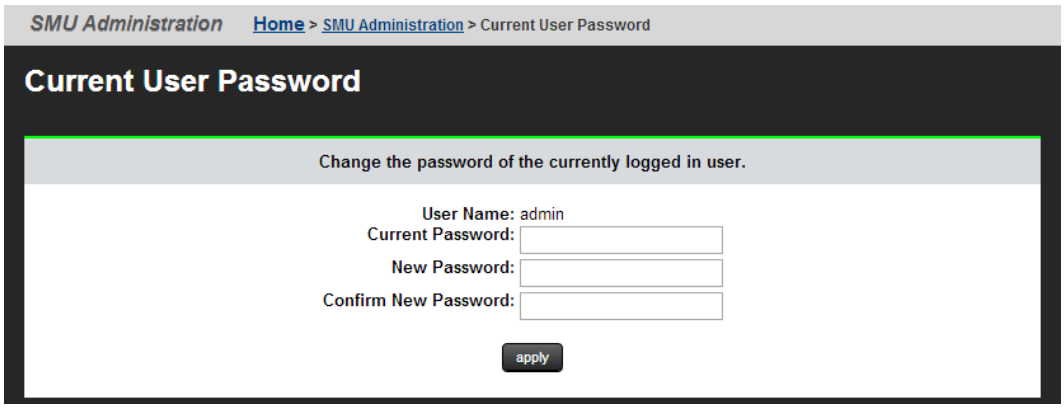
Any logged in user can change their own password. A global administrator can also change the password of any user, whether the user is currently logged in or not.

Changing your own password

Note: If your log in is authenticated through a RADIUS server, you cannot change their password using NAS Manager, you must change it using the tools/utilities for the RADIUS server.

Procedure

1. Navigate to **Home > SMU Administration > Current User Password** to display the **Current User Password** page.



The following table describes the fields on this page:

Field/Item	Description
User Name	Displays your user login name (cannot be changed).
Current Password	Displays a series of dots representing the currently specified password (the actual password cannot be displayed).
New Password	The new password. The password cannot exceed 256 characters.
Confirm New Password	The new password again. Must be exactly the same as what you entered in the **New Password** field.
apply	Saves the new password.

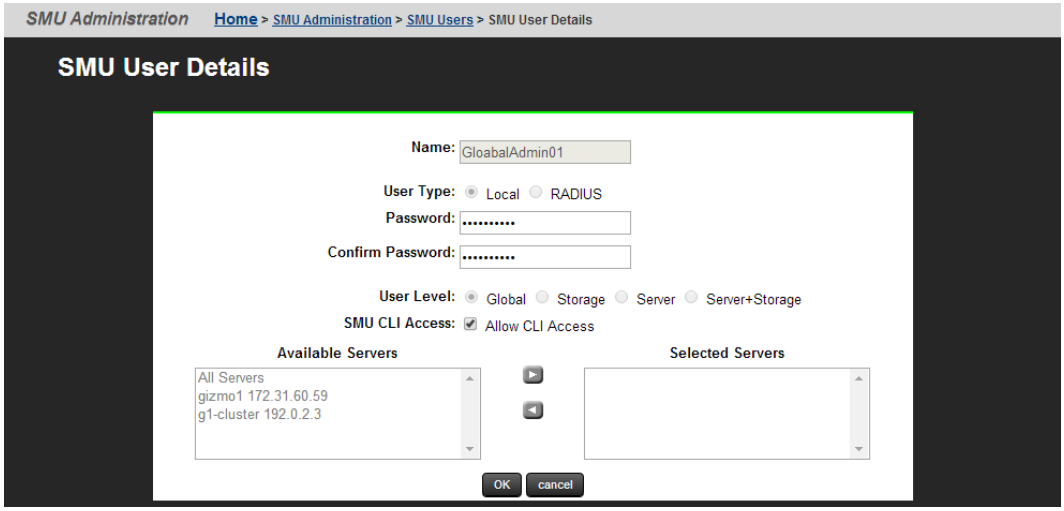
2. Enter your current password in the **Current Password** field.
   If you have forgotten you password, contact a global administrator and ask them to give you a new password. (Passwords are stored in an encrypted form, and are not retrievable or visible by anyone. If a user forgets their password, they must be given a new password, which they can then change.)
3. Enter your new password in the **New Password** field.

4. Enter the new password again in the **Confirm New Password** field.
5. When finished, click **apply** to save the new password.

Changing another user's password

Procedure

1. Navigate to **Home > SMU Administration > SMU Users** to display the **SMU Users** page.
2. Click **details** to display the **SMU User Details** page.



Item/Field	Description
Name	Administrator's user name. Cannot be changed.
User Type	Describes if the user is authenticated by the SMU itself (local users), or if the user is authenticated by a RADIUS server.
Password and Confirm Password	For users authenticated by the SMU only (local users). These fields do not apply for users authenticated by a RADIUS server. The password for the user. Characters are hidden, and the exact same password must be entered in both fields. The password cannot exceed 256 characters.
User Level	Displays the user level or type of administrative role. • **Global Administrators** can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server+Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access. • **Storage Administrators** manage storage devices, as specified in the administrator profile created by the Global Administrator.

Item/Field	Description
	Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users. • **Server Administrators** manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices. Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules. • **Server+Storage Administrators** manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator. Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components. • If the User Type is Local, you can modify the password. • If the User Type is RADIUS, you cannot modify the password, because the password is managed on RADIUS servers. • If the User Level is Global, you can select or clear the **Allow CLI Access** check box. • If the User Level is server, storage, or server+storage, you can add or remove servers from the user's scope of management. Global users implicitly have access to manage all servers and storage. Non-global users cannot be given CLI access. You cannot change the User Type or User Level of a user. If such a change is needed, delete the old user and create a new user.
SMU CLI Access	For global administrators only, when the check box is selected, the administrator can access the SMU using the CLI as well as NAS Manager.
Available HNAS Servers	Not available for global administrators, because global administrators are allowed to manage all storage and all servers. For server administrators, storage administrators, and server +storage administrators, lists the HNAS servers managed by the SMU to which the administrator has not yet been give management privileges. The "All Servers" entry is used to allow privileges to all servers managed by the SMU.
Selected HNAS Servers	Not available for global administrators, because global administrators are allowed to manage all storage and all servers. For server administrators, lists the HNAS servers that the administrator can manage. Note that a Server administrator cannot manage the storage attached to these servers. For storage administrators, lists HNAS servers that have attached storage that the administrator can manage. Note that a storage

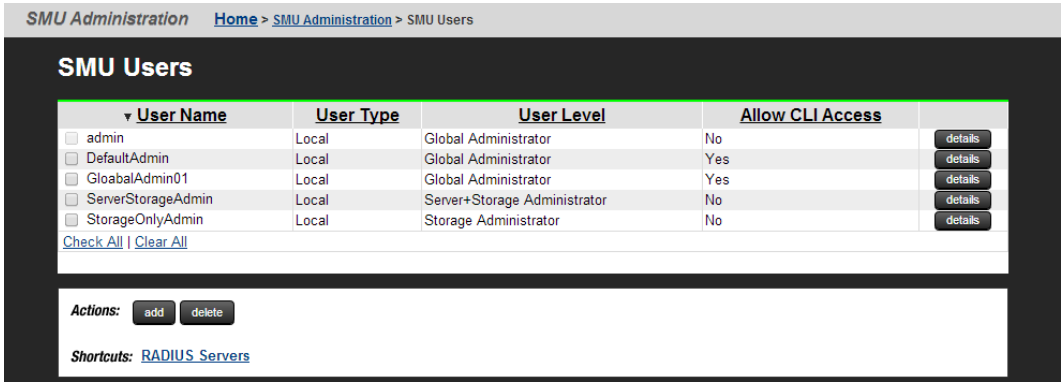
Item/Field	Description
	administrator cannot manage these servers, only the storage attached to these servers. For server+storage administrators, lists HNAS servers that the administrator can manage. The server+storage administrator can also manage the storage attached to these servers.
OK	Saves the currently defined user profile and returns to the **SMU Users** page.
Cancel	Returns to the **SMU Users** page without saving the profile.

3. Enter the new password in the **Password** field.
4. Enter the new password again in the **Confirm Password** field.
5. When finished, click **OK** to save the new password.

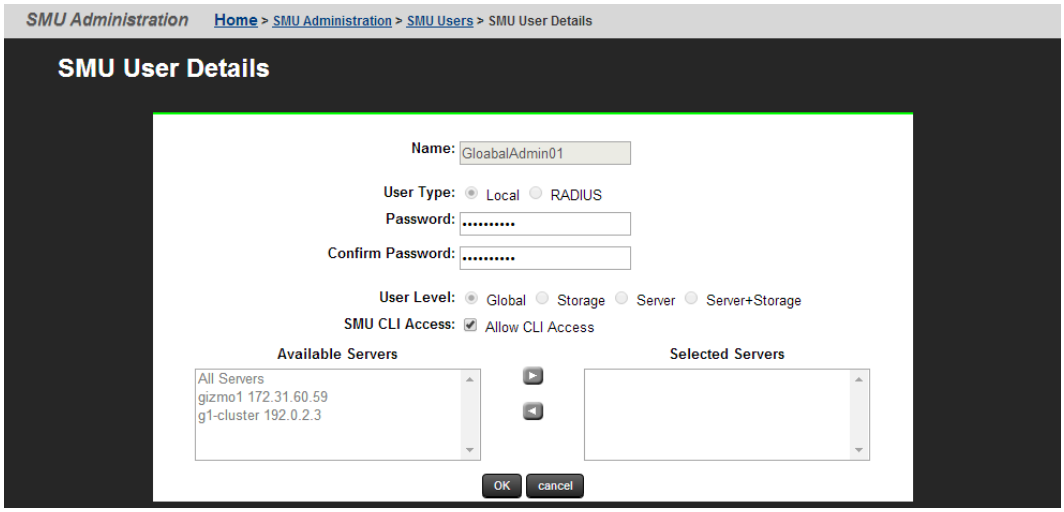
Changing an SMU user profile

Procedure

1. Navigate to **Home > SMU Administration > SMU Users** to open the **SMU Users** page.



2. Click **details** to display the **SMU User Details** page for the user whose profile you want to modify.



Item/Field	Description
Name	Administrator's user name. Cannot be changed.
User Type	Describes if the user is authenticated by the SMU itself (local users), or if the user is authenticated by a RADIUS server.
Password and Confirm Password	For users authenticated by the SMU only (local users). These fields do not apply for users authenticated by a RADIUS server. The password for the user. Characters are hidden, and the exact same password must be entered in both fields. The password cannot exceed 256 characters.
User Level	Displays the user level or type of administrative role. • **Global Administrators** can manage everything in the system: file systems, file services, or file system related features and functions, storage devices and their components. Also, the Global Administrator creates and manages SMU user profiles (Server Administrators, Storage Administrators, Server+Storage Administrators, and other Global Administrators). Global Administrators also control what servers and storage devices each administrator can access. • **Storage Administrators** manage storage devices, as specified in the administrator profile created by the Global Administrator. Storage Administrators can manage only storage devices and their components (racks, physical disks, SDs, and storage pools). Storage Administrators cannot manage file systems, file services, or file system related features and functions, and they cannot manage users. • **Server Administrators** manage servers and clusters, as specified in the administrator profile created by the Global Administrator. Server Administrators cannot manage storage devices. Server Administrators can manage file systems and file services such as CIFS Shares, NFS Exports, and they can manage file system related features and functions such as snapshots, quotas, and migration policies and schedules.

Item/Field	Description
	• **Server+Storage Administrators** manage servers, clusters, and storage devices, as specified in the administrator profile created by the Global Administrator. Server+Storage administrators can manage everything Server Administrators and Storage Administrators can manage: file systems, file services, or file system related features and functions, and they can also manage storage devices and their components. • If the User Type is Local, you can modify the password. • If the User Type is RADIUS, you cannot modify the password, because the password is managed on RADIUS servers. • If the User Level is Global, you can select or clear the **Allow CLI Access** check box. • If the User Level is server, storage, or server+storage, you can add or remove servers from the user's scope of management. Global users implicitly have access to manage all servers and storage. Non-global users cannot be given CLI access. You cannot change the User Type or User Level of a user. If such a change is needed, delete the old user and create a new user.
SMU CLI Access	For global administrators only, when the check box is selected, the administrator can access the SMU using the CLI as well as NAS Manager.
Available HNAS Servers	Not available for global administrators, because global administrators are allowed to manage all storage and all servers. For server administrators, storage administrators, and server +storage administrators, lists the HNAS servers managed by the SMU to which the administrator has not yet been give management privileges. The "All Servers" entry is used to allow privileges to all servers managed by the SMU.
Selected HNAS Servers	Not available for global administrators, because global administrators are allowed to manage all storage and all servers. For server administrators, lists the HNAS servers that the administrator can manage. Note that a Server administrator cannot manage the storage attached to these servers. For storage administrators, lists HNAS servers that have attached storage that the administrator can manage. Note that a storage administrator cannot manage these servers, only the storage attached to these servers. For server+storage administrators, lists HNAS servers that the administrator can manage. The server+storage administrator can also manage the storage attached to these servers.
OK	Saves the currently defined user profile and returns to the **SMU Users** page.
Cancel	Returns to the **SMU Users** page without saving the profile.

3. Edit the SMU user password.

Note: For users authenticated by the SMU only (local users), not available for users authenticated by a RADIUS server.

To edit the user's password, type the new password in the **Password** and **Confirm Password** fields.

4. For global administrators only, allow or disallow SMU CLI access.

   When the check box is selected, the administrator can access the SMU by using the CLI as well as NAS Manager.

5. Specify server and/or storage management rights.
   - To grant management privileges for a server or the storage attached to a server, move the server from the **Available Servers** list to the **Selected Servers** list.
   - To revoke management privileges for a server or the storage attached to a server, move the server from the **Selected Servers** list to the **Available Servers** list.
   - To move the server between the **Available Servers** and the **Selected Servers** lists, select the server, and use the arrow buttons between the lists.
6. Click **OK** to save the profile and return to the **SMU Users** page.

SMU user authentication

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

Active Directory users are assigned full access rights to the SMU functionality.

For *local and RADIUS* users the user profile details are specified when the user account is created.

The user profile:

- Indicates if the user is to be authenticated locally,or through a RADIUS server.
- Specifies the user's access (privilege) level, meaning it specifies if the user is a:
  - Global administrator.
  - Storage administrator.
  - Server administrator.
  - Server+Storage administrator.
- Specifies the servers the user is allowed to access.

- Specifies if the user has CLI access (for RADIUS and Local Users).

Active Directory user authentication

Active Directory is an LDAP-compliant hierarchical database of objects. It is very popular in enterprise environments and is becoming a de facto standard for user authentication.

After Active Directory connection settings and groups have been configured for the SMU, it will allow logins from enabled users who supply their Active Directory name and password. This is typically the same name and password that the user would use to log into Windows and other enterprise applications. Unlike SMU local and RADIUS user names, Active Directory user names are case-insensitive. Active Directory passwords are case-sensitive and cannot be changed from the SMU; they are maintained in the Active Directory server.

There are a number of benefits for SMU users. The administrator does not need to maintain a separate set of user details, because the SMU can just make use of the Active Directory enterprise user database. Users can login using their usual name and password instead of having to remember a separate set of credentials for the SMU. And instead of configuring access for individual users, the SMU administrator just has to specify the Active Directory *groups* whose members have login rights.

It is possible to assign more restrictive user levels and managed severs to Active Directory users according to their group membership. So it is possible to define a group of users who have only *server* level access, for example, or access to a restricted set of managed HNAS servers.

Although the SMU supports RADIUS and Active Directory for external authentication, they are mutually exclusive; it is not possible to have them both configured for external authentication at the same time.

When a login attempt is made, the SMU first tries to authenticate the credentials as a local user. If that fails, and Active Directory is configured, they are authenticated as an Active Directory user.

Active Directory authentication requests are sent to servers in the configured sequential order. If a successful connection cannot be made to the first server, it attempts to contact the second server and so on. When a connection is made and an authentication response received (either positive or negative) it is treated as definitive. It does not then contact further servers because all servers are assumed to have identical content.

Using Transport Layer Security (TLS) with Active Directory authentication

TLS is a cryptographic protocol which provides security between applications over a network.

For Active Directory authentication, the SMU supports up to TLS 1.2. It negotiates with the domain controller to use the highest version of TLS which is common to both.

The SMU requires domain controllers to respond on port 389. It is not possible to configure the SMU to use any other port.

Configuring Active Directory servers

Global Administrators can provide information to configure, modify, and list Active Directory servers for authentication on the **Active Directory Servers** page.

Before you begin

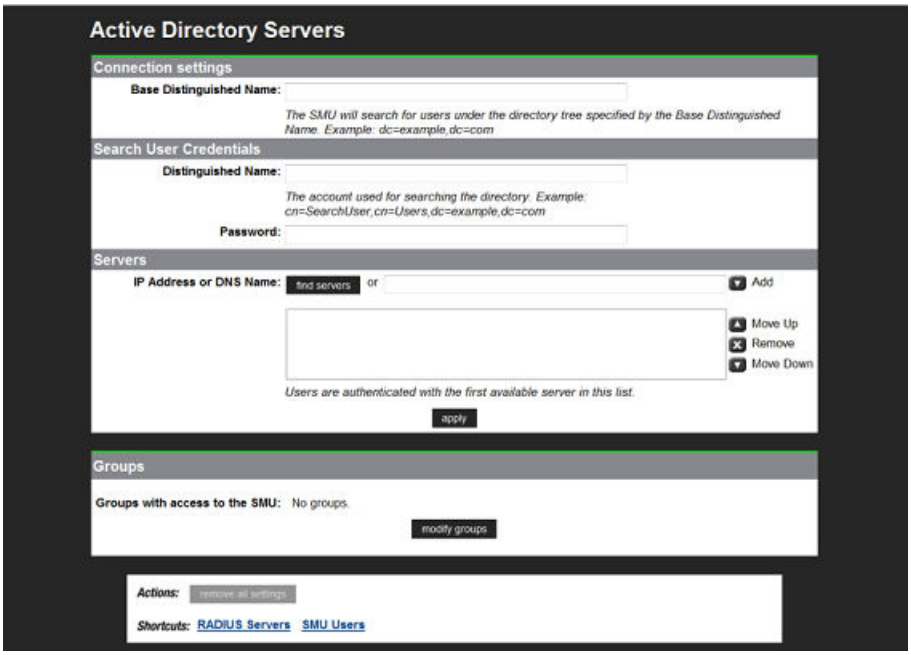
In order to enable Active Directory use, the SMU administrator needs to know the following information:

- The domain in which the Active Directory users and groups that will access the SMU are located.
- The LDAP distinguished name and password of an Active Directory user that has read access to users and groups on the Active Directory servers. This is referred to as the Search User. The user can search for users or groups under the supplied base distinguished name.
- The addresses of one or more Active Directory servers that maintain the users and groups for the domain. The content of all configured servers must be identical. If DNS servers have been configured for the SMU, then the SMU should be able to automatically discover these server addresses via the **find servers** button on the setup page. SRV records must be setup in order for **find servers** to find the Active Directory servers.
- The Active Directory group or groups whose members are to be given the right to log into the SMU.
- If RADIUS was previously in use and it is to be replaced by Active Directory, then the RADIUS configuration must first be removed before Active Directory can be configured. This is done from the **Home>SMU Administrator>RADIUS Servers** page by clicking the **remove all settings** button. No RADIUS user will be able to log into the SMU after this is done.

Procedure

1. Navigate to **Home > SMU Administrator** to display the **Active Directory Servers** page.
2. Enter the **Base Distinguished Name**.

   This name must be entered in LDAP distinguished name (DN) format which consists of a sequence of "attribute=value" pairs separated by comma or semi-colon. The Base Distinguished Name should contain the domain component (dc) attributes for the organization's domain. So for the domain *example.com* it would be "*dc=example, dc=com*". The name may also contain organization unit (ou) attributes.



The following table describes the fields on this page:

Field/Item	Description
Connection settings	
Base Distinguished Name	The LDAP root location for users and groups. The name is recommended to contain just the domain components.
Search User Credentials	
Distinguished Name	The LDAP distinguished name for a user that has search capabilities.
Password	The password for the search user.
Servers	
IP Address or DNS Name	The address of one or more Active Directory servers for the domain. Each server should hold identical content. The maximum number of servers is 20.
find servers	Queries DNS to show the list of available Active Directory servers for the domain.
Add	Add an Active Directory server after you have entered its fully qualified domain name or IP address.
Move Up **Move Down**	If there is more than one server, use these buttons to prioritize the list.
Remove	Remove a server from the list.

Field/Item	Description
apply	Submit the page and save the connection settings and server list to the SMU database.
Groups	
Groups with access to the SMU	Shows groups with access to the SMU. Active Directory users who belong to these groups can access the SMU.
Modify groups	Click to go to the **Active Directory Groups** page, where you can add groups.
Actions	
remove all settings	Removes all Active Directory server settings, including server list, connection settings, search user credentials and groups. After this action, Active Directory users can no longer log into the SMU.

3. Enter the **Distinguished Name**.

   This is the Distinguished Name of the Search User, an existing user that has permission to access Active Directory. An Search User DN would typically contain common name (cn) and possibly organization unit (ou) attributes as well as the domain components. The domain components should match those used in the Base Distinguished Name. An example Search User DN is "*cn= ldapguest, cn=users, dc=example, dc=com".*
4. Enter the **Password** of the Search User (an existing user that may access the directory).
5. There are two ways to add Active Directory servers.
   - Enter the fully qualified domain name or IP address of the server, and click **Add**.
   - Click **find servers**.The list of discovered servers is displayed.

     Note: The DNS server or servers must be configured for the SMU (under Name Services) for **find servers** to work.

     - Select one or more servers and click **add** to add them to the list. No more than 20 Active Directory servers can be configured at a time.
     - When you are finished, click **close** to return to the **Active Directory Servers** window.



6. If there is more than one server, the list can be prioritized using **Move Up** or **Move Down** .
7. Click **Apply** to submit this page and save the connection settings and server list to the SMU database.
   The SMU will perform a connection test to check that it can access the configured servers with the supplied details and display a warning if the SMU cannot, giving the user the opportunity to modify the settings or to save them as they are.

   Any information, warnings and errors related to Active Directory configuration or authentication are logged to `/var/opt/smu/log/mgr/mgr.log` and `/var/opt/smu/log/mgr/security.log`

Configuring Active Directory groups

In order to allow Active Directory users to log into the SMU, it is necessary to configure one or more groups. Once a group has been added and saved, all users who are members of that group will be able to log into the SMU using their Active Directory name and password. Active Directory users belonging to the subgroups of the configured group will also have SMU access.

Before you begin

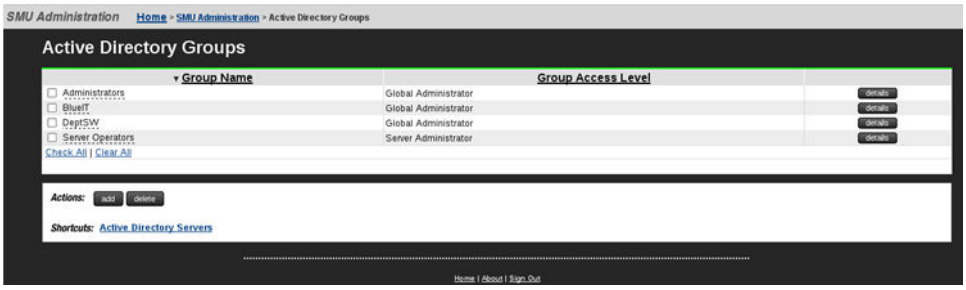
Note that the administrator is only able to configure groups after Active Directory servers have been added on the **Active Directory Servers** page.

Procedure

1. Navigate to the **Home > SMU Administrator > Active Directory Groups** to display the **Active Directory Groups** page.
   This page shows all Active Directory groups that have been added. Note that Active Directory groups can be associated with a group access level. For example, it is possible to define a group of users who only have *server* level of access. Any groups that were added in a previous version of the SMU that has been upgraded will be displayed in this list with a User Level of *Global Administrator*.

   If an Active Directory user is member of more than one configured groups in the SMU, then their access level will be derived by combining

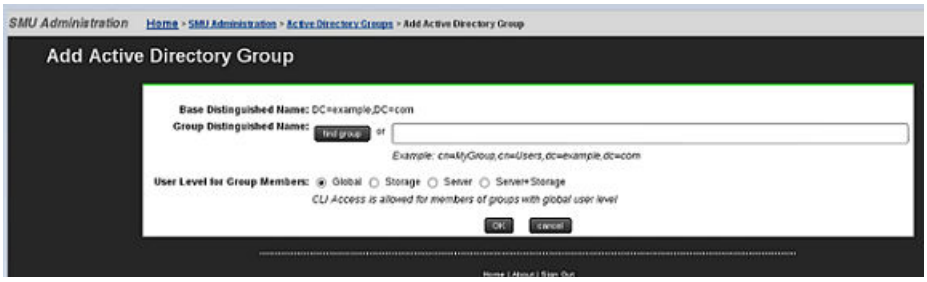
the access level for all configured Active Directory groups. For example, if a user is a member of one group defined with *storage* level, but is also a member of a group with *server* level, then that user will have *server +storage* access to the SMU.



The following table describes the fields on this page:

Field/Item	Description
Group Name	Group name is the user-friendly name of an Active Directory group existing on the Active Directory server. The full distinguished name for a group can be viewed by hovering the mouse over the group name. The sort order of the table can be changed by clicking over a column heading.
Group Access Level	Shows the group access level. This defines the access level given to Active Directory users who are members of the group when they log onto the SMU. On an external or virtual SMU, if the Group Access Level is **Global**, then group members are given SMU CLI access. SMU CLI access is not available on an embedded SMU or a NAS module SMU.
details	Click the **details** button in the right-hand column to view details of the associated group.
Check All	Checks all boxes under **Group Name**.
Clear All	Clears all checked boxes under **Group Name**.
add	Click to add a group. Takes you to the **Add Active Directory Group** page.
delete	Existing groups can be deleted by checking the box in left-hand column and clicking the **delete** button. The user is asked for confirmation before deleting. If all groups are being deleted, the user is warned that no Active Directory users will be authenticated.
Active Directory Servers	Takes you to the **Active Directory Servers** page.

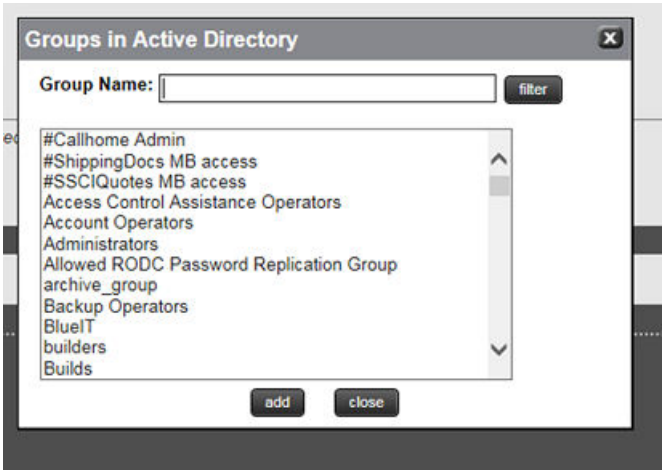
2. Click **add** and use the **Add Active Directory Group** page to add groups.



The following table describes the fields on this page:

Field/Item	Description
Base Distinguished Name	The LDAP root location for users and groups. The name is recommended to contain just the domain components.
Group Distinguished Name	The LDAP root location for users and groups. The name is recommended to contain just the domain components. Groups can be added manually by entering their distinguished name and then pressing the **OK** button. A maximum of 100 groups can be added. Alternatively, groups can be added by using the **find group** button.
find group	Queries the Active Directory to show the list of available groups. The list can be filtered by entering a partial group name. A maximum of 1000 group names is displayed.
User Level for Group Members	The user levels that can be assigned to group members are the same as those that can be assigned to local or RADIUS users and have the same meanings. The default is **Global**, but the level can be modified by selecting one of the other radio buttons.
OK	Click to save the group details. The SMU checks that the group exists in Active Directory. If the group does not exist (or if the SMU failed to access any AD server) the user is asked for confirmation that they still wish to save it. After saving the group, the updated group list page is displayed.
cancel	Cancels input.

3. There are two ways to add groups:
   - Enter the full Distinguished Name for the group (for example "*CN=Mygroup, CN=users, DC=example, DC=com*") and click the **add** button.
   - Click the **find group** button.
     - Groups that exist under this Base DN are displayed in a dialog window. The list can be filtered by entering a partial group name. A maximum of 1000 group names is displayed. Select a group from the list. Only one group can be added at a time.
     - Click **add** to add the group's distinguished name to this page.
     - Click **close** to return to the **Active Directory Groups** page without selecting a group from the list.



4. Select a User Level to be assigned to members of the group.

   CLI access is given to members of all groups defined with the **Global** level.

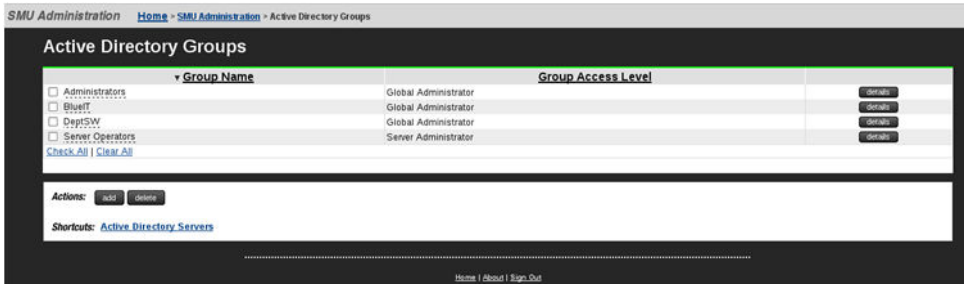
   Active directory users are given the same access level to all managed HNAS servers.

5. Click **OK** to save the group.

   The SMU will perform a test to check the group exists in Active Directory and displays warning if it is not, giving the user the opportunity to modify the group.

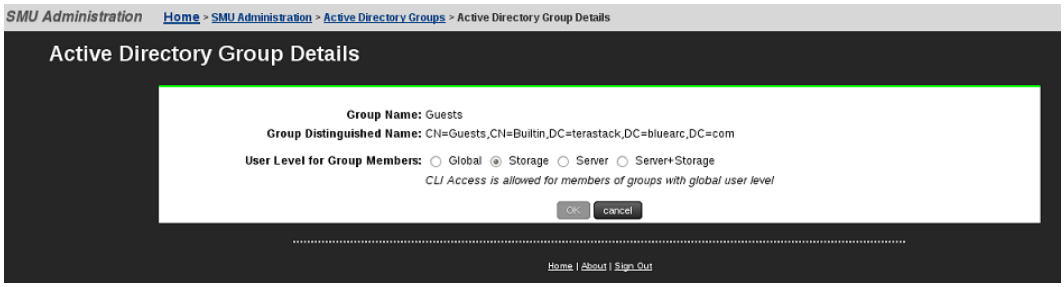
   Any information, warnings and errors related to Active Directory configuration or authentication are logged to `/var/opt/smu/log/mgr/mgr.log` and `/var/opt/smu/log/mgr/security.log`

   On returning to **Active Directory Groups** page, the current list of configured groups is displayed.



6. Click the **details** button in the right-hand column to view details of a previously defined group.

   When displaying the group details, the SMU checks that the group exists in Active Directory and displays a warning if it does not exist or if it could not access an Active Directory server. The user level cannot be modified once the group has been added. In order to modify the user level, the group would have to be deleted, then added again. Click the **cancel** button to return to the **Active Directory Groups** page.



The following table describes the fields on this page:

Field/Item	Description
Group Name	Name of group that details are provided for.

Field/Item	Description
Group Distinguished Name	The LDAP root location for users and groups. The name is recommended to contain just the domain components.
User Level for Group Members	The user levels that can be assigned to group members are the same as those that can be assigned to local or RADIUS users and have the same meanings. The default is **Global** , but the level can be modified by selecting one of the other radio buttons.
OK	No details can be modified for a group, so the **OK** button is disabled.
cancel	Returns to the **Active Directory Groups** page.

User authentication through RADIUS servers (HNAS server only)

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting management for computers to connect and use a network service.

RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The SMU acts as a RADIUS client component that communicates with the RADIUS server to validate logins. The RADIUS server is usually a background process running on a Unix or Microsoft Windows server.

RADIUS serves three functions:

- Authenticates users or devices before granting them access to a network.
- Authorizes those users or devices for certain network services.
- Accounts for usage of those services.

The RADIUS server compatibility is as follows:

- For IPv4 only, works with FreeRADIUS 2.1 or Windows 2003 Internet Authentication Service (IAS).
- For IPv6, requires FreeRADIUS 2.2 or Windows 2008 Network Policy Server (NPS).

Configuring user authentication through a RADIUS server requires the following:

- The RADIUS server must be set up and operational.
- The SMU must be able to communicate with the RADIUS server using the network.
- You must know the RADIUS server's:
  - IP address or DNS name.
  - Authentication port.
  - Shared secret for the SMU.

You can specify and prioritize multiple RADIUS servers for authentication.

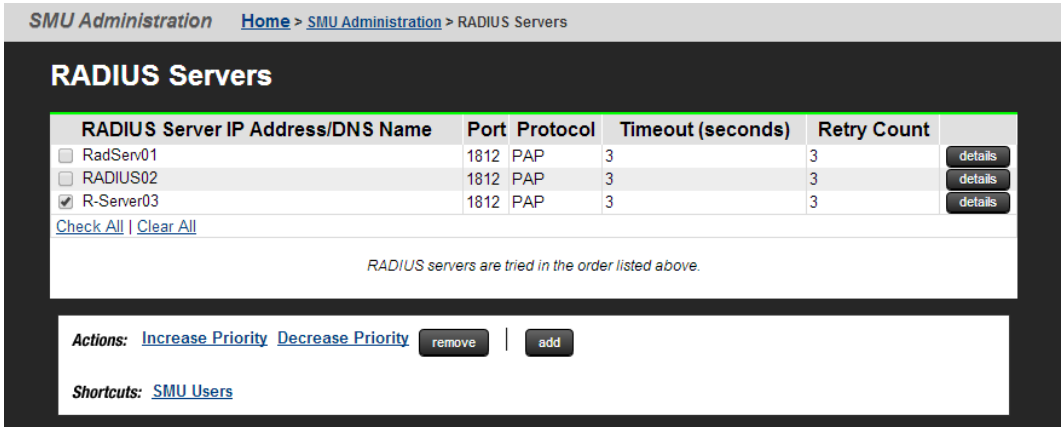
Note: The SMU contacts RADIUS servers in order of priority; the SMU will always try to contact higher priority servers before lower priority servers, and you cannot map SMU users to authenticate through a specific RADIUS server.

If you specify an incorrect secret or there are network problems that prevent the SMU from communicating with the highest priority RADIUS server, the SMU will try to contact the secondary RADIUS server, then the third RADIUS server, then the next server, until the SMU has tried to contact all the RADIUS servers in the list.

Displaying list of RADIUS servers

Procedure

Navigate to **Home > SMU Administration > RADIUS Servers**.



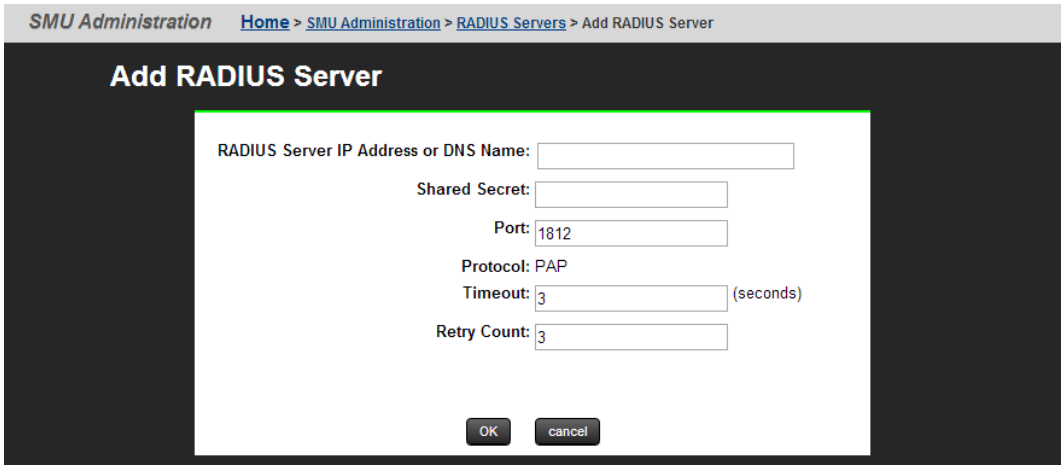
Field/Item	Description
RADIUS server IP address/DNS name	Specifies the RADIUS server IP address or DNS name. To connect with the RADIUS server, you must enter either an IP address or a DNS name. An IP address is preferred, both because it eliminates the dependency on the network DNS severs, and to improve login performance.
Port	The port number on which each server listens. **Note:** The default RADIUS server authentication port is 1812, but you should check with the RADIUS server administrator to make sure that 1812 is the correct port.
Protocol	The RADIUS server protocol. PAP is the default.
Timeout	Specifies the timeout count. The default is 3 seconds. The timeout is the number of seconds the SMU waits before retrying (retying is re-transmitting the authentication request to the same RADIUS server). If the timeout is reached and there is no response from the first RADIUS server in the list, the SMU attempts another retry.
Retry Count	Specifies the retry count. The default is 3. When the retry limit is reached, the SMU sends the request to the next RADIUS server in the list. When the retry limit for the second server is reached, the

Field/Item	Description
	SMU attempts to reach the next server in the list, until there are no more servers to try. If the timeout is reached, and there are no more servers to try, the user cannot be authenticated, and the login fails.
details	Displays the **RADIUS Server Details** page in which you can view the details of the selected RADIUS server.
Check All	Selects all of the RADIUS servers in the server list.
Clear All	Unselects any selected RADIUS servers in the server list.
Increase Priority and **Decrease Priority**	Click **Increase Priority** to increase the server priority. Click **Decrease Priority** to decrease the server priority. The SMU contacts RADIUS servers in order of priority; the SMU will always try to contact higher priority servers before lower priority servers, and you cannot map SMU users to authenticate through a specific RADIUS server. If you specify an incorrect secret or there are network problems that prevent the SMU from communicating with the highest priority RADIUS server, the SMU will try to contact the secondary RADIUS server, then the third RADIUS server, then the next server, until the SMU has tried to contact all the RADIUS servers in the list.
remove	Removes the selected RADIUS server.
add	Opens the **Add Server RADIUS** page where the properties of the new server account are defined.
remove all settings	Removes all RADIUS Servers settings.
SMU Users	Opens the **SMU Users** page where you can view and add new SMU users.

Adding a RADIUS server

Procedure

1. Navigate to **Home > SMU Administration > RADIUS Servers** to display the **RADIUS Servers** page.
2. Click **add** to display the **Add RADIUS Server** page.



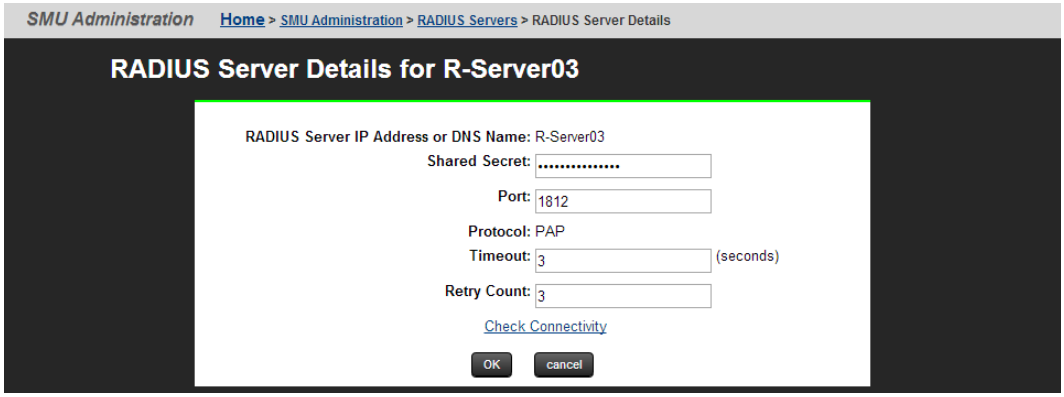
Field/Item	Description
RADIUS server IP address or DNS name	To connect with the RADIUS server, specify an IPv4 or IPv6 address, or a host name (host name is not recommended). An IP address is preferred, both because it eliminates the dependency on the network DNS sever(s), and to improve login performance. The **SMU Network Configuration** page (navigate to **Home > SMU Administration > SMU Network Configuration**) shows the active IP addresses. It is recommended that IPv4 on eth0 and the current IPv6 addresses be added to the "allowed client" list on each RADIUS server. For more information on setting up the SMU Network Configuration for IPv6, see the *Network Administration Guide*.
Shared Secret	Specify the shared secret. Some RADIUS Servers limit the length of the shared secret and require that it be comprised only of characters that can be typed on a keyboard which uses only 94 out of 256 possible ASCII characters. If the shared secret must be a sequence of keyboard characters, choose shared secrets that are at least 22 characters long and consisting of a random sequence of upper and lower case letters, numbers, and punctuation. • To ensure a random shared secret, use a computer program to generate a random sequence at least 22 characters long. Windows 2008 Server allows you to generate a shared secret when adding the RADIUS client. • The SMU will support a shared secret from 1 up to 128 characters. • Use a different shared secret for each RADIUS server-RADIUS client pair.
Port	Specify the RADIUS server authentication port. The default RADIUS server authentication port is 1812, but you should check with the RADIUS server administrator to make sure that 1812 is the correct port.
Protocol	The protocol for the RADIUS server.
Timeout	Specify the timeout, which is the number of seconds the SMU waits before retrying (retying is re-transmitting the authentication request

Field/Item	Description
	to the same RADIUS server). The default is 3 seconds. If the timeout is reached and there is no response from the first RADIUS server in the list, the SMU attempts another retry.
Retry Count	Specify the retry count. The default is 3. When the retry limit is reached, the SMU sends the request to the next RADIUS server in the list. When the retry limit for the second server is reached, the SMU attempts to reach the next server in the list, until there are no more servers to try. If there are no more servers to try, the user cannot be authenticated, and the login fails.
OK	When you are done making changes, click **OK** to test connectivity and save the configuration for this RADIUS server and return to the **RADIUS Servers** page.
cancel	Exits without saving the configuration.

Displaying details of RADIUS server

Procedure

1. Navigate to **Home > SMU Administration > RADIUS Server** to display the **RADIUS Server** page.
2. Select a RADIUS server, and click **details** to display the **RADIUS Server Details** page.



Field/Item	Description
RADIUS server IP address or DNS name	The RADIUS server IP address or DNS name.
Shared Secret	The shared secret, displayed with asterisks.
Port	The RADIUS server authentication port.
Protocol	Protocol associated with the RADIUS server.

Field/Item	Description
Timeout	The number of seconds the SMU waits before retrying (retrying is re-transmitting the authentication request to the same RADIUS server). If the timeout is reached and there is no response from the first RADIUS server in the list, the SMU attempts another retry.
Retry Count	When the retry limit is reached, the SMU sends the request to the next RADIUS server in the list. When the retry limit for the second server is reached, the SMU attempts to reach the next server in the list, until there are no more servers to try. If the timeout is reached, and there are no more servers to try, the user cannot be authenticated, and the login fails.
Check connectivity	Click to check the connectivity status of the RADIUS server.
OK	Saves configuration changes, and closes the page.
cancel	Closes the page without saving configuration changes.

5

Setting up security

This chapter describes how to set up security on your storage system.

- Working with certificates
- Configuring SMU security (NAS module only)

Working with certificates

A digital certificate can be thought of as an electronic passport that allows the SVP and storage system to exchange information securely over the Internet using the public key infrastructure (PKI).

You can use a Secure Sockets Layer (SSL) certificate, HCS certificate, or both to create a secure, encrypted connection between the SVP and the storage system.

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.

Before you begin

- 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.

Before you begin

- 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.

Managing SSL certificates

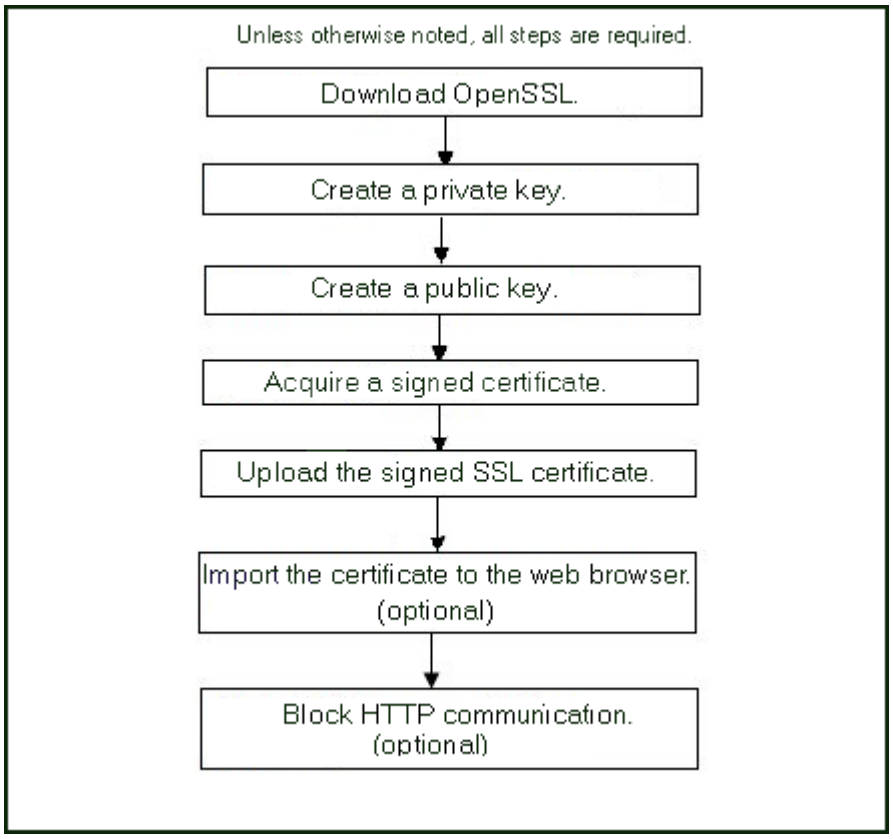
To improve the security of remote operations between the SVP and the storage system, you can set up a Secure Sockets Layer (SSL) encrypted connection between them.

SSL certificates (also known as digital certificates) are used to establish a secure encrypted connection between an SVP and a storage system. The SSL connection protects the Hitachi Device Manager - Storage Navigator User ID and password that is exchanged during each visit (or session).

SSL certificates consist of small data files that digitally bind a cryptographic key to an SVP's log on credentials. When installed on the SVP, SSL activates the padlock and the HTTPS protocol, allowing secure connections between the SVP and the storage system.

Flow of SSL communication settings

The following figure 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/).



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.

Before you begin

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.

Before you begin

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 208.
- 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 208.

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.

Before you begin

- 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.

Before you begin

- 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.

Before you begin

- 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.
- Updating the SSL certificate might change the system drastically and may lead to service processor failure. Therefore take sufficient care to consider 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 210 back to default.

Before you begin

- 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 206.
- 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 207.

- 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 208.
- 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.

Selecting a cipher suite

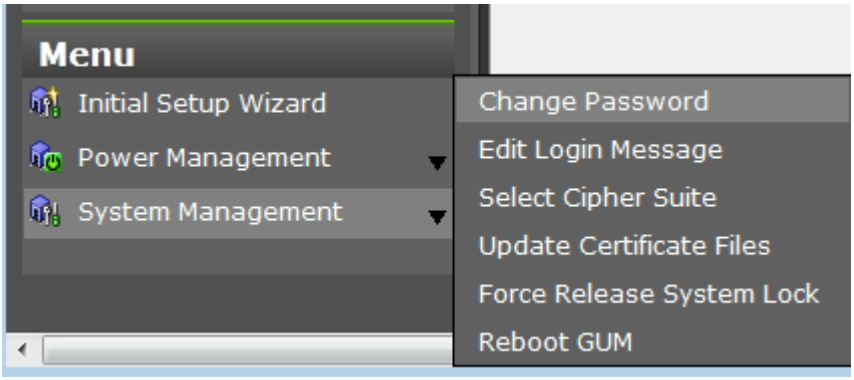
Cipher suites are part of SSL Version 3 and OSI Transport Layer Security Version 1 Cipher Specifications.

Before you begin

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.

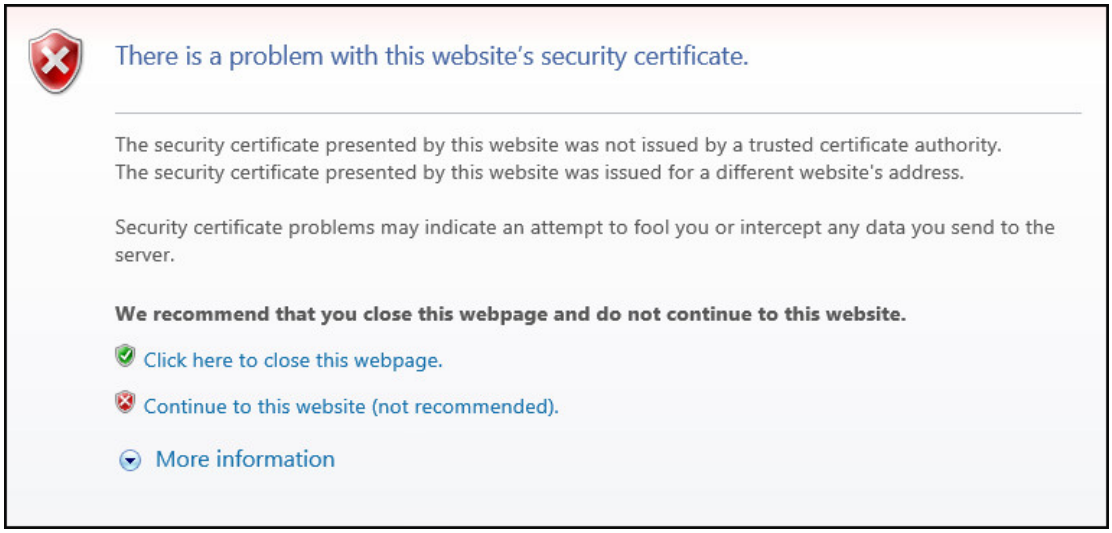
- TLS_RSA_WITH_AES_128_CBC_SHA (Prioritize Transmission Speed). This selection provides higher communication speed and lower security.
- TLS_RSA_WITH_AES_128_CBC_SHA256 (Prioritize Security). This selection provides higher security and lower communication speed.

4. Click **Apply** to save the setting and close the dialog box.

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.



Updating the certificate files

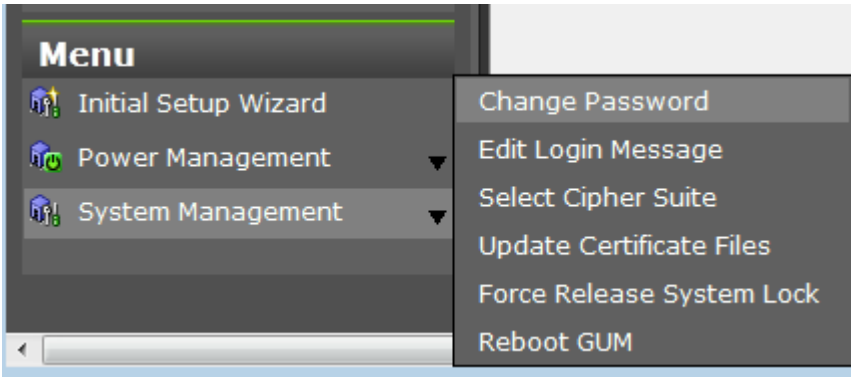
The **Update Certificate Files** window is used to update the certificates that are used for communication between the SVP and the storage system.

Before you begin

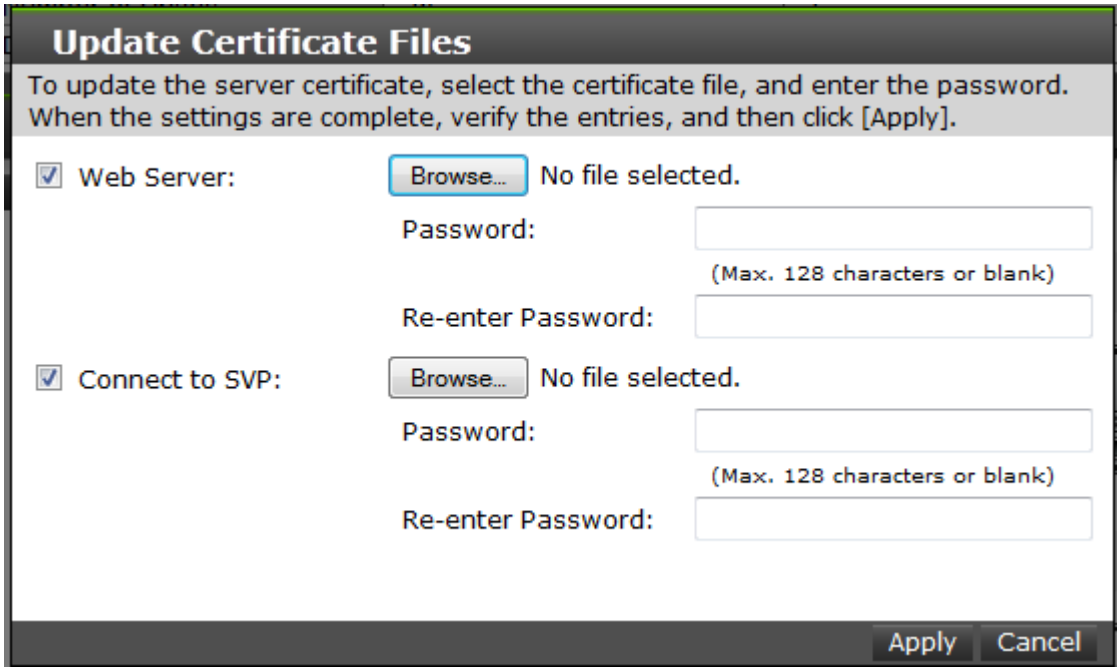
- You must have the Storage Administrator (View & Modify) role to complete this procedure.

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.**



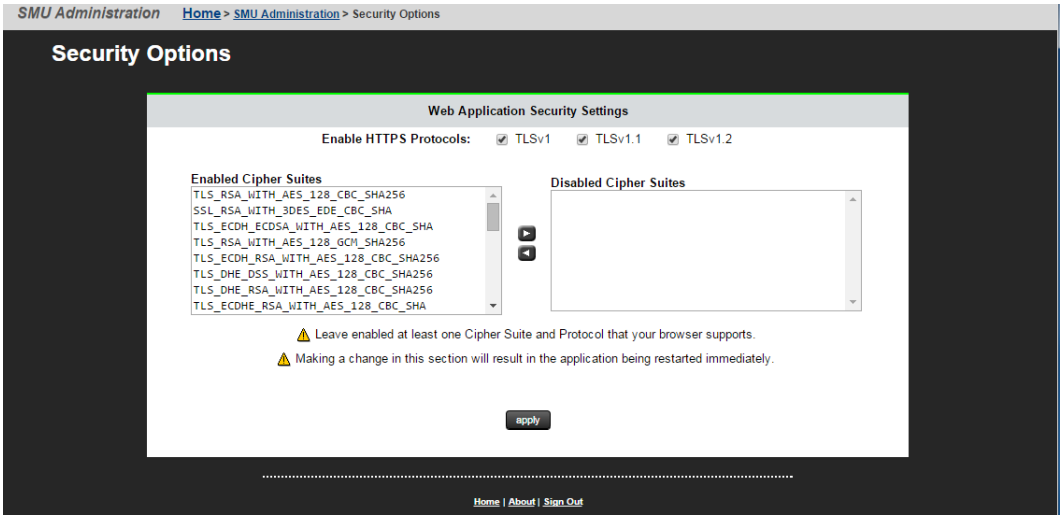
4. Browse to the certificate file and click **Open**. The **File Upload** window closes and returns you to the **Update Certificate Files** dialog box.
5. In the Web Server **Password:** field, enter the certificate password.
6. Enter the password again in the Web Server **Re-enter Password:** field.
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.

Configuring SMU security (NAS module only)

This screen allows you to change web application security settings.

The SMU can be configured to control the hosts that can access the SMU and auxiliary devices managed by the SMU.

Note: If you have a standby SMU, it may take up to 5 minutes after a configuration change to be synchronized with the active SMU



Procedure

1. Navigate to **Home > SMU Administration > Security Options**.

Field/Item	Description
Web Application Security Settings	This section allows you to change web application security settings. **Note:** Making any change in this section results in the application being restarted immediately.
Enable HTTPS Protocols	By default, all HTTPS protocols are enabled, and the boxes next to the protocols are checked. Uncheck the check box next to a protocol to change its state to disabled. Leave at least one protocol enabled that your browser supports.
Enabled Cipher Suites	By default, all cipher suites are enabled and are shown in the Enabled Cipher Suites list box.
Disabled Cipher Suites	To disable cipher suites, use the arrow to move selected cipher suites to the Disabled Cipher Suites list box. Leave at least one cipher suite enabled that your browser supports.
apply	Click **apply** to save your changes.

2. Optionally, to disable cipher suites, use the arrow to move enabled cipher suites from the **Enabled Cipher Suites** list at the left to the **Disabled Cipher Suites** list at the right. It is necessary to have at least one cipher suite remain enabled.



Note: Take care before disabling cipher suites, because not all cipher suites are supported by all browsers.

3. Optionally, to disable protocols, at **Enable HTTPS Protocols**, uncheck the check box next to a protocol to change its state to disabled. It is necessary to have at least one protocol remain enabled.



Note: Take care before disabling HTTPS protocols, because not all HTTPS protocols are supported by all browsers.

4. Click **apply** to save the currently defined security options.

6

Alert notifications

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

- ☐ Viewing alert notifications
- ☐ Configuring alert notifications
- ☐ Sending test messages
- ☐ Using the Windows event log

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.

Before you begin

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

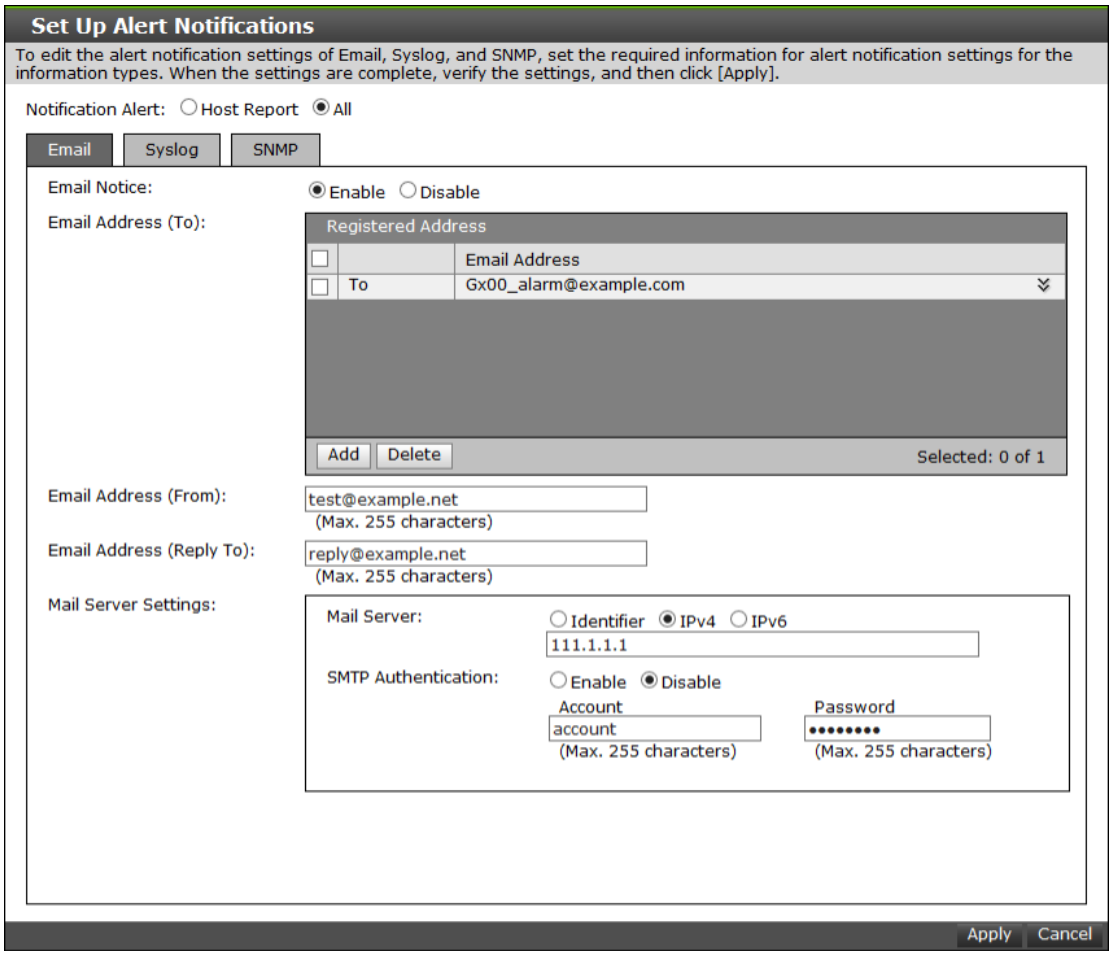
Procedure

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.



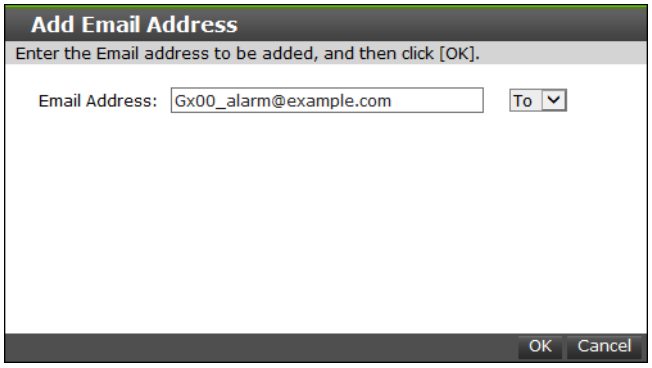
3. Select the type of report to send.
   - **Host Report**: Sends alerts only to the hosts for which a SIM report setting is made.
   - **All**: Sends alerts to all hosts.

   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.

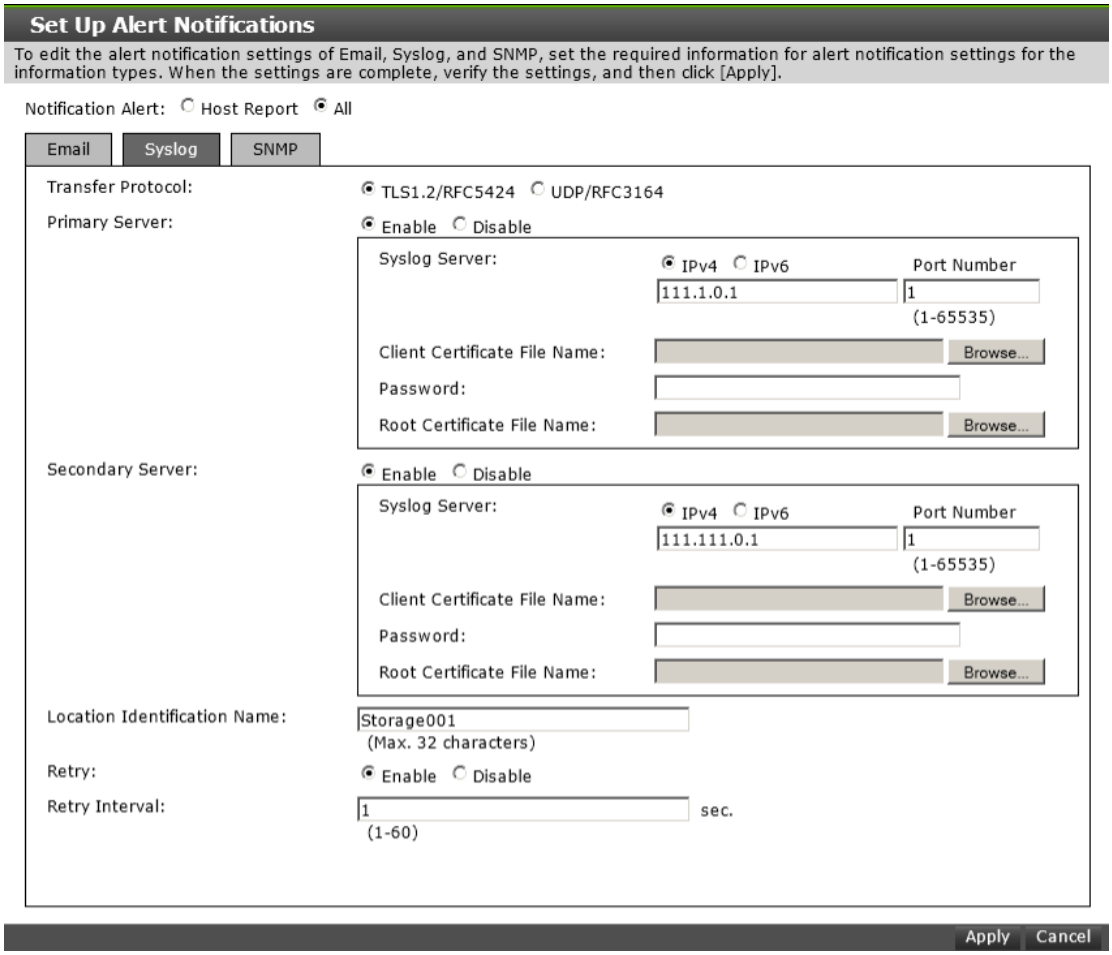


3. Enter the email address and then use the pull-down menu to select the type of address: **To**, **Cc**, or **Bcc.**
4. Click **OK** to save the email address and close the dialog box.
5. Enter an email address in **Email Address (From)**.
6. Enter an email address in **Email Address (Reply To:)**.
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.

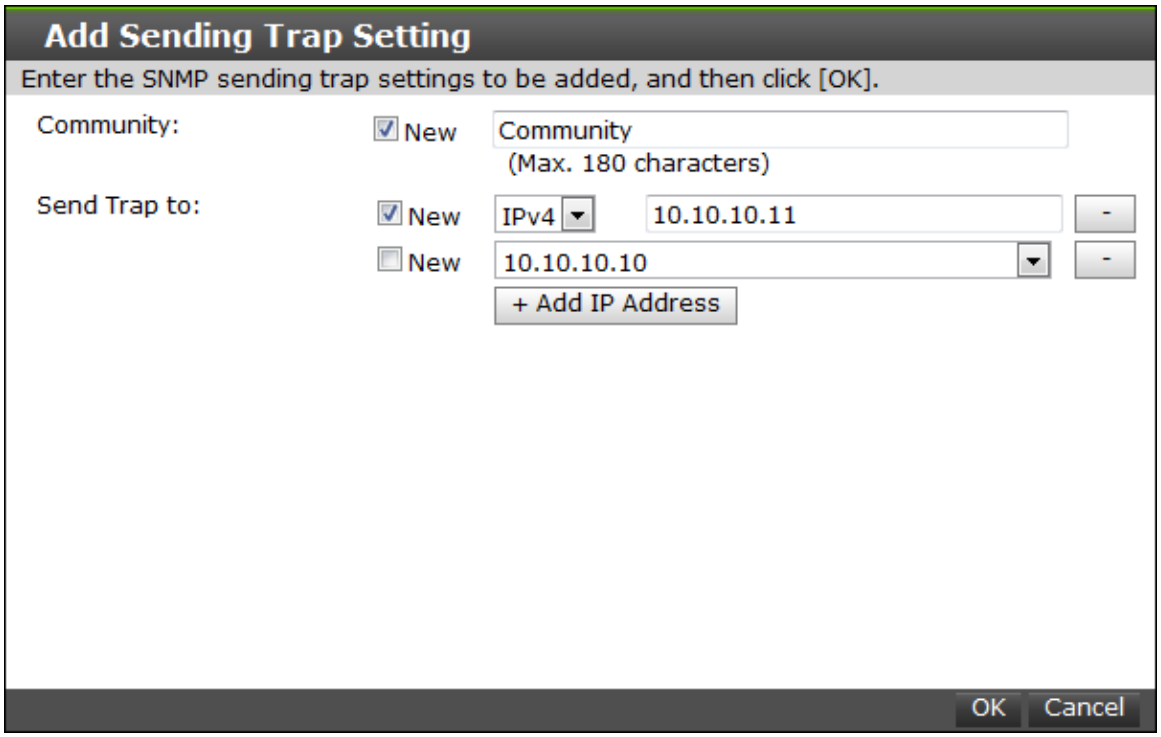


2. Select the type of transfer protocol to use.
3. In **Primary Server**:
   a. Click **Enable** to use the server or **Disable** not to use it.
   b. Select the type of IP address to use for the server: **IPv4** or **IPv6**.
   c. In **Client Certificate File Name**, click **Browse** to select a client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



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.

Using the Windows event log

Some failure information is output to the Windows event log.

Monitoring failure information in the Windows event log

You can manage the Windows error information by outputting failure information to the event log.

Before you begin

- The storage system status in the storage device list must be READY.

Procedure

1. Open a Windows command prompt with administrator permissions in SVP.
2. Execute the following command to move the current directory:
   `cd /d C:\Mapp\wk\`*`model-identification-number`*`\DKC200\mp\pc`

   - The default installation directory is `C:\Mapp`:<*installation-directory-of-SVP*>

   Note:
   - `C:\Mapp` indicates the installation directory of Device Manager - Storage Navigator. If you specified another directory, replace `C:\Mapp`: with the specified installation directory.
   - Without moving the current directory, failure information is not output to the Windows event log if you execute the batch file in step 3.

   - *model-identification-number*: Use the format `83`*`<model-name><serial-number>`*, where <*model-name*> is one of the following:
     VSP G200: 2000

VSP G400 or VSP F400, VSP G600 or VSP F600: 4000
VSP G800 or VSP F800: 6000
For example, for a VSP G600 that has the serial number 400102, the value is `834000400102`.

3. Execute the following batch file:
   `eventlog.bat` *`action monitoring-period`*

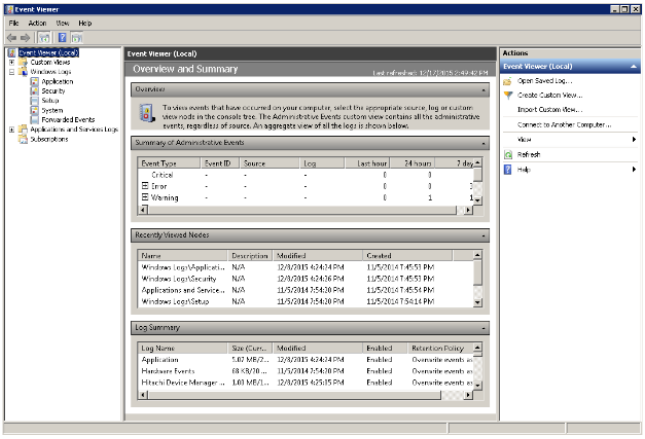
   - *action*: Specify one of the following:
     0: Stop outputting failure information
     1: Start outputting failure information
     when this parameter is omitted, 0 is set.
   - *monitoring-period*: If you specified 1 for *action*, specify the monitoring period, from 5 to 720 minutes.
   - A space is required between `eventlog.bat` and *action*.
   - A space is required between *action* and *monitoring-period*.
   - The command prompt is displayed if the command finishes without any errors.
4. Close the command prompt.

Viewing the Windows event log

You can view the Windows event log which is output to the SVP.

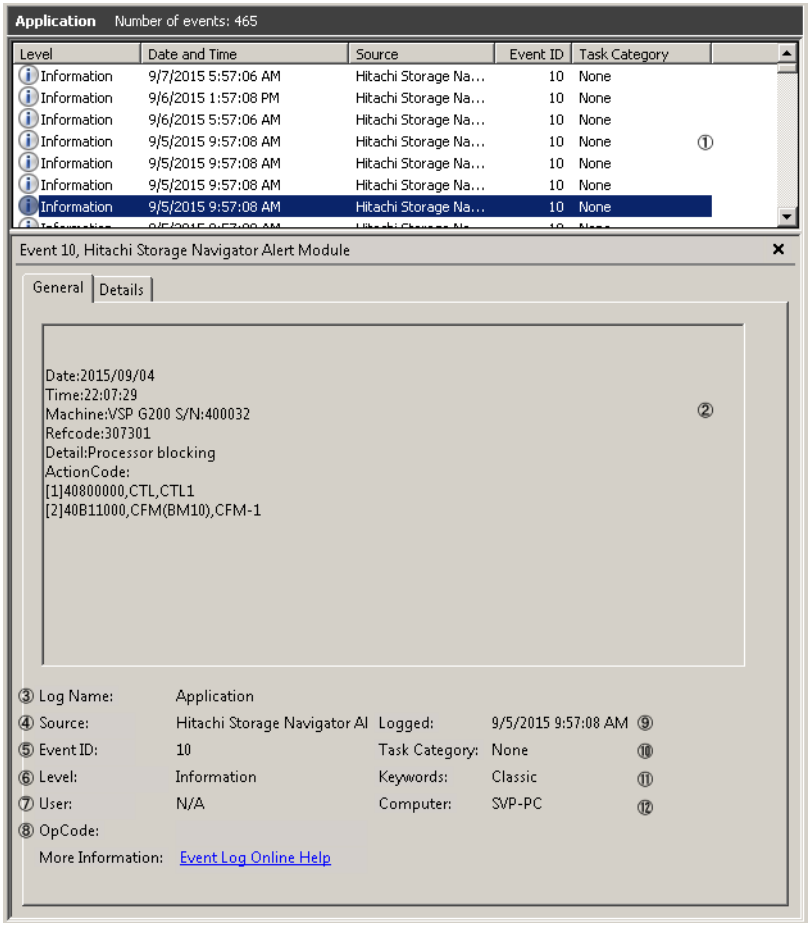
Procedure

1. From the Windows start menu, click **Control Panel** > **System and Security** > **Administrative Tools** > **Event Viewer**.
2. Click **Windows Logs** > **Application** in the left pane.



Output example of the failure information

The following is an example of the storage system failure information.



#	Item	Description
1	Overview of the event info	Displays the overview of the event information
2	Detail of the event info	Displays the selected information Date: Date of the event occurrence Time: Time of the event occurrence Machine: Model name and serial number of the storage system Refcode: Reference code* Detail: Detailed failure information* ActionCode: Includes action code, expected failure parts, and location. A maximum of 8 failure information can be shown.
3	Log name	Displays the log type This is always displayed as "Application"
4	Source	Displays the name of the application which issued the event

#	Item	Description
		This is always displayed as "Hitachi Storage Navigator Alert Module"
5	Event ID	Displays the event ID This is always displayed as "10"
6	Level	Displays the event alert level • Error: Acute or Serious • Warning: Moderate • Information: Service
7	User	This is always displayed as "N/A"
8	OpCode	This is always displayed as blank
9	Logged	Displays the date and time when the event log was registered
10	Task category	This is always displayed as "None"
11	Keywords	This is always displayed as "Classic"
12	Computer	Displays the computer name on which the event occurred
*For reference code, failure details, and alert level, see the SNMP failure trap reference code section in the *Hitachi SNMP Agent User Guide*.		

7

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 chapter describes the types of available licenses, license capacity calculation, and instructions for installing, enabling, disabling, and uninstalling license keys.

- ☐ Overview
- ☐ License key types
- ☐ Cautions on license capacities in license-related windows
- ☐ Managing licenses
- ☐ License key expiration

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.

If you do not install the 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.

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, when an LDEV is 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 capacity 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.

Cautions on license capacities in license-related windows

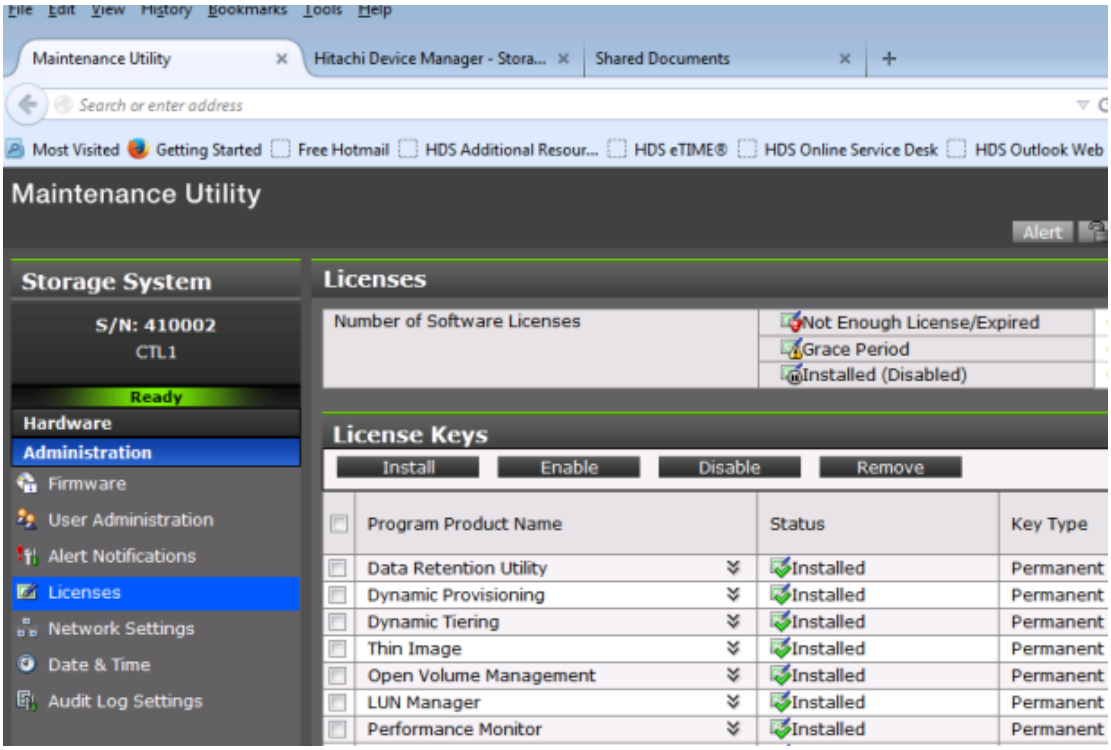
License capacities are displayed not only in license-related windows but also in the **Pools** window and the **Replication** window.

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 in the maintenance utility to install and uninstall block license keys.



Use NAS Manager to install and enable both block and file license keys on VSP Gx00 models with NAS modules. Using NAS Manager, you can install both block and file licenses but only remove file licenses. To remove block licenses, you must use the maintenance utility.

Related tasks

- Enabling a license on page 235
- Disabling a license on page 235
- Removing a software license on page 236

Related references

- Examples of license information on page 237

Installing block and file licenses using NAS Manager

Use NAS Manager to install and enable both block and file license keys on VSP Gx00 models with NAS modules. Using NAS Manager, you can install both block and file licenses but only remove file licenses. To remove block licenses, you must use the maintenance utility.

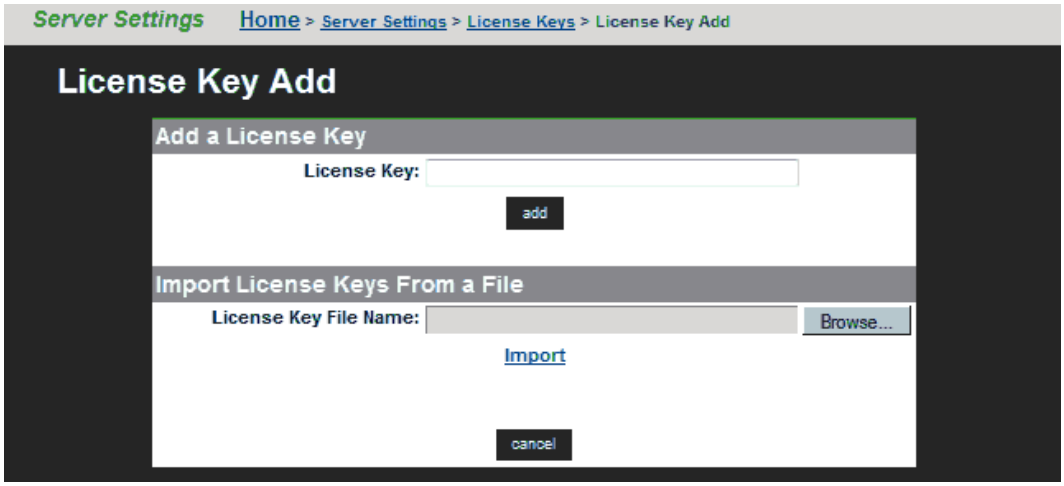
Adding a license key

Adding a license key can enable services or increase the capabilities of your system. To add a license key:

Procedure

1. Navigate to **Home > Server Settings > License Keys**.

2. Click **add**.



The following table describes the fields on this page:

Field/Item	Description
Add a File License Key	
File License Key	Enables the user to manually enter the license key.
Import File License Keys From a File	
File License Key File Name	Enables the user to import a license key from a file.
Import Block License Keys From a File (NAS module only)	
Block License Key File Name	Enables the user to import a software application license key from a file.
cancel	Closes the page without saving configuration changes.

Note: After adding a license key, if a reboot is required in order to start a service/protocol or enable a feature, you are instructed to reboot or restart the system.

For a file license, you can either enter the key manually or import it from a file. For a block license, you can only import the key from a file:

- To enter the key manually, type it in the field, then click **add**.
- To import the key, click **Choose File / Browse**, navigate to the file, select the key file, then click **Import**.

After all the keys have been entered or imported, they will be displayed on the **License Keys** page. Follow the instructions to reboot the system (if necessary).

Installing block licenses using maintenance utility

Before you begin
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.**

Enabling a license

You can enable a license that is in disabled status.

Before you begin
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.**

Disabling a license

You can disable a license that is in enabled status.

Before you begin

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.

Before you begin

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 236

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.

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

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.

8

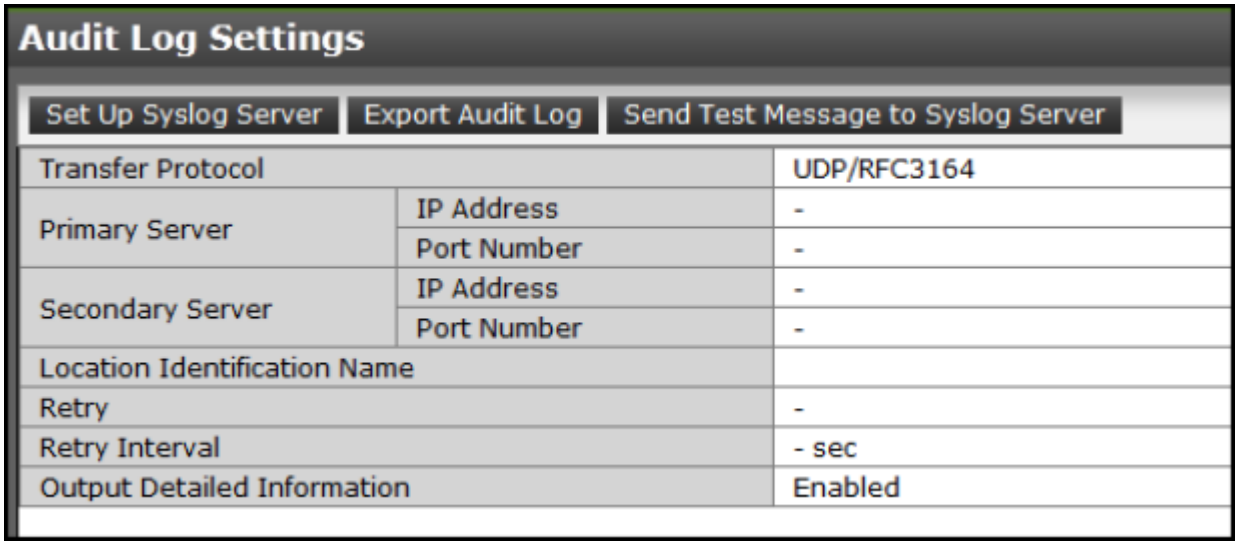
Configuring audit logs

This chapter describes how to change the audit log settings in the maintenance utility.

- [Audit log settings]

Audit log settings

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



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 240
- Exporting an audit log on page 241
- Sending a test Syslog message on page 223

Setting up a syslog server

Before you begin

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

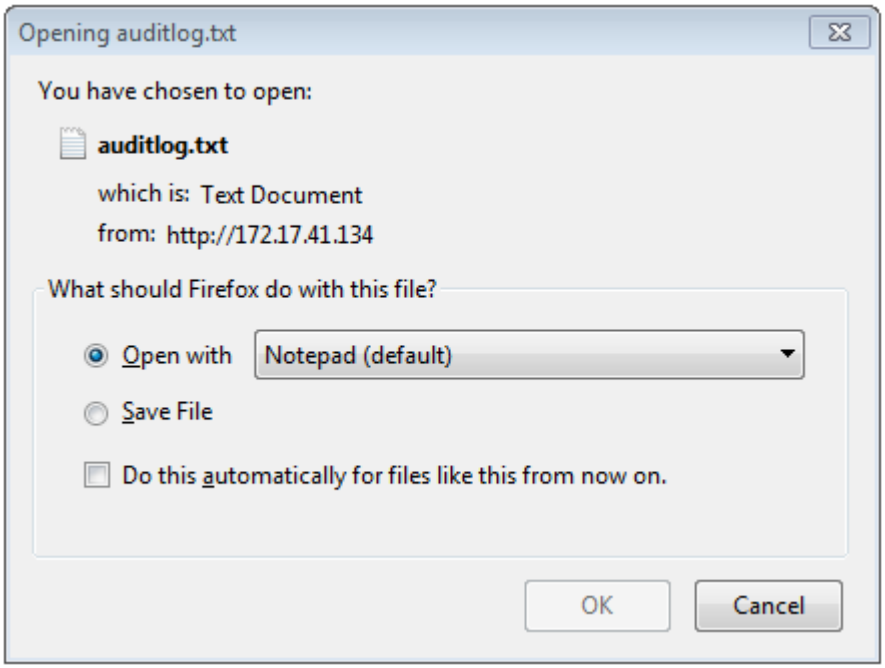
Use the following procedure to send a display an audit log file on the screen or to save it to a file on the SVP or your laptop.

Before you begin

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**.



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

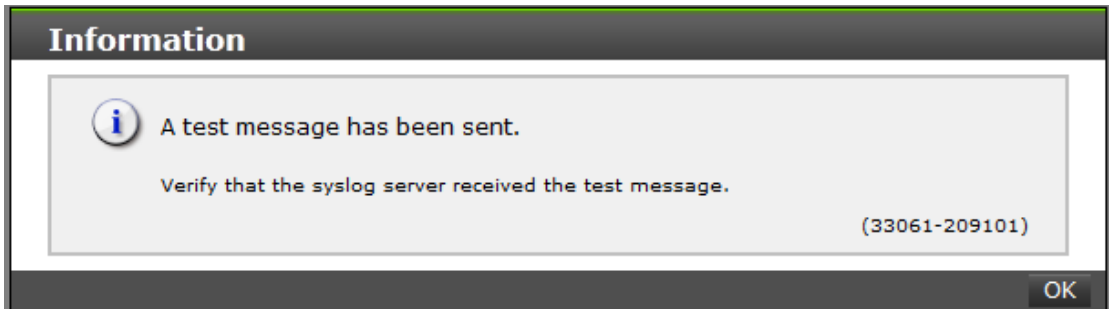
Use the following procedure to send a test audit log message to the syslog server.

Before you begin

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:



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.

9

Managing storage system reports

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

- About storage system reports
- Viewing a Device Manager - Storage Navigator report
- Collecting dump files using the Dump tool

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

Before you begin

- 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.
- The window to specify the saving folder location may not be displayed when downloading the report in Google Chrome. In this case, follow Chrome Menu > Settings > Show advanced settings and uncheck the Protect you and your device from dangerous sites checkbox under Privacy.

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 create up to 20 configuration reports for each storage system. If you already created 20 reports, delete unnecessary reports first, and then create a new report.

Before you begin

You must have Storage View permission to perform this task.

Procedure

1. Open the **Create Configuration Report** window.
   In Hitachi Command Suite:
   a. On the **Resources** tab, expand the **Storage Systems** tree.
   b. Right-click the local storage system, and then click **Reports > Create Configuration Report**.

   In Device Manager - Storage Navigator:
   - 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.

Before you begin

Users that create the report or users with the 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.

Before you begin

- You must be logged into the SVP.
- Device Manager - Storage Navigator must be running.
- The configuration information must be refreshed by selecting File > Refresh All in Device Manager - Storage Navigator.
- All other users (including the SVP user) must stop using the Dump tool.
- Stop all maintenance operations.
- Dump tools from other storage systems must not be used during the process.



Note: If the error is in regards to Device Manager - Storage Navigator starting up, collect information about the SVP using the Dump tool, without Device Manager - Storage Navigator running.

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_832000400001, enter the following:

   ```
   C:\MAPP\wk\832000400001\DKC200\mp\pc>Dump_Detail.bat C:\Result_832000400001
   ```

   Note:
   - A space is required between Dump_Detail.bat and C:\Result.
   - The dump file name is hdcp.tgz. To manage dump files by storage systems, we recommend adding a serial number to the output folder name. For example, if the serial number is 832000400001, the folder name should be C:\Result_832000400001.
   - When the tool is being executed, is displayed in the command prompt. When the execution is completed, is displayed.

     "Executing..."

     "zSv_AutoDump.exe is completed."

5. A completion message box displays. Press any key to acknowledge the message and close the message box.

   hdcp.tgz: This is the dump file. Give this file to the maintenance personnel. If you save too many dump files in the SVP storage, space might not be available. Therefore, move the dump file outside of SVP storage.

   zSv_AutoDump.log: This is the log file of the dump tool. If the dump file is not output, give this log file to the maintenance personnel. If the dump file is output, delete the log file.
6. Close the Windows command prompt.

A

Raidinf command reference (obtaining configuration reports and tier relocation logs)

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

- raidinf command list and command description
- raidinf -login
- raidinf add report
- raidinf delete report
- raidinf download report
- raidinf get reportinfo
- raidinf add relocationlog
- raidinf download relocationlog
- raidinf delete relocationlog
- raidinf get relocationloginfo
- raidinf -logout
- raidinf -h

raidinf command list and command description

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

Table 10 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 add relocationlog`	Generates a tier relocation log file.
`raidinf download relocationlog`	Downloads a tier relocation log file.
`raidinf delete relocationlog`	Deletes a tier relocation log file.
`raidinf get relocationloginfo`	Lists a tier relocation log file.
`raidinf -logout`	Logs out of Device Manager - Storage Navigator.
`raidinf -h`	Displays the raidinf command syntax.

Table 11 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.

Symbol	Description
	• 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>] [-serial <serial>]
```

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.
`[-serial <serial>]`	If two or more DKCs are managed by the SVP, this is specified to identify the system to execute the raidinf command. You cannot omit this option if two or more DKCs are managed by the SVP. In operations after the log in, such as report creation, use the serial number specified when logging in. You do not need to specify the serial number after the log in.

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
```

This example authenticates `user01` using the password `xxxxxx` with TCP port number 6443 and serial number 430123:

```
# raidinf -login user01 xxxxxx -servername svp.xxx.co.jp -port
6443 -serial 430123
```

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 add relocationlog

The `raidinf add relocationlog` command is used to generate a tier relocation log.

If another user has already generated a tier relocation log, an error occurs if a tier relocation login user tries to obtain tier relocation logs. When this happens, you must delete the existing tier relocation logs.

Syntax

```
raidinf add relocationlog -servername {<hostname> | <ipaddress>}
-logname <logname>>
```

Options and parameters

Option	Description
`-servername {<hostname> | <ipaddress>}`	Specifies the host name or IP address of the SVP.
`[-logname <logname>>]`	Specifies the tier relocation log name, up to 32 characters. All characters exceeding 32 are ignored. If the tier relocation log is omitted, the default name *YYMMDDXXXXXX*-RelocationLog is specified. A hyphen cannot be specified at the beginning of the tier relocation log name.

Examples

The following example generates a tier relocation log with the default log name:

```
# raidinf add relocationlog -servername 10.213.74.121
RelocationLogName             CreateTime
160201-400001-RelocationLog     2016/02/01-12:43:10
```

The following example generates a tier relocation log named

```
160201-400001-RelocationLog:
# raidinf add relocationlog -servername 10.213.74.121 -report
160201-400001-RelocationLog
RelocationLogName             CreateTime
160201-400001-RelocationLog     2016/02/01-12:43:10
```

The following items are output:

- `RelocationLogName`
  The tier relocation log name is displayed.
- `CreateTime`
  The time when the log was generated is displayed.

raidinf download relocationlog

The `raidinf download relocationlog` command is used to download a tier relocation log.

A tier relocation log which is being generated cannot be downloaded. The name of the downloaded file is `tier_relocation_log_name.tgz`. The log is overwritten with the same name if the name already exists.

Example: If the name of the tier log relocation log is `160201-400001-RelocationLog`, the downloaded file name will be as follows:

```
Log_160201-400001-RelocationLog.tgz
```

Syntax

```
raidinf download relocationlog -servername {<hostname> |
<ipaddress>}
-logname <logname>> -targetfolder <folder>
```

Options and parameters

Option	Description
`-servername {<hostname> | <ipaddress>}`	Specifies the host name or IP address of the SVP.
`[-logname <logname>>]`	Specifies the tier relocation log name, up to 32 characters. All characters exceeding 32 are ignored. If the tier relocation log is omitted, the default name *YYMMDDXXXXXX*-RelocationLog is specified. If you specify `LatestLog` as the tier relocation log name, the log with the most recent date is downloaded.
`-targetfolder <folder>`	Specifies a folder name to which a tier relocation log is downloaded. The folder whose name you specify must already exist, and you must have write permissions to the folder.

Examples

The example below shows how to download the log with the most recent date. In the following example, `Log_160201-400001-RelocationLog.tgz` is downloaded to `C:\tmp`:

```
# raidinf download relocationlog -servername 10.213.74.121 –
logname LatestLog -targetfolder C:\tmp
```

The example below shows how to download the tier relocation log by specifying the tier relocation log name, `160201-400001-RelocationLog`. In

the following example, `Log_160201-400001-RelocationLog` is downloaded to `C:\tmp`:

```
# raidinf download relocationlog -servername 10.213.74.121 -
report
160201-400001-RelocationLog -targetfolder C:\tmp
```

raidinf delete relocationlog

The `raidinf delete relocationlog` command is used to delete a tier relocation log.

Syntax

```
raidinf delete relocationlog -servername {<hostname> |
<ipaddress>}
-logname <logname>>
```

Options and parameters

Option	Description
`-servername {<hostname> | <ipaddress>}`	Specifies the host name or IP address of the SVP.
`[-logname <logname>>]`	Specifies the tier relocation log name, up to 32 characters. All characters exceeding 32 are ignored. If you specify `LatestLog` as the tier relocation log name, the log with the most recent date is deleted.

Examples

The following example deletes the tier relocation log with the most recent date:

```
# raidinf delete relocationlog -servername 10.213.74.121 –
logname LatestLog
```

The example below shows how to delete the tier relocation log by specifying the tier relocation log name, `160201-400001-RelocationLog`. In the following example, `160201-400001-RelocationLog` is deleted in the SVP:

```
# raidinf delete relocationlog -servername 10.213.74.121 –report
160201-400001-RelocationLog
```

raidinf get relocationloginfo

The `raidinf get relocationloginfo` command is used to list tier relocation logs. The tier relocation logs which are being generated are not listed.

Syntax

```
raidinf delete relocationlog -servername {<hostname> |
<ipaddress>}
```

Options and parameters

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

Examples

The example below shows how to generate a tier relocation log by specifying the tier relocation log name, `160201-400001-RelocationLog`.

```
# raidinf add relocationlog -servername 10.213.74.121 -report
160201-400001-RelocationLog
RelocationLogName             CreateTime
160201-400001-RelocationLog     2016/02/01-12:43:10
```

The following items are output:

- `RelocationLogName`
  The tier relocation log name is displayed.
- `CreateTime`
  The time when the log was generated is displayed.

The example below shows the script for checking if the tier relocation log was created by using the `raidinf get relocationloginfo` command. In this example, if the creation of the tier relocation log was completed successfully, the tier relocation log is downloaded.

```
REM
REM Create Completed Relocation Log
Script(CreateCompletedRelocationLog.bat)
REM
SET SERVER= <hostname-or-IP-address-of-SVP>
SET LOG_NAME=DailyRelocationLog
raidinf get relocationloginfo -servername %SERVER% | find
"%LOG_NAME%"
>NUL
if not ERRORLEVEL 1 raidinf download relocationlog -servername
%SERVER% -targetfolder C:\tmp -logname "%LOG_NAME%"
```

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.
`-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 chapter 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.

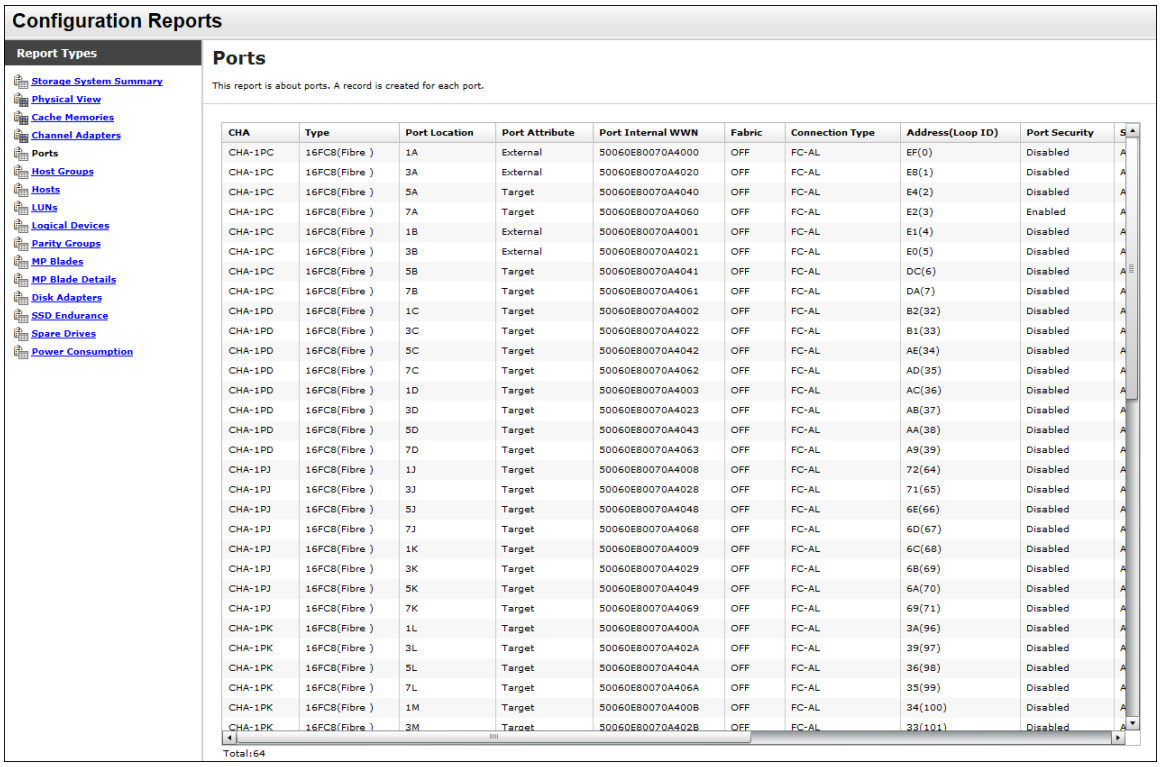
To create, download, and delete reports, see Viewing a Device Manager - Storage Navigator report on page 244.

- Reports in table view
- Reports in graphical view
- CSV files

Reports in table view

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

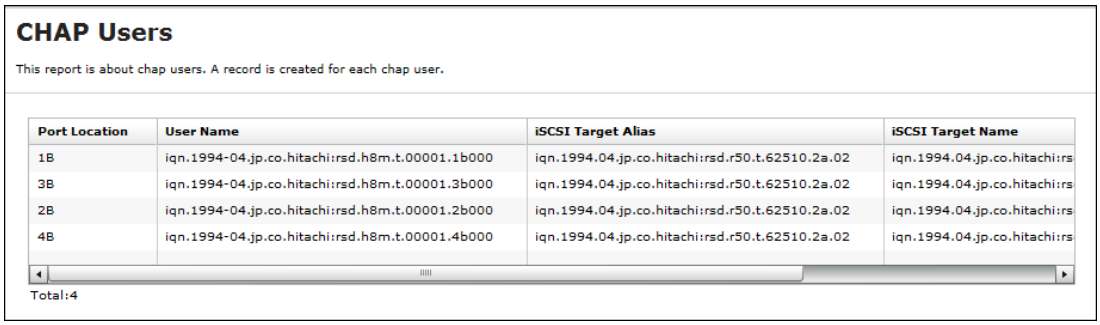
The following figure provides examples of reports in table format. The icons are displayed before the names of the reports in table view. If the icons are not displayed correctly, update the window.



- 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

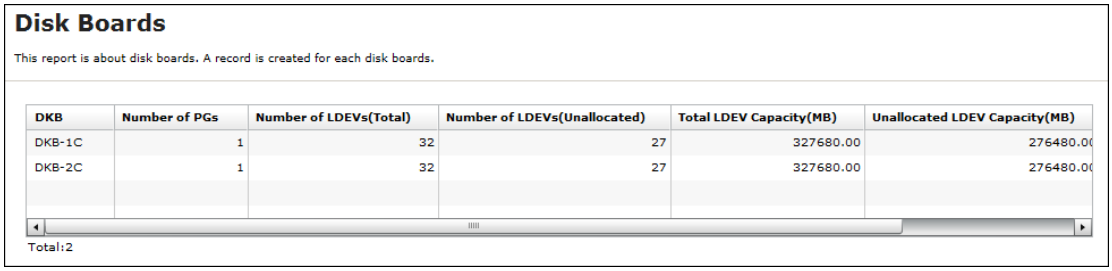
The following figure shows an example of a CHAP Users report. The table following the figure describes the items in the report.



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

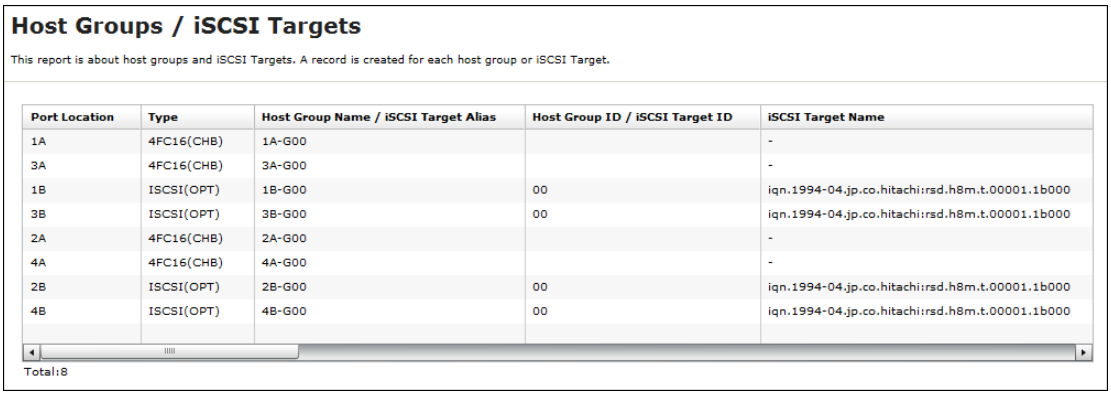


Item	Description
DKB	Location of the disk board. • "External" is displayed when the storage system has an external storage system. • "External (FICON DM)" is displayed when the storage system has volumes for FICON DM.
Number of PGs	The number of the parity groups that the disk board controls. • If "DKB" 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 figure shows an example of a Host Groups / iSCSI Targets report. The table following the figure 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

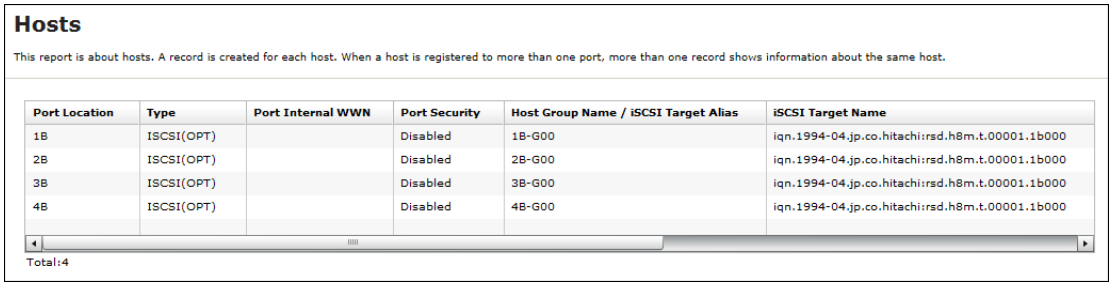
Total:8

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 figure shows an example of a hosts report. The table following the figure 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.

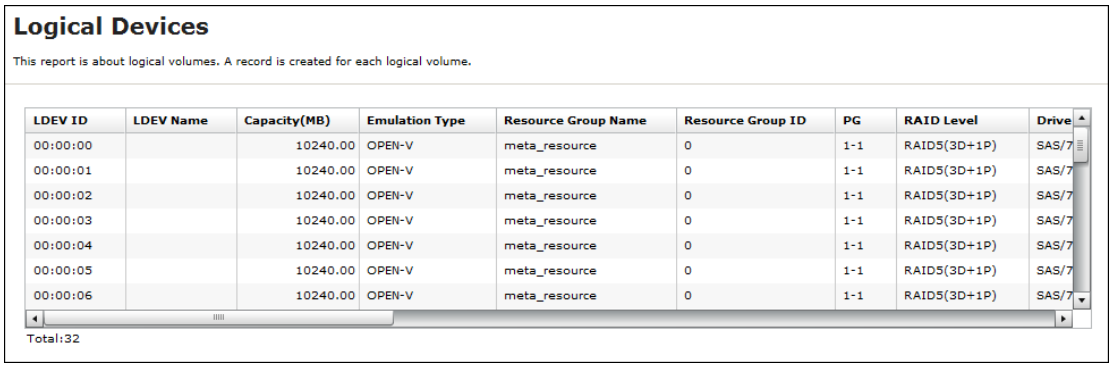


Item	Description
Port Location	Name of the port
Type	Port type
Port Internal WWN	Port WWN
Port Security	Port security setting

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 figure shows an example of a logical volumes report. The table following the figure 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

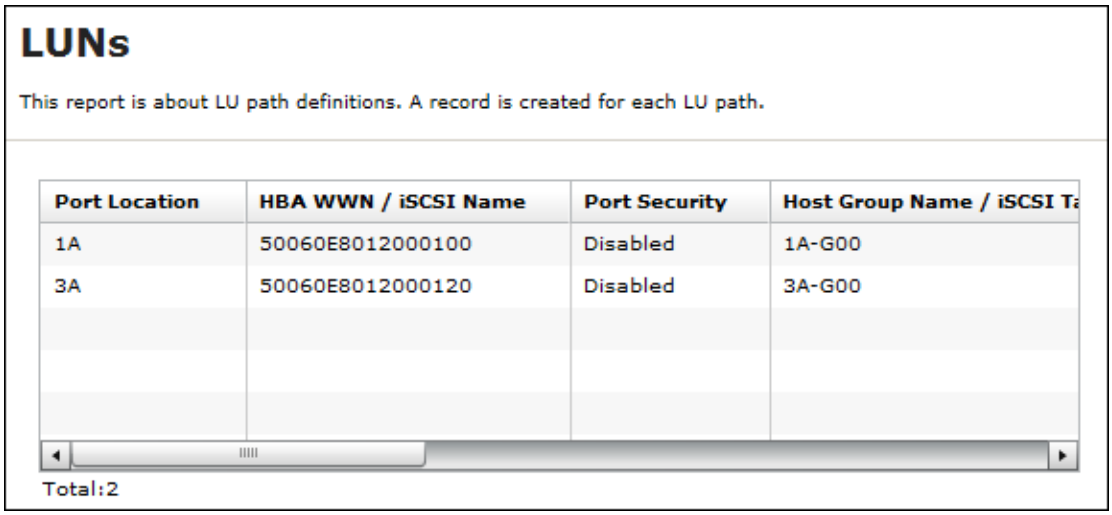
Total:32

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	Indicates whether the parity group to which the LDEV belongs is encrypted. • For internal volumes: Enabled (encrypted) or Disabled (not encrypted) • For external volumes: blank
T10 PI	Indicates the T10 PI attribute set for the LDEV. • Enabled • Disabled • Blank if the emulation type is not OPEN-V
ALUA Mode	Indicates whether the ALUA mode is enabled: • Enabled: ALUA mode is enabled. • Disabled: ALUA mode is disabled.
Notes: **1.** A hyphen (-) displays if the LDEV is an external volume.	

LUNs report

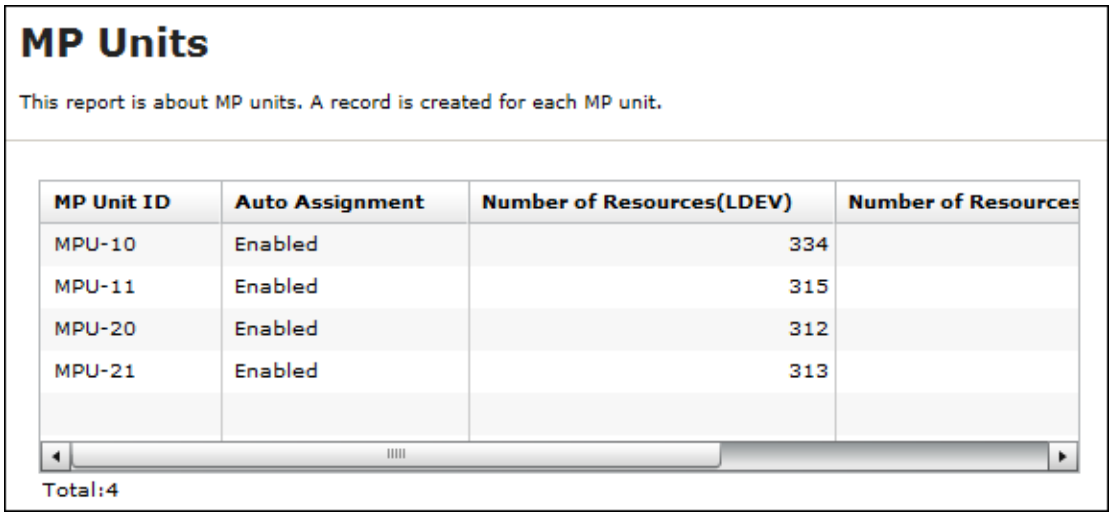
The following figure shows an example of an LU path definitions report. A record is created for each LU path. The table following the figure describes the items in the report.



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

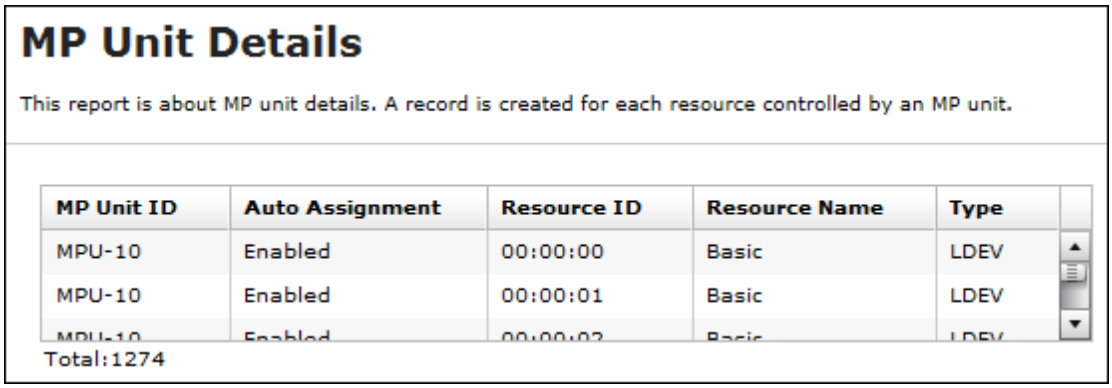
The following figure shows an example of an MP units report. The table following the figure describes the items in the report.



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

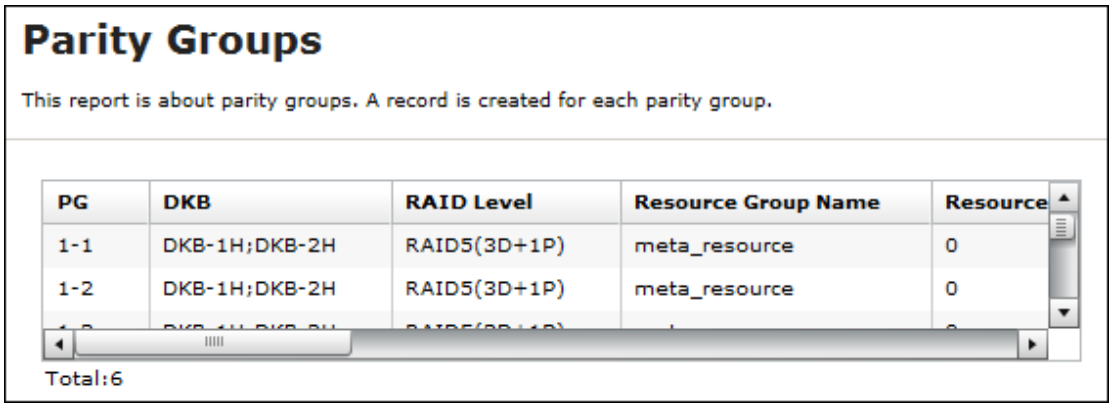
The following figure shows an example of an MP unit details report. The table following the figure describes the items in the report.



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



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

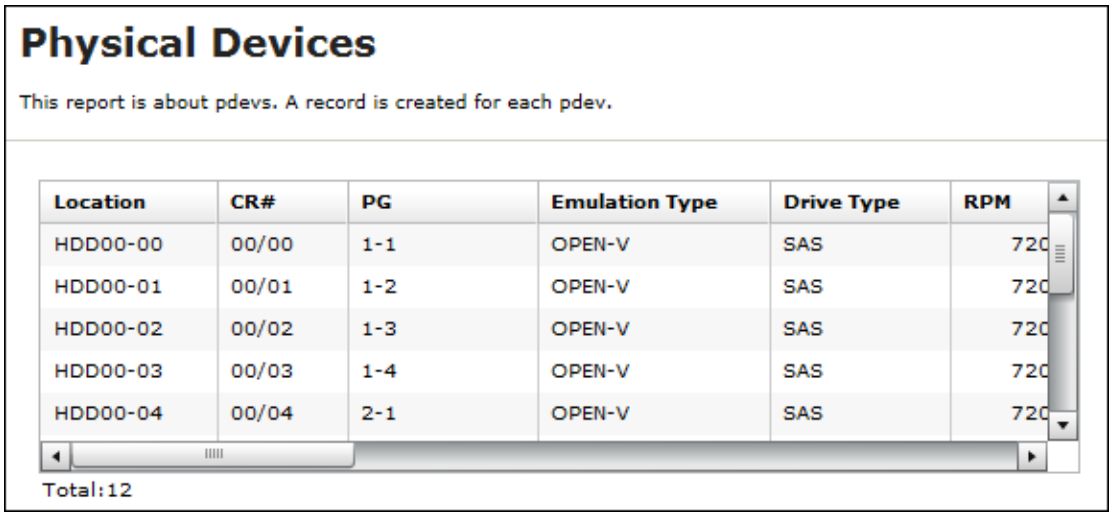
Item	Description
Drive Type-Code	The type code of the drive in the parity group. • The type code of the first drive in the parity group. • If the parity group contains external volumes, the drive type code displays the vendor, the model, and the serial number of the storage system. • Separated by semicolons (;) 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	Indicates whether the parity group is encrypted. • For internal volumes: Enabled (encrypted) or Disabled (not encrypted) • For external volumes: A hyphen (-) is displayed
Accelerated Compression	Accelerated compression of the parity group • If accelerated compression is supported, Enabled or Disabled is displayed. • If accelerated compression is not supported, 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

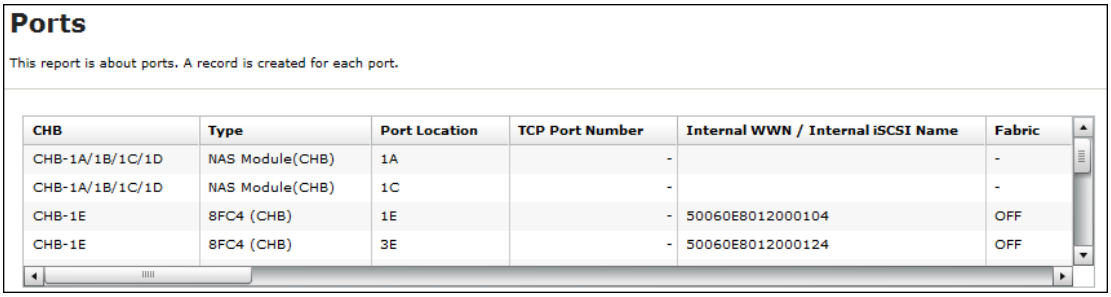
The following figure shows an example of part of a Physical Devices report. The actual report includes more columns of information. A record is created for each physical device. The table following the figure describes the items in the report.



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 figure shows an example of part of a ports report. The actual report includes several more columns of information. The table following the figure 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	Internal WWN / Internal iSCSI Name	Fabric
CHB-1A/1B/1C/1D	NAS Module(CHB)	1A	-		-
CHB-1A/1B/1C/1D	NAS Module(CHB)	1C	-		-
CHB-1E	8FC4 (CHB)	1E	-	50060E8012000104	OFF
CHB-1E	8FC4 (CHB)	3E	-	50060E8012000124	OFF

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)
Internal WWN / Internal iSCSI Name	WWN / iSCSI name 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. Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal)

Item	Description
IPv6 : Global Address 2	IPv6 global address 2 of the port. Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal)
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)
CHAP User Name	User name for the CHAP authentication
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
SFP Data Transfer Rate	Maximum transfer rate of SFP which the mounted package supports. • 8G • 10G • 16G • 32G • Blank if the Package Type is 10iSCSI2c (CHB) or NAS module (CHB).
T10 PI Mode	Indicates whether the T10 PI mode can be applied to the port. • Enabled • Disabled • Blank if the port type is a Fibre port other than 16FC2(CHB). For iSCSI ports, a hyphen (-) is displayed.
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

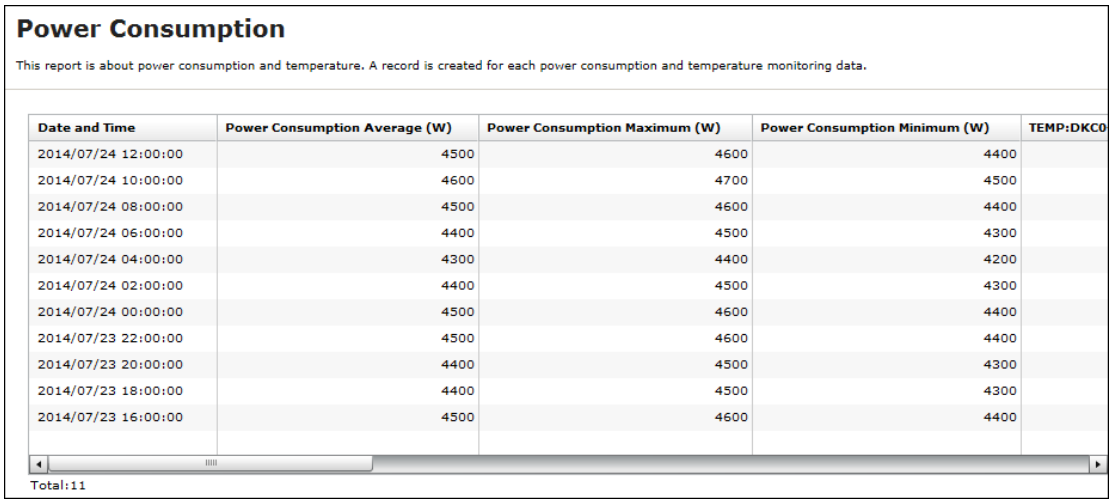
Item	Description
Number of PGs	The number of the parity groups having the logical volumes that can be accessed through the port
Number of DKBs	The number of the disk boards controlling the parity group that contains the logical volumes that can be accessed through the port

Power Consumption report

The following figure 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 figure describes the items in the report.

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.

If a failure occurs in the storage system, the correct information might not be output.



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

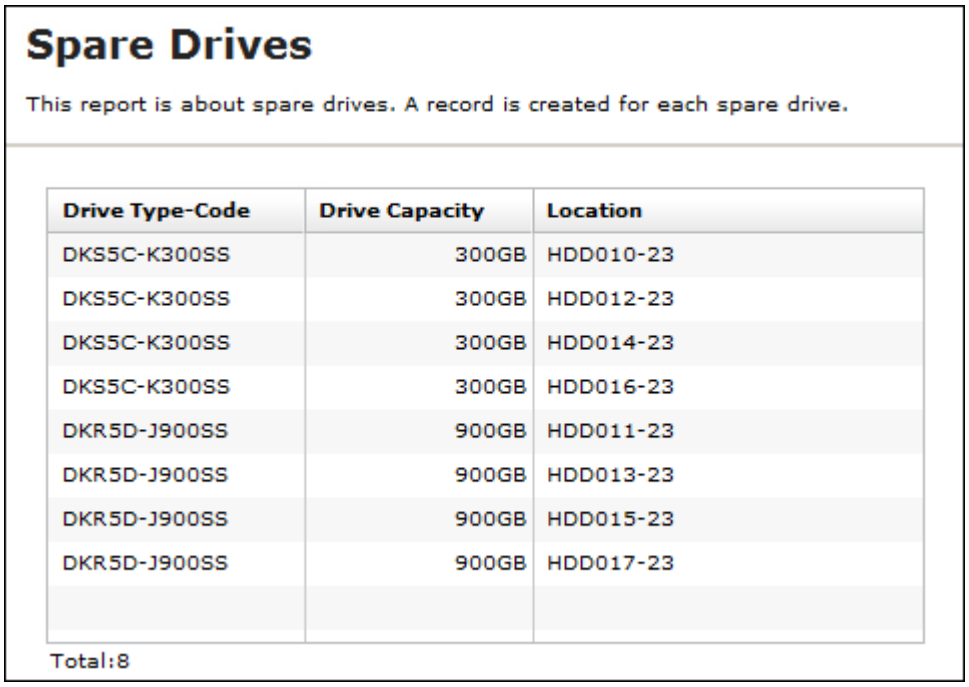
Item	Description
TEMP:DKC0-Cluster1 Minimum (degrees C)	Minimum temperature of DKC0:CL1
TEMP:DKC0-Cluster2 Average (degrees C)	Average temperature of DKC0:CL2
TEMP:DKC0-Cluster2 Maximum (degrees C)	Maximum temperature of DKC0:CL2
TEMP:DKC0-Cluster2 Minimum (degrees C)	Minimum temperature of DKC0:CL2

Table 12 Power Consumption report

Item	Description
Date and Time	Date and time when temperature was recorded
TEMP:DB00-DBPS00-1 Average (Temperature in degrees C) TEMP:DB00-DBPS00-1 Maximum (Temperature in degrees C), TEMP:DB00-DBPS00-1 Minimum (Temperature in degrees C), TEMP:DB00-DBPS00-2 Average (Temperature in degrees C), TEMP:DB00-DBPS00-2 Maximum (Temperature in degrees C), TEMP:DB00-DBPS00-2 Minimum (Temperature in degrees C)	Average temperature, maximum temperature, and minimum temperature of the DB for the two-hour period. Outputs in the following format: TEMP:DB *XX* -DBPS *XX* -*CL* Average, Maximum, or Minimum (Temperature in degrees Celsius) • *XX*: DB number 00 to 07 (VSP G200) 00 to 23 (VSP G400, G600, VSP F400, F600) 00 to 47 (VSP G800 or VSP F800) • CL: Cluster number (1 or 2)

Spare Drives report

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



Spare Drives

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

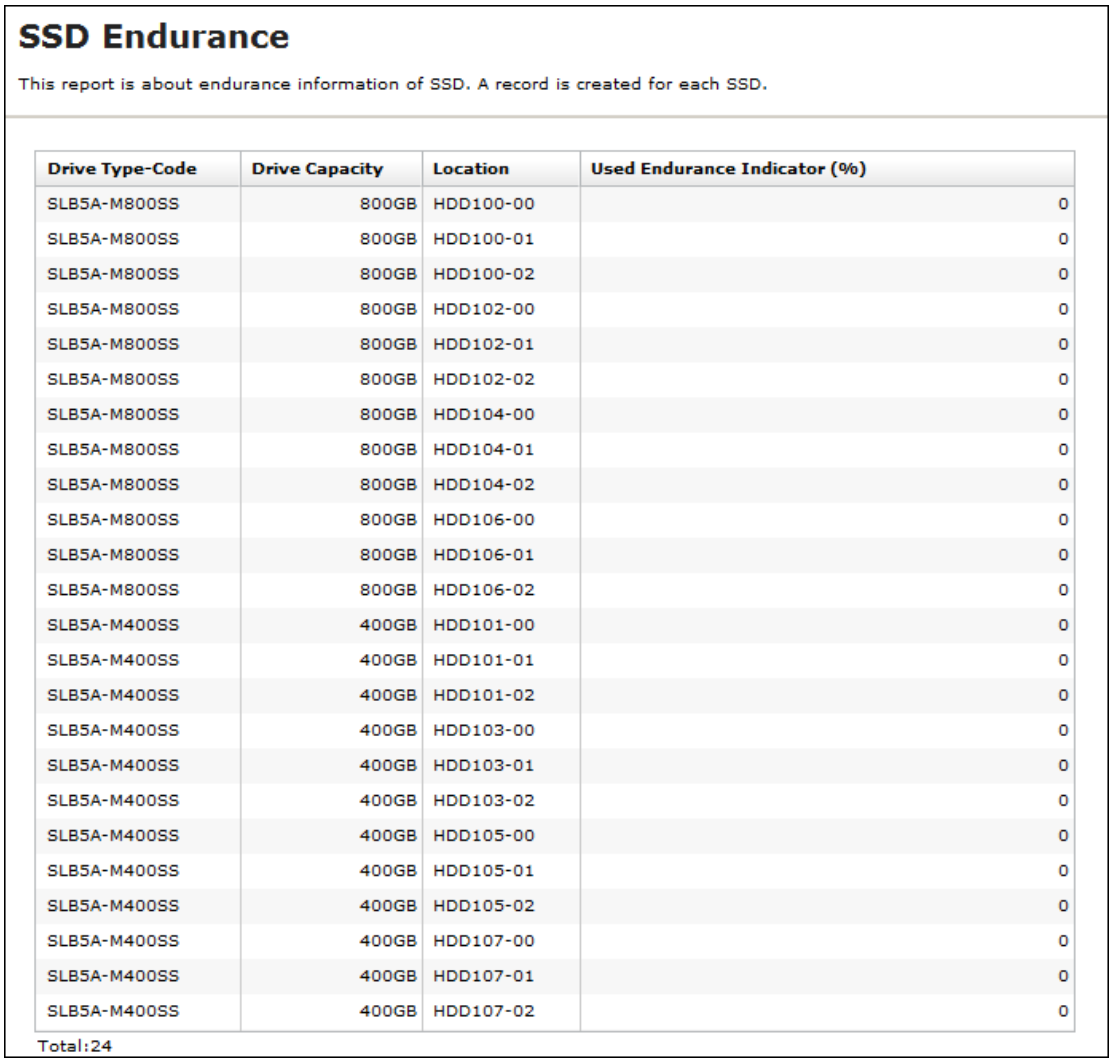
Drive Type-Code	Drive Capacity	Location
DKS5C-K300SS	300GB	HDD010-23
DKS5C-K300SS	300GB	HDD012-23
DKS5C-K300SS	300GB	HDD014-23
DKS5C-K300SS	300GB	HDD016-23
DKR5D-J900SS	900GB	HDD011-23
DKR5D-J900SS	900GB	HDD013-23
DKR5D-J900SS	900GB	HDD015-23
DKR5D-J900SS	900GB	HDD017-23

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



SSD Endurance

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

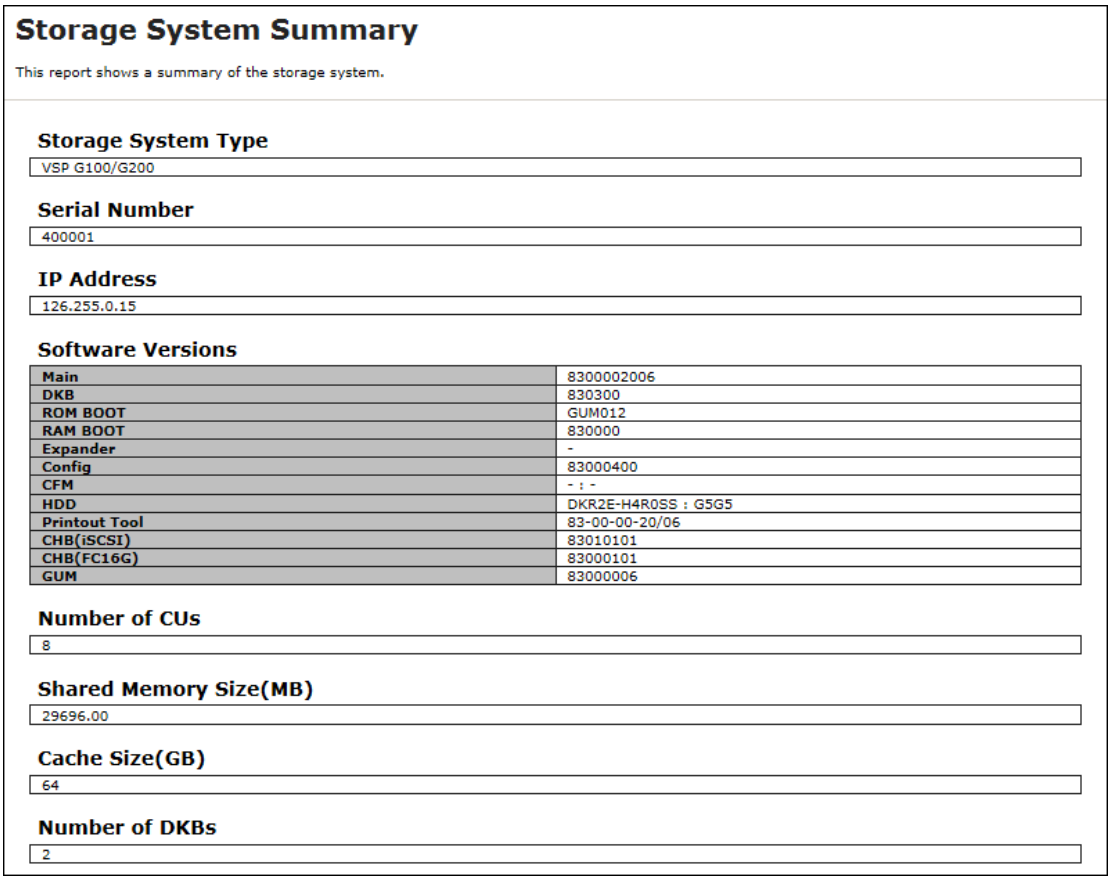
Drive Type-Code	Drive Capacity	Location	Used Endurance Indicator (%)
SLB5A-M800SS	800GB	HDD100-00	0
SLB5A-M800SS	800GB	HDD100-01	0
SLB5A-M800SS	800GB	HDD100-02	0
SLB5A-M800SS	800GB	HDD102-00	0
SLB5A-M800SS	800GB	HDD102-01	0
SLB5A-M800SS	800GB	HDD102-02	0
SLB5A-M800SS	800GB	HDD104-00	0
SLB5A-M800SS	800GB	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 figure shows an example of part of a Storage System Summary report. The actual report includes several more rows of information. The table following the figure 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

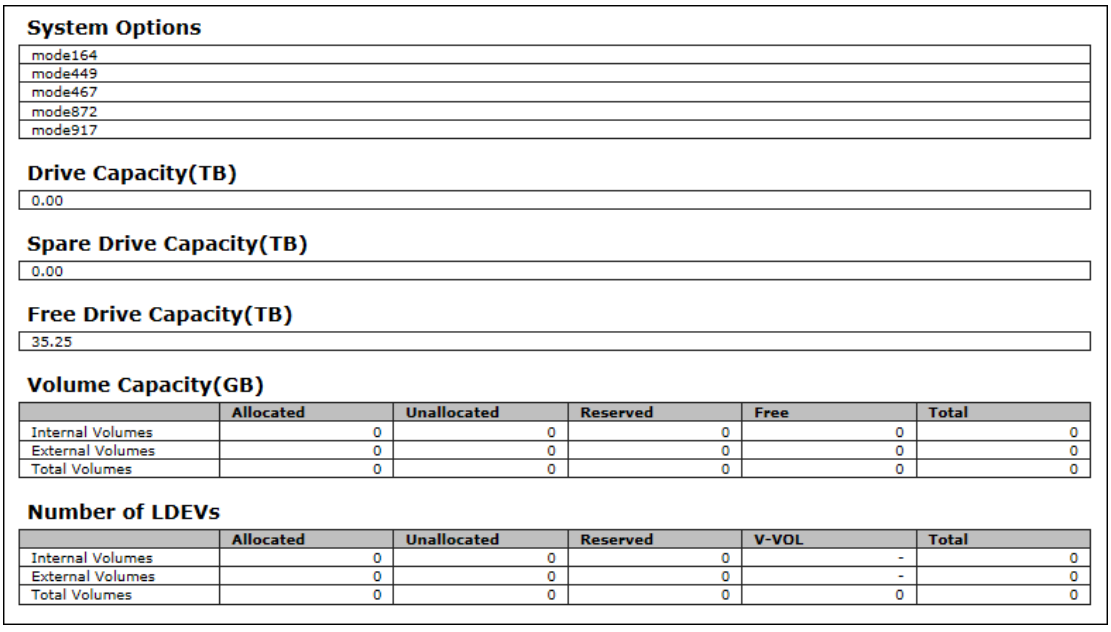
Cache Size(GB)

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

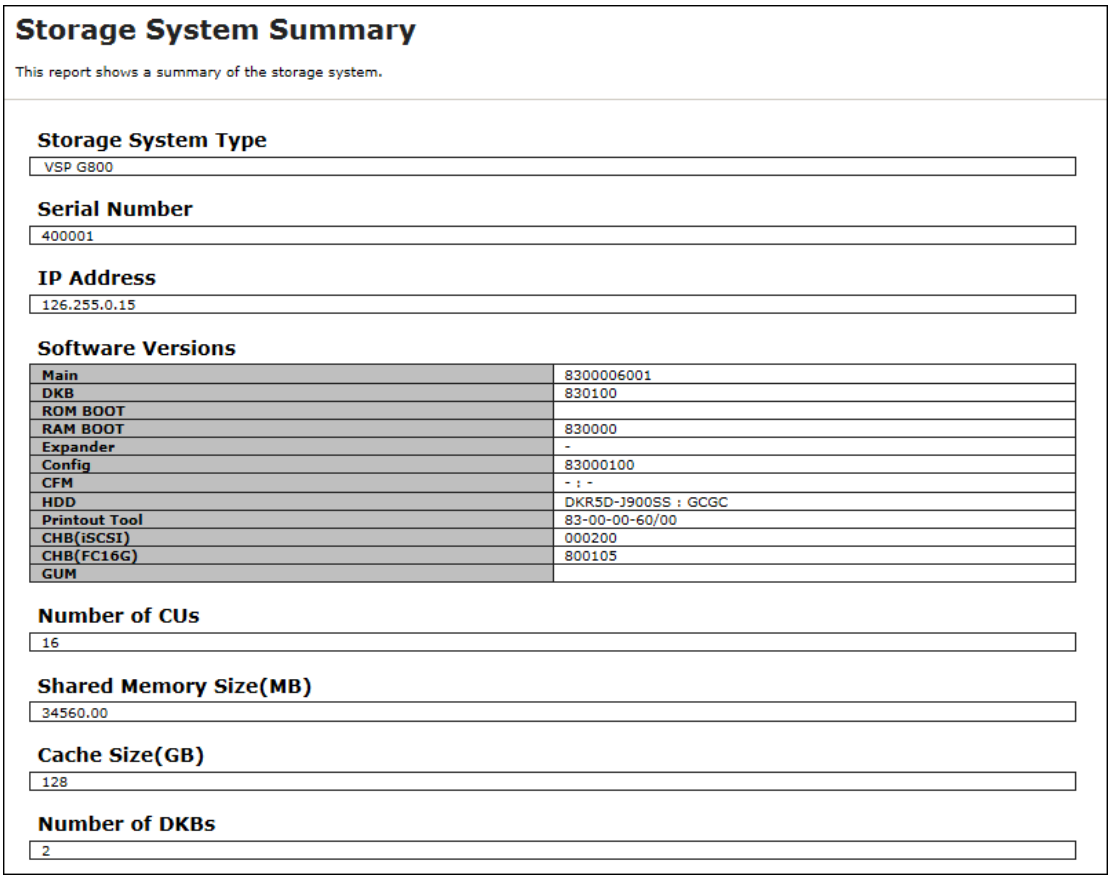
Volume Capacity(GB)

	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

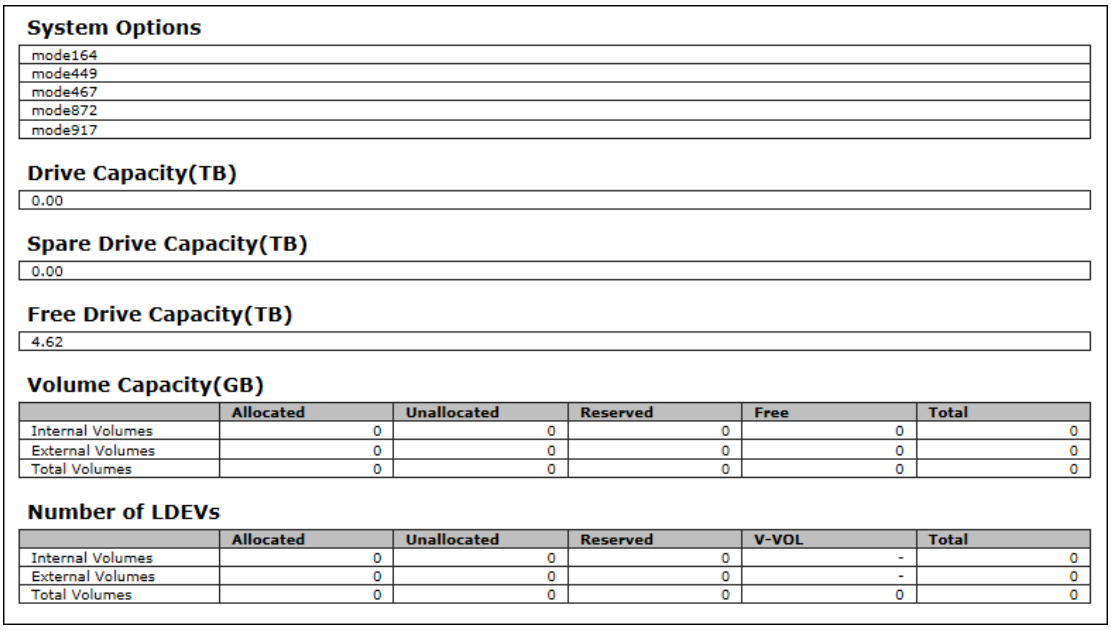
Cache Size(GB)

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
Software Versions	Version of the following programs. • Main • DKB • ROM BOOT • RAM BOOT • Expander • Config • CFM • HDD • Printout Tool • CHB (iSCSI) • CHB (FC16G) • CHB (FC32G) • GUM • Unified Hypervisor • NASFWINST • NASFW
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.** 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.

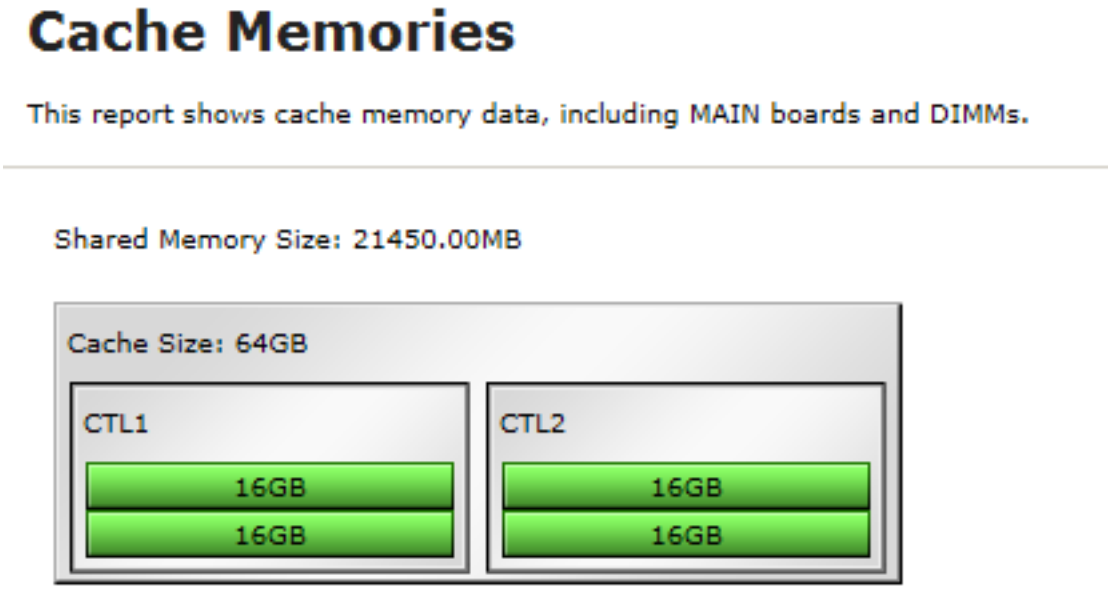


Figure 7 Cache Memories report (VSP G200)

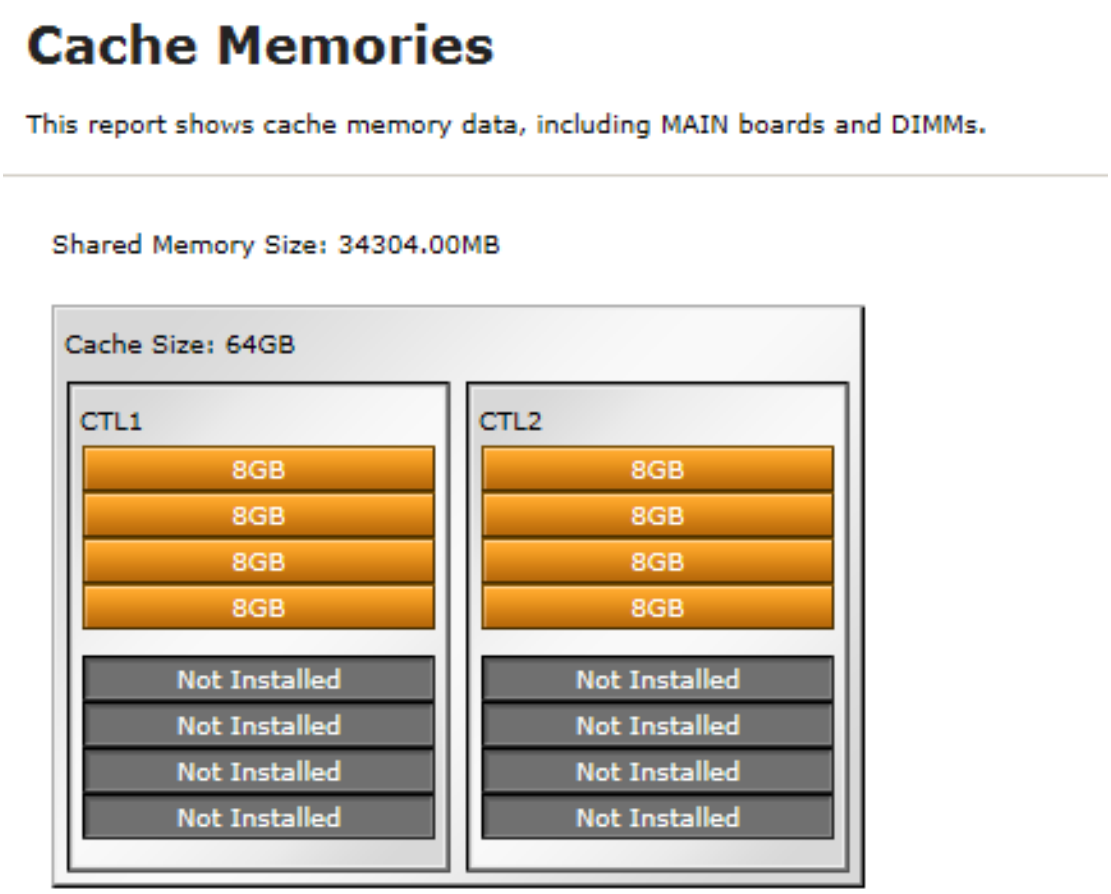


Figure 8 Cache Memories report (VSP G400, G600, VSP F400, F600)

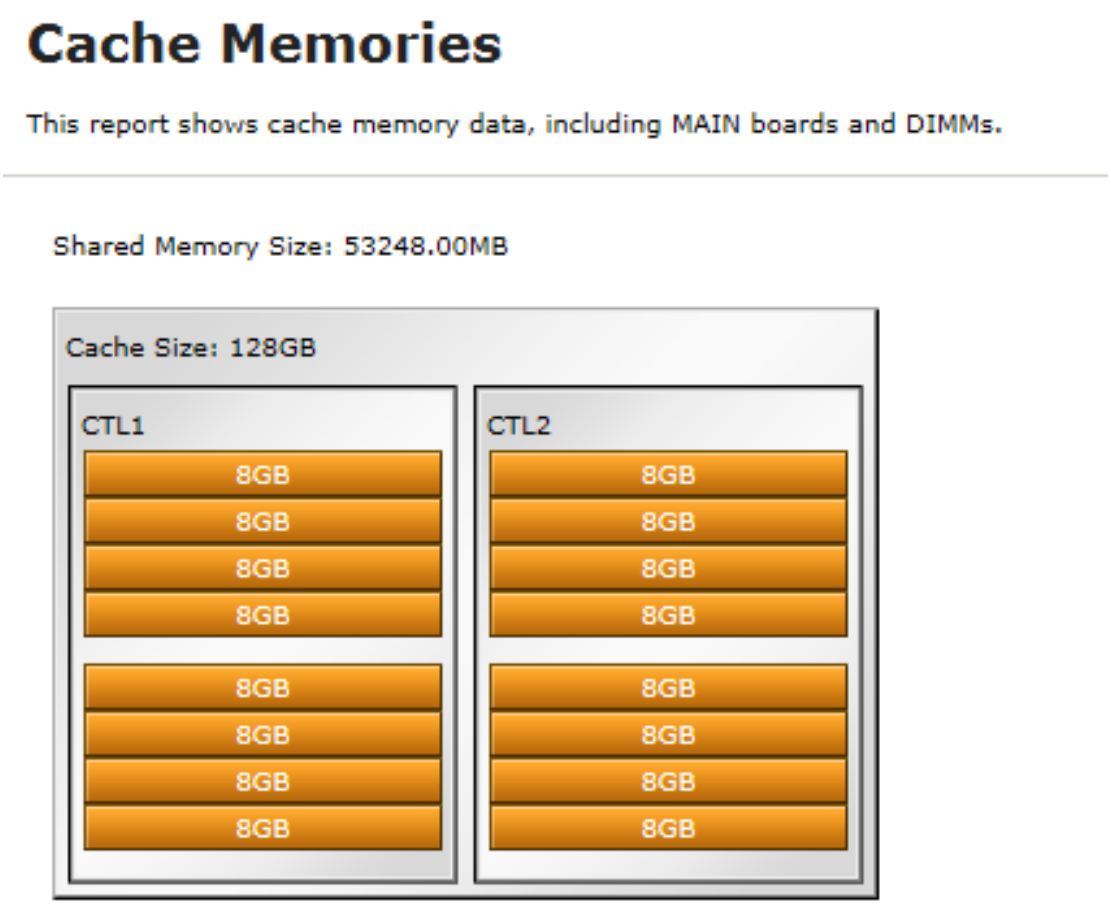


Figure 9 Cache Memories report (VSP G800, VSP F800)

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 show which channel boards are installed (green keys) and which channel boards are not installed (gray keys).

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.

If a NAS module is mounted on a channel board, the status of the module is displayed.

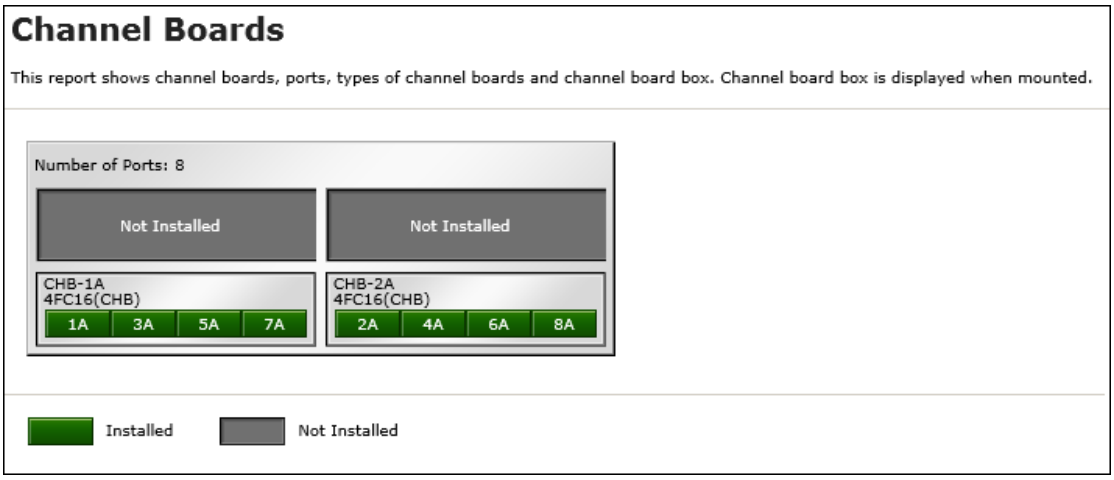


Figure 10 Channel Boards (VSP G200)

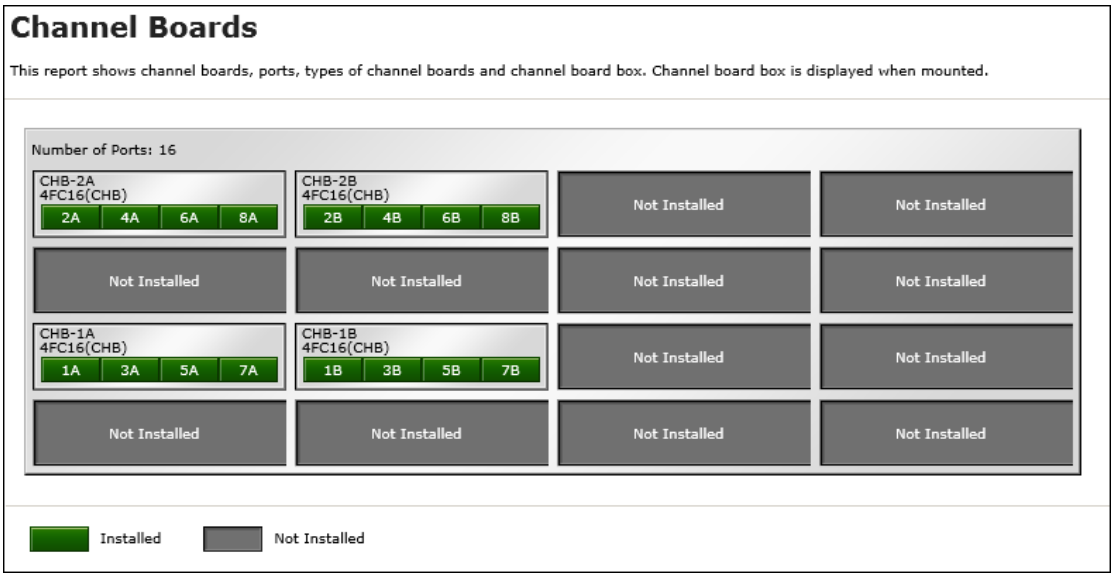


Figure 11 Channel Boards report (VSP G400, G600, VSP F400, F600)

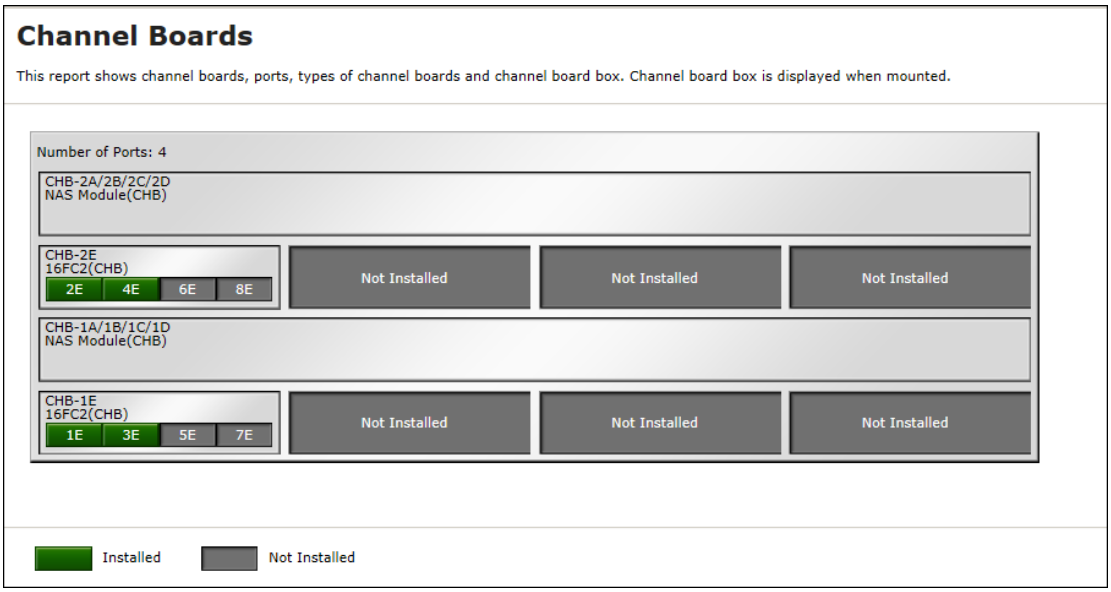


Figure 12 Channel Boards Report (when a NAS module is mounted)

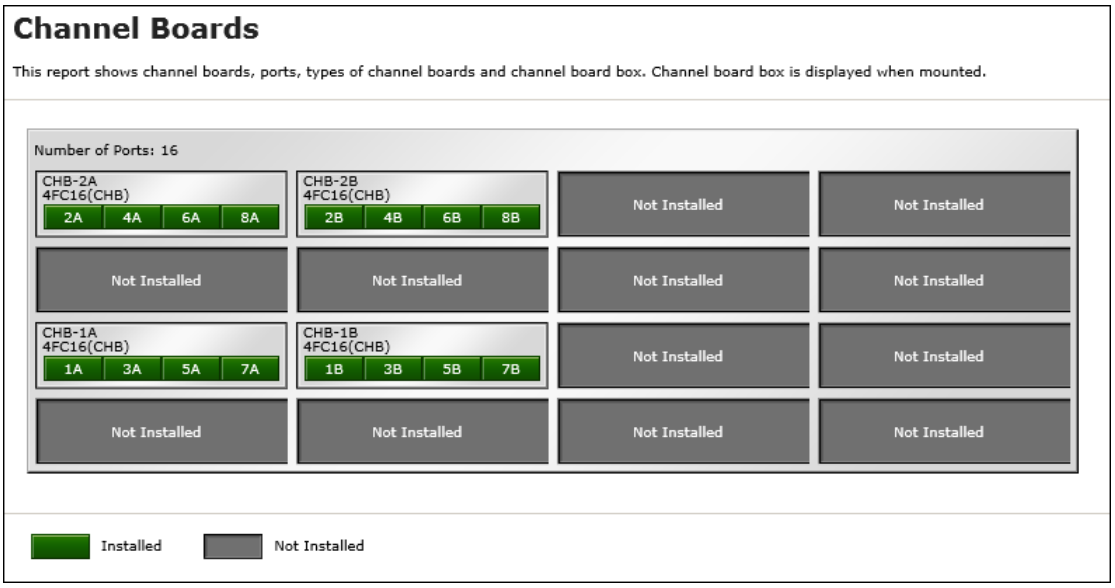


Figure 13 Channel Boards report (VSP G800, VSP F800)

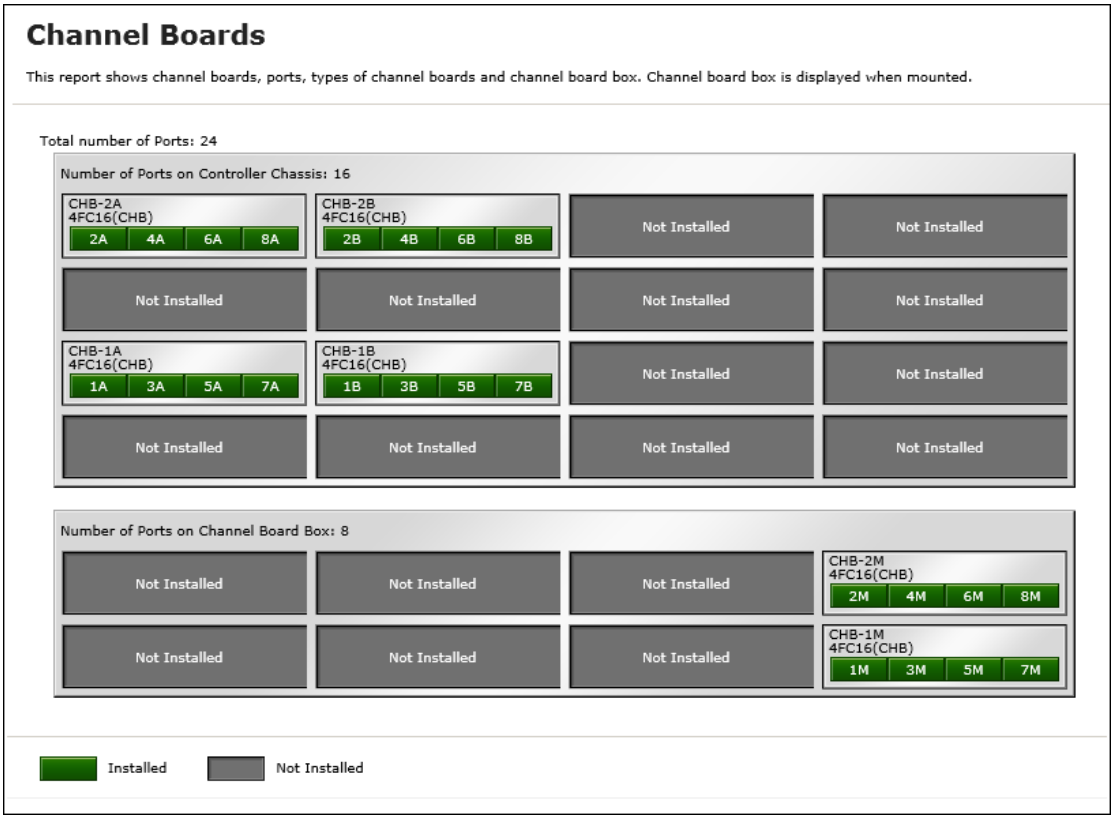


Figure 14 Channel Boards report (when a channel board box is connected)

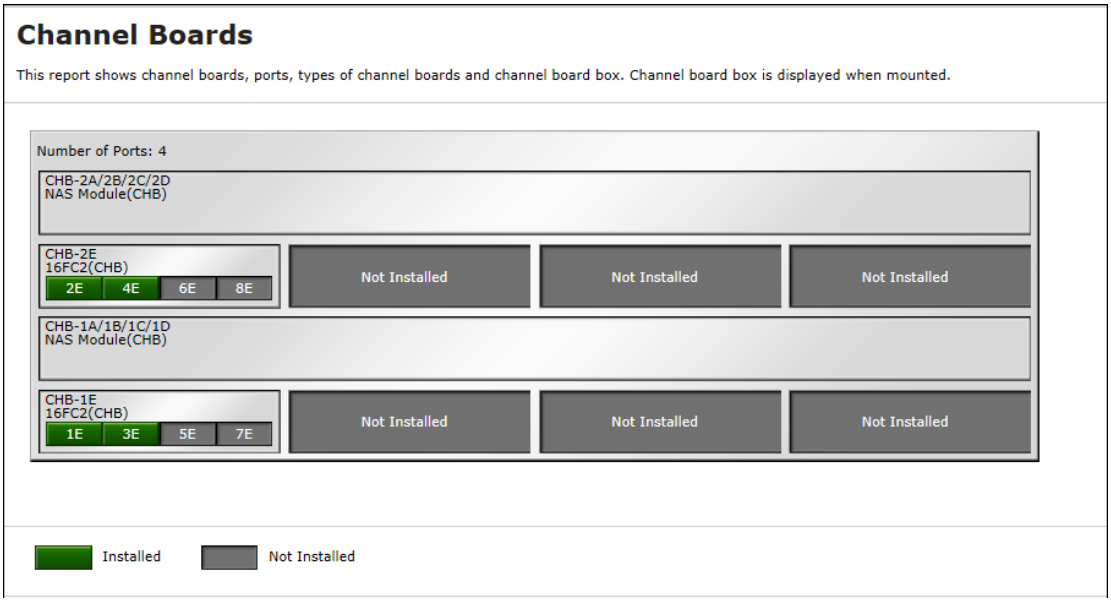


Figure 15 Channel Boards report (when a NAS module is mounted)

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.

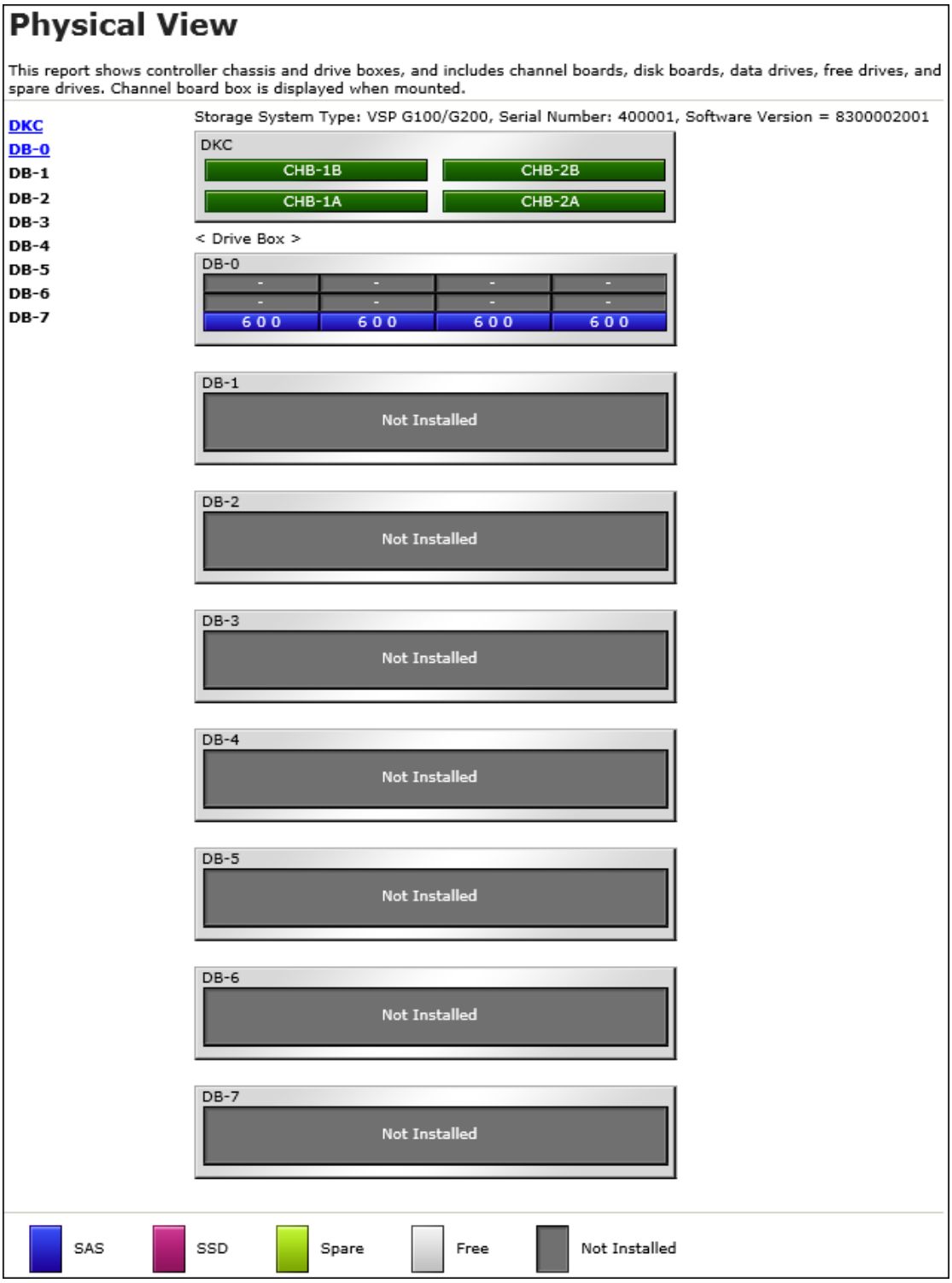


Figure 16 Physical View report (VSP G200)

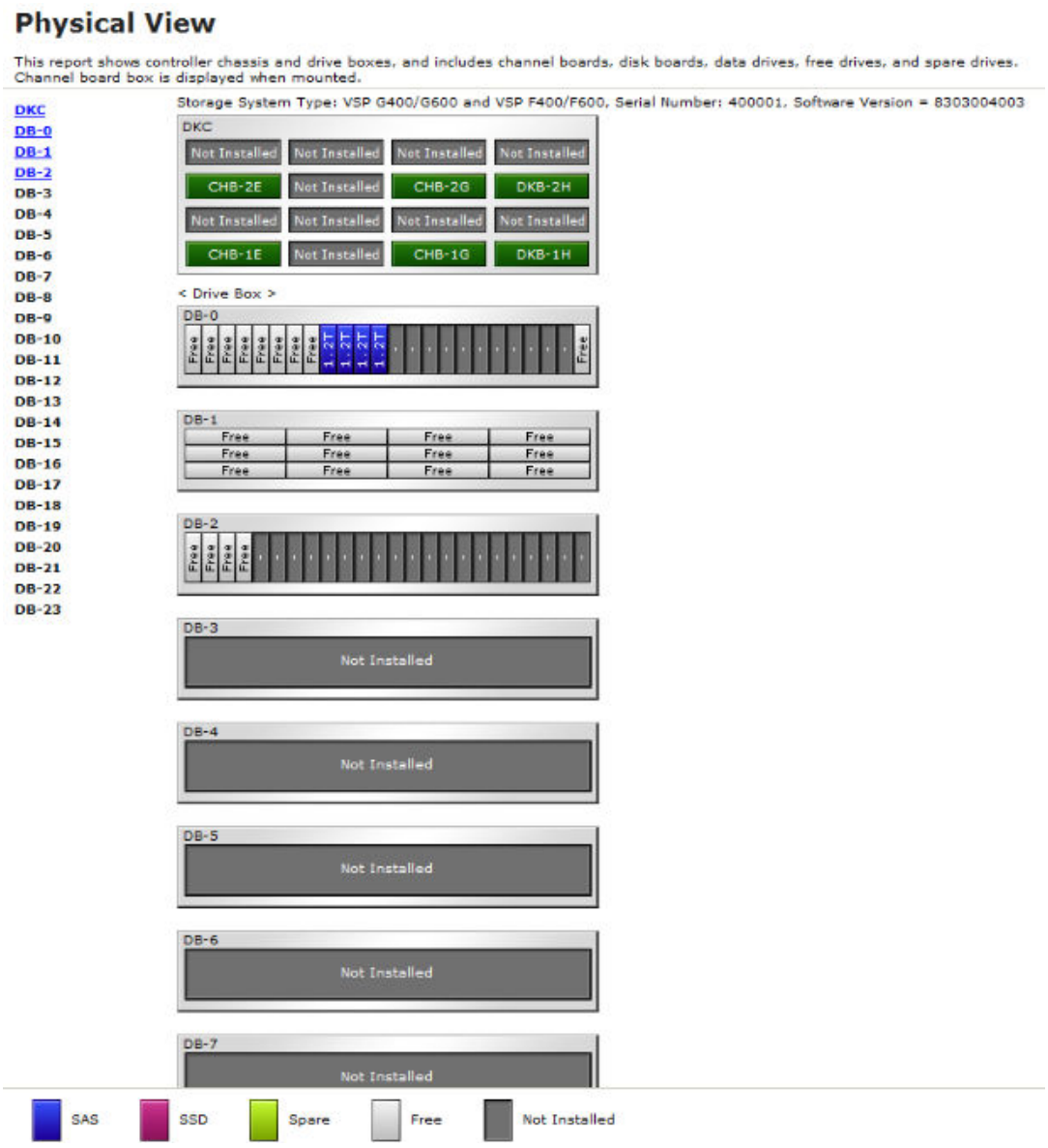


Figure 17 Physical View report (VSP G400, G600, VSP F400, F600)

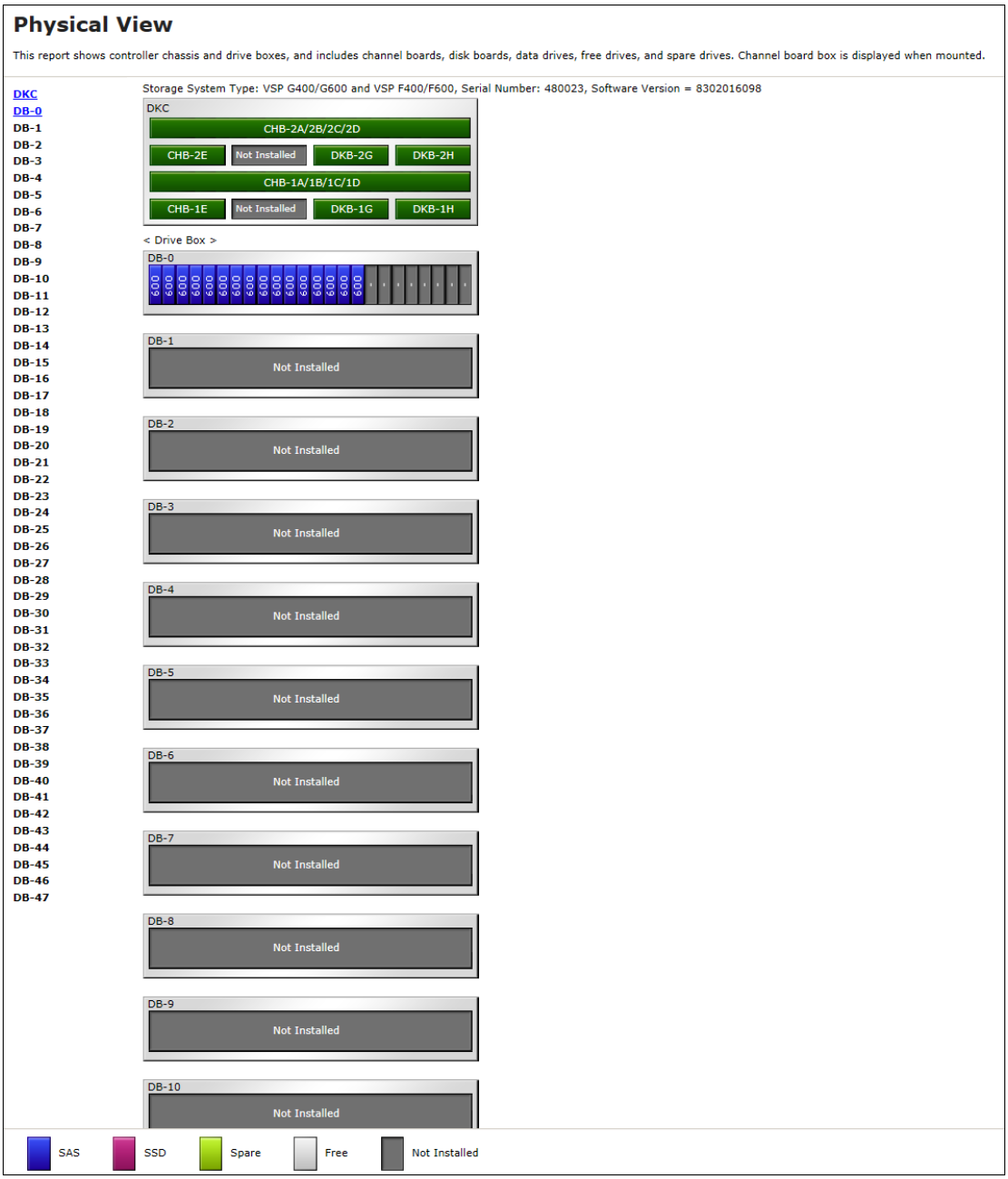


Figure 18 Physical View report (when a NAS module is mounted)

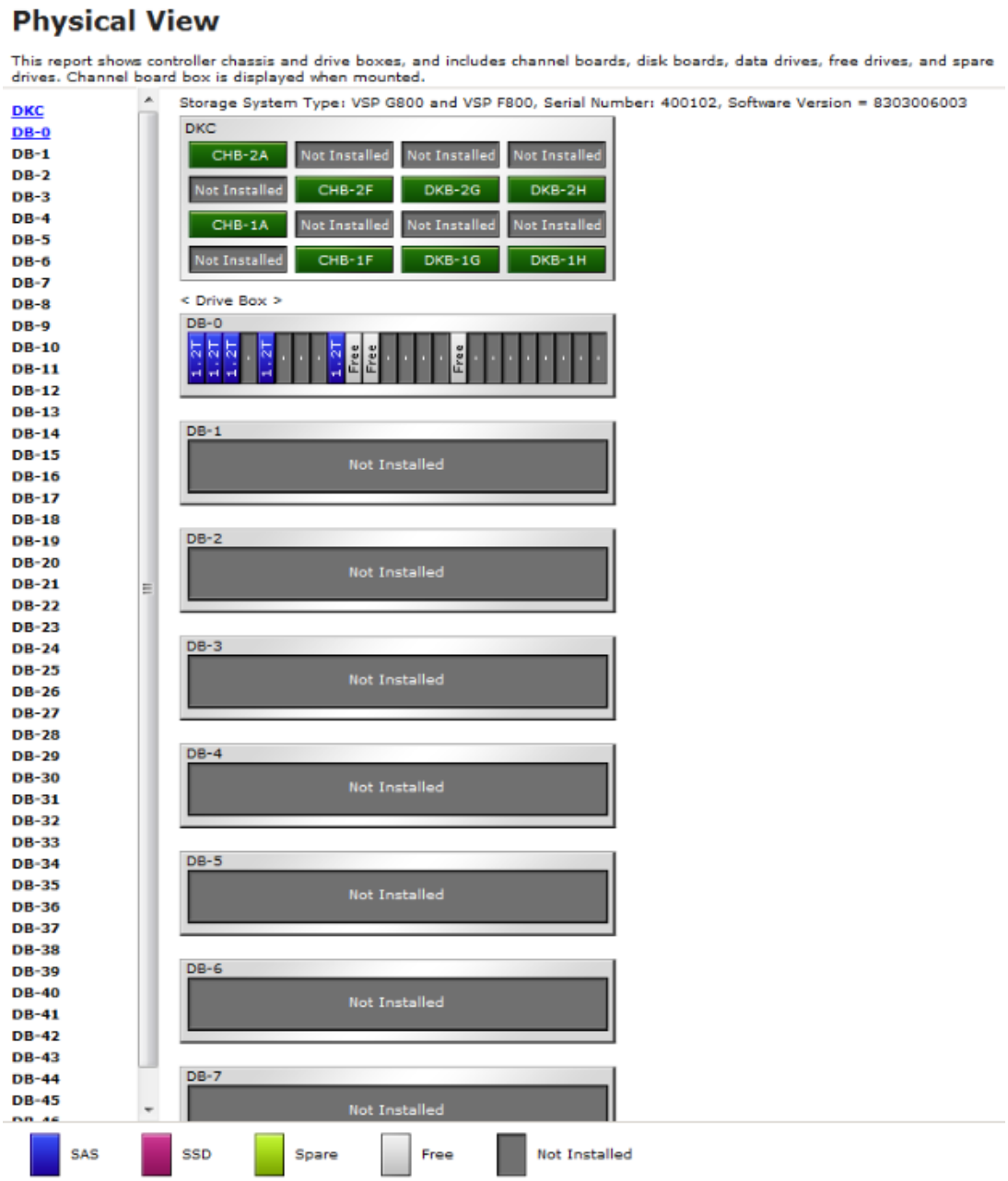


Figure 19 Physical View report (VSP G800, VSP F800)

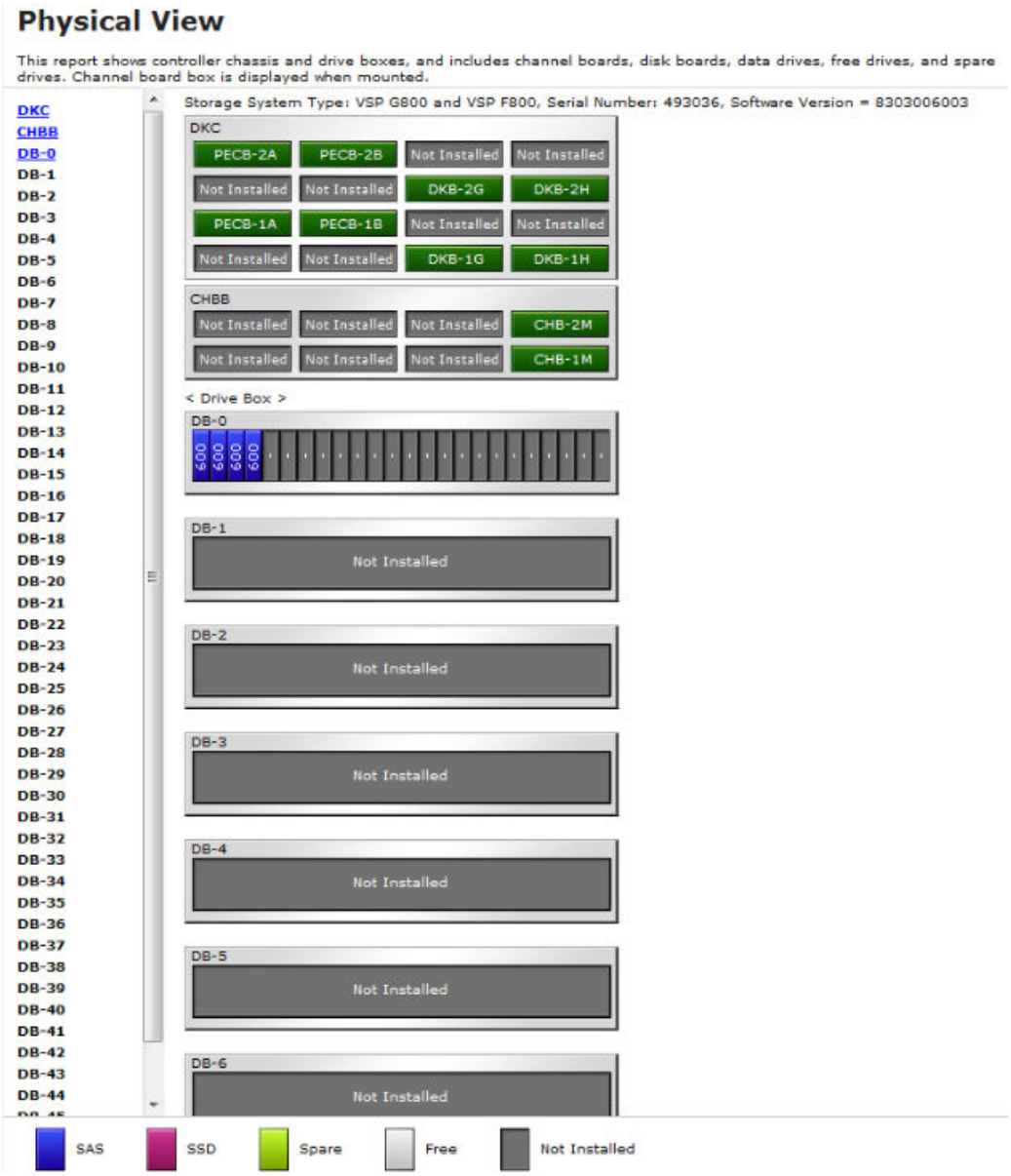


Figure 20 Physical View report (when a channel board box is connected)

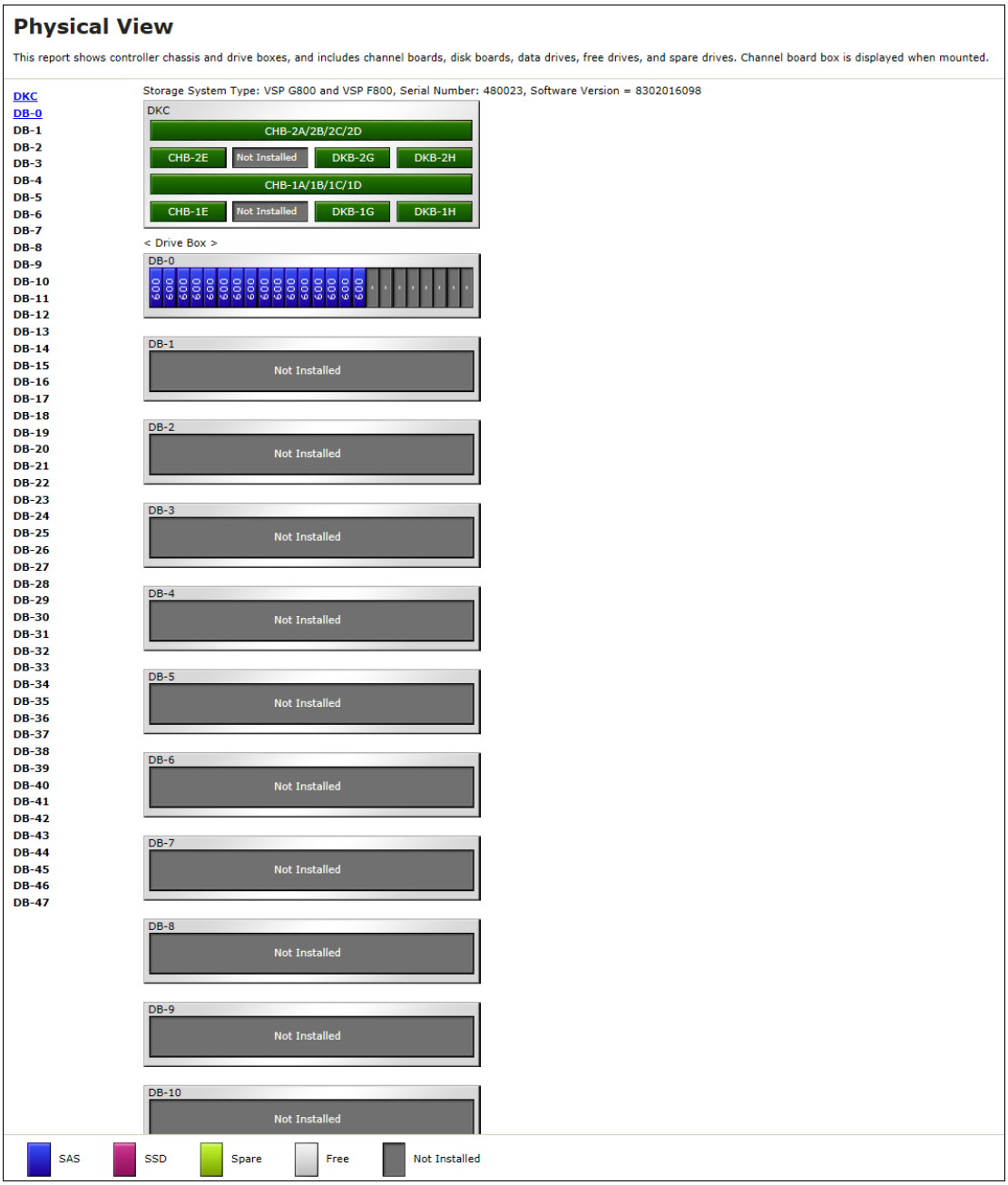


Figure 21 Physical View report (when a NAS module is mounted)

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 13 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. Information about the NAS module is not displayed in this CSV file.
Unified Hypervisor Cache Size (GB)	The cache memory capacity (blank/16/32/64) (Unit: GB) assigned for Unified Hypervisor usage within the total cache memory capacity in controller board. • Blank if Unified Mode of DkcInfo.csv is Off. This item is not displayed for VSP G200.

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. Information about the NAS module is not displayed in this CSV file.

Table 14 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 15 ChaStatus.csv file (Title: <<CHB Status>>)

Item	Content
CHB Location	CHB name (CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D if Package Type is NAS module)
PCB Status	Status of this CHB[1] (Blank if CHB location is CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D in NAS module)
Port#00, #01, …, #03	Status of ports on this CHB (Blank if CHB location is CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D in NAS module)
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 16 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

Item	Content
	• 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 17 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 18 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 19 DkcInfo.csv file (Title: <<DKC Information>>)

Item	Content
Storage System Type	Storage system type.

Item	Content
	Output example: • G200[1] • VSP G400, G600 and VSP F400, F600[2] • VSP G800 and VSP F800[3]
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
Unified Mode	Unified Mode of the storage system. • On: Operating with Unified Mode • Off: Not operating with Unified Mode This item is not displayed for VSP G200.
Notes: • To determine if the model type is VSP G200, see PpInfo.csv on page 326. ○ VSP G200: Install is Enabled for Model upgrade license • To determine whether the model type is VSP G400, VSP F400, VSP G600, or VSP F600, see PpInfo.csv on page 326. ○ VSP G400: Install is Disabled for both Model upgrade license and All Flash Array ○ VSP F400: Install is Disabled for Model upgrade license and Install is Enabled for All Flash Array ○ VSP G600: Install is Enabled for Model upgrade license and Install is Disabled for All Flash Array ○ VSP F600: Install is Enabled for both Model upgrade license and All Flash Array • To determine whether the model type is VSP G800 or VSP F800, see PpInfo.csv on page 326. ○ VSP G800: Install is Disabled for All Flash Array ○ VSP F800: Install is Enabled for All Flash Array	

DkuTempAveInfo.csv

This CSV file contains information about DB temperature for every two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit*.

DkuTempAveInfo.csv shows the average temperature as DB temperature data. The total number of items depends on the model (VSP G200: 17, VSP G400/VSP G600/VSP F400/VSP F600: 49, VSP G800/VSP F800: 97).

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and

DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period. If a failure occurs in the storage system, the correct information might not be output.

Table 20 DkuTempAveInfo.csv file (Title: <<DB temperature average Information>>)

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: *YYYY/MM/DD hh:mm:ss*
DB00 DBPS001 Temperature average	Average temperature (°C) for the two-hour period of DB00 DBPS001
DB47 DBPS472 Temperature average	Average temperature (°C) for the two-hour period of DB47 DBPS472 For VSP G200, item shows up to DB07 DBPS072. For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232.

Note: An item name is displayed as DB*xx* DBPS*xxy*. The names are listed in ascending order of the DB number. See DkuTempInfo.csv on page 300 for locations and values for DB*xx* and DBPS*xxy.*

DkuTempInfo.csv

This CSV file contains information about DB temperature for every two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit*.

DkuTempInfo.csv shows the average temperature, maximum temperature, and minimum temperature as DB temperature data. The total number of items depends on the model (VSP G200: 49, VSP G400/ VSP G600/VSP F400/VSP F600: 145, VSP G800, VSP F800: 289).

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period. If a failure occurs in the storage system, the correct information might not be output.

Table 21 DkuTempInfo.csv file (Title: <<DB temperature Information>>)

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: *YYYY*/*MM*/*DD hh*:*mm*:*ss*
DB00 DBPS001 Temperature average	Average temperature (°C) for the two-hour period of DB00 DBPS001
DB00 DBPS001 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DB00 DBPS001
DB00 DBPS001 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DB00 DBPS001
DB47 DBPS472 Temperature average	Average temperature (°C) for the two-hour period of DB47 DBPS472 For VSP G200, item shows up to DB07 DBPS072. For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232.
DB47 DBPS472 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DB47 DBPS472 For VSP G200, item shows up to DB07 DBPS072. For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232.
DB47 DBPS472 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DB47 DBPS472 For VSP G200, item shows up to DB07 DBPS072. For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232.

***Note:** An item name is displayed as DB*xx* DBPS*xxy*. The names are listed in ascending order of the DB number.

The following tables list DB*xx* and DBPS*xxy*: *xx* values, where *xx* is a value from 00 to 07 (VSP G200), 00 to 23 (VSP G400, G600, VSP F400, VSP F600), or 00 to 47 (VSP G800, VSP F800).

DB #	0	1	2	3	4	5
xx	00	01	02	03	04	04
DB*xx*	DB00	DB01	DB02	DB03	DB04	DB05
DB*xxy*	DBPS00y	DBPS01y	DBPS02y	DBPS03y	DBPS04y	DBPS05y

DB #	42	43	44	45	46	47
xx	42	43	44	45	46	47
DB*xx*	DB42	DB43	DB44	DB45	DB46	DB47
DB*xxy*	DBPS42y	DBPS43y	DBPS44y	DBPS45y	DBPS46y	DBPS47y

The following table lists the DBPS*xxy: y* values (where DB# is 0 and *xx* is 00)

DB#	0	
y	1	2
DBPS*xxy: y*	DBPS001	DBPS002

DkuTempMaxInfo.csv

This CSV file contains information about DB temperature for every two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit*.

DkuTempMaxInfo.csv shows the maximum temperature as DB temperature data. The total number of items depends on the model (VSP G200: 17, VSP G400/VSP G600/VSP F400/VSP F600: 49, VSP G800/VSP F800: 97).

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period. If a failure occurs in the storage system, the correct information might not be output.

Table 22 DkuTempMaxInfo.csv file (Title: <<DB temperature maximum value Information>>)

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: *YYYY*/*MM*/*DD hh*:*mm*:*ss*
DB00 DBPS001 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DB00 DBPS001
DB47 DBPS472 Temperature maximum value	Maximum temperature (°C) for the two-hour period of DB47 DBPS472 For VSP G200, item shows up to DB07 DBPS072.

Item	Description
	For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232.

Note: An item name is displayed as DB*xx* DBPS*xxy*. The names are listed in ascending order of the DB number. See DkuTempInfo.csv on page 300 for locations and values for DB*xx* and DBPS*xxy.*

DkuTempMinInfo.csv

This CSV file contains information about DB temperature for every two hours. A record is DB temperature information obtained from the environment monitor. A record output to the first line shows the latest temperature information. Because DB temperature information is measured by DBPS, items are displayed in this unit*.

DkuTempMinInfo.csv shows the average temperature as DB temperature data. The total number of items depends on the model (VSP G200: 17, VSP G400/VSP G600/VSP F400/VSP F600: 49, VSP G800/VSP F800: 97).

The DB temperature data displayed in DkuTempAveInfo.csv (average temperature only), DkuTempMaxInfo.csv (maximum temperature only), and DkuTempMinInfo.csv (minimum temperature only) is the same value as the DB temperature data for DkuTempInfo.csv.

If the system is in maintenance mode or the SVP is rebooted, the data that is output every two hours might not contain data for the period. If a failure occurs in the storage system, the correct information might not be output.

Table 24 DkuTempMinInfo.csv file (Title: <<DB temperature minimum value Information>>)

Item	Description
Date	Year, month, and date when temperature data was acquired in the format: *YYYY/MM/DD hh:mm:ss*
DB00 DBPS001 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DB00 DBPS001
DB47 DBPS472 Temperature minimum value	Minimum temperature (°C) for the two-hour period of DB47 DBPS472 For VSP G200, item shows up to DB07 DBPS072. For VSP G400, VSP G600, VSP F400, VSP F600, item shows up to DB23 DBPS232.

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*. Information about the NAS module is not displayed in this CSV file.

Table 25 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
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

Item	Content
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 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), 32FC4R (CHB) • iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB)
IP Address	IP address for an iSCSI target of an external storage system • IPv6: *XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX*:*XXXX* (hexadecimal) • IPv4:

Item	Content
	XXX.XXX.XXX.XXX (decimal) • Blank if "Package Type" is iSCSI.
TCP Port Number	TCP port number (1 through 65535) for the 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.

If a failure occurs in the storage system, the correct information might not be output.

Table 26 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: *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)

Item	Description
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*. Information about the NAS module is not displayed in this CSV file.

Table 27 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*. Information about the NAS module is not displayed in this CSV file.

Table 28 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

Item	Content
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 29 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, 2PORT)

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. Information about the NAS module is not displayed in this CSV file.

Table 30 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:	

Item	Content
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. Information about the NAS module is not displayed in this CSV file.

Table 31 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) Blank if "IPv6 | Mode" is Disabled.
Channel Speed	Data transfer speed of the port (10 Gbps)
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

Item	Content
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
IPv6 | Global Address 2	IPv6 global address 2 of the port • Output example: *xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx*:*xxxx* (hexadecimal) • Output example: Auto Auto is displayed if the global address 2 is automatically set. Blank if "IPv6 | Mode" is Disabled.

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. Information about the NAS module is not displayed in this CSV file.

Table 32 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 33 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 34 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 35 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*.

Table 36 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 • Deduplication system data volume • 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.

Item	Content
	(MPU-10, MPU-11, MPU-20, MPU-21)
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	Indicates whether the parity group identified by ECC Group is encrypted. • For internal volumes: Enabled (encrypted) or Disabled (not encrypted) • 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.
ALUA Mode	Indicates whether the ALUA mode is enabled. • Enabled: ALUA mode is enabled. • Disabled: ALUA mode is disabled.
Accelerated Compression	Indicates whether accelerated compression is enabled. For internal volumes: • Enabled: accelerated compression is enabled. • Disabled: accelerated compression is disabled. If the parity group with LDEV does not support accelerated compression, a blank space is displayed. Also, for external volumes, a blank is displayed.

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 37 LdevStatus.csv file (Title: <<LDEV Status>>)

Item	Content
VDEV#	Virtual device number in which the LDEV is defined
VDEV Status	VDEV status of "VDEV#" • 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*.

Table 38 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)

Item	Content
	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*.

Table 39 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 CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D if Package Type is NAS module.

Package Type	CHB type for CHB Location:
	• Fibre:
	  ○ 8FC4 (CHB)
	  ○ 16FC2 (CHB)
	  ○ 32FC4R (CHB)
	• iSCSI:
	  ○ 10iSCSI2o (CHB)
	  ○ 10iSCSI2c (CHB)
	• NAS module:
	  ○ NAS module (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

Item	Description
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) or 32FC4R (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
Asymmetric Access State	Asymmetric access status (output only for an open system CHA that is Fibre or FCoE) Indicates the asymmetric access status: • Active/Optimized: Prioritized • Active/Non-Optimized: Lower priority Blank if "Package Type" is iSCSI

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*.

Table 40 LunPortInfo.csv file (Title: <<LUN Port Information>>)

Item	Content
Port	Port name.
Security Switch	The setting status of the security switch: • On • Off • Blank if "Package Type" is NAS module
Port Address	Port address (2-digit hexadecimal number) Blank if "Package Type" is iSCSI or NAS module
Loop ID	Port address (0 - 125, decimal) Blank if "Package Type" is iSCSI or NAS module
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch: • On • Off • Blank if "Package Type" is iSCSI or NAS module
Connection	One of the Fibre topology settings: • Point to Point • FC-AL • Blank if "Package Type" is iSCSI or NAS module
Channel Speed	Channel Speed of this port • 1 Gbps • 2 Gbps • 4 Gbps

Item	Content
	• 8 Gbps • 10 Gbps • 16 Gbps • 32 Gbps • Auto • Blank if "Package Type" is NAS module
WWN	WWN of this port (hexadecimal number) Blank if "Package Type" is iSCSI or NAS module
CHB Location	CHB on which the port is installed. CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D if "Package Type" is NAS module.

Package Type	CHB type for CHB Location
	• Fibre:
	  ○ 8FC4 (CHB)
	  ○ 16FC2 (CHB)
	  ○ 32FC4R (CHB)
	• iSCSI:
	  ○ 10iSCSI2o (CHB)
	  ○ 10iSCSI2c (CHB)
	• NAS module:
	  ○ NAS Module (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) or 32FC4R (CHB)

MicroVersion.csv

This CSV file contains information about software versions.

Table 41 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)

Item	Content
CHB (FC32G)	32G FC protocol chip firmware version (8 digits)
CHB (iSCSI)	CHB(iSCSI) protocol chip firmware version (8 digits)
GUM	GUM firmware version (8 digits)
Unified Hypervisor	Unified Hypervisor version (8 digits) • The version is displayed in each CL1, CL2. • This item is not displayed in VSP G200.
NASFWINST	NASFWINST version (9 digits) • The version is displayed in each CL1, CL2. • This item is not displayed in VSP G200.
NASFW	NASFW version (9 digits) • The version is displayed in each CL1, CL2. • This item is not displayed in VSP G200.

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 42 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) 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)

Item	Content
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 43 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 44 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 The MPU#01 or MPU#03 line is blank if Unified Mode of DkcInfo.csv is On. • 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# The display in MPU#00-01, MPU#00-03, MPU#01-01, or MPU#01-03 is blank if Unified Mode of DkcInfo.csv is On. For VSP G200, MPU#00-00 to 03 only
CMG#00-00 to 01	Path status[1] with the cache module for the CTL number

Item	Content
CMG#01-00 to 01	(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 The display in MPU#00-01, MPU#00-03, MPU#01-01, or MPU#01-03 is blank if Unified Mode of DkcInfo.csv is On.
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 45 MpPcbStatus.csv file (Title: <<MP PCB Status>>)

Item	Content
MPU ID	MP unit ID (MPU-10, MPU-11, MPU-20, MPU-21) MPU-10 and MPU-20 are displayed if Unified Mode of DkcInfo.csv is On.
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 46 PcbRevInfo.csv file (Title: <<PCB Revision Information>>)

Item	Content
Cluster#	Cluster number • 1

Item	Content
	• 2
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 47 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 48 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

Item	Content
Device Type	Drive type • 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 for 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
Accelerated Compression	Accelerated compression setting. • Enabled: accelerated compression is enabled. • Disabled: accelerated compression is disabled. If the parity group with PDEV does not support accelerated compression, or if the ECC Group is Spare Drive, a blank space is displayed.

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 49 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 50 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

PkInfo.csv

This CSV file contains information about channel boards (CHBs). A record is created for each CHB.

Table 51 PkInfo.csv file (Title: <<PK>>)

Item	Content
CHB Location	CHB name CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D if "Package Type" is NAS module.
Port#	Number of the port installed on the CHB (2-digit hexadecimal number)
Port	Name of port installed on the CHB
Package Type	CHB type indicated on the CHB Location • Fibre: 8FC4 (CHB), 16FC2 (CHB), 32FC4R (CHB) • iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB) • NAS module: NAS module (CHB)
SFP Kind	SFP (Small Form factor Pluggable) Kind • Short Wave • Long Wave • Blank if "Package Type" is 10iSCSI2c (CHB) or NAS module (CHB).
SFP Status	SFP Status: • Normal • Failed • Not Fix • Blank if "Package Type" is 10iSCSI2c (CHB) or NAS module (CHB).
Fabric	One of the Fibre topology settings indicating the setting status of the Fabric switch: • On • Off • Blank if "Package Type" is iSCSI or NAS module.
Connection	One of the Fibre topology settings • Point to Point • FC-AL • Blank if "Package Type" is iSCSI or NAS module.
Port Address	Port address (00 to ff, 2-digit hexadecimal number) Blank if "Package Type" is iSCSI or NAS module.
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 or NAS module.
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) or 32FC4R (CHB).
SFP Data Transfer Rate	Maximum transfer rate of SFP which the mounted package supports. • 8G • 10G • 16G • 32G • Blank if the "Package Type" is 10iSCSI2c (CHB) or NAS module (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 229.

Table 52 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
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 53 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

Item	Content
	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 54 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 55 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 56 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*.

Table 57 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.

Item	Content
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 or NAS module.
Nickname	Nickname of the host Blank if the "Package Type" is iSCSI or NAS module.
Host Group#	Host group number (00 to ff, hexadecimal) iSCSI target ID will be output if the "Package Type" is iSCSI.
CHB Location	Name of port installed on the CHB CHB-1A/1B/1C/1D or CHB-2A/2B/2C/2D if "Package Type" is NAS module.
Package Type	CHB type indicated on the CHB Location • Fibre: 8FC4 (CHB), 16FC2 (CHB), 32FC4R(CHB) • iSCSI: 10iSCSI2o (CHB), 10iSCSI2c (CHB) • NAS module: NAS module (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) or 32FC4R (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, and so on).

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

Hitachi 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 a 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 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. Encryption keys can be backed up to, and restored from, 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 a 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

A

accelerated data compression 75
accessing a storage system
  without the management software 58
account
  release lock 154
Active Directory authentication 188
adding
  RADIUS servers 198
adding SVP to trusted zone 49
administration
  tasks 18
  tools 18
administrator password 118
Adobe Flash 46
Alert notifications 217–219
  configuring 218
  email 220
  SNMP 222
  Syslog 220
audit log
  exporting 241
Audit logs
  settings 240
authentication server 162
Authentication server
  protocols 163
authentication servers 165
Authentication servers 164
authorization server 162
authorization servers 165
Authorization servers
  requirements 164

B

backing up user accounts 143
block storage
  configuring 63
built-in groups 156
built-in user 47

C

Cache Memories report 283
certificate files 213
certificates
  obtaining 208
certificates, obtaining 208
changing 113, 121
changing a user's password 151
Changing assigned resource groups 161
changing permissions 152
changing the date and time 116
  controller settings 116
  SVP clock 116
Channel Boards report 285
cipher suite 212
client computer
  UNIX requirements 43
  Windows requirements 42
Configuration files
  creating 166
configuring Active Directory groups 192
configuring active directory servers 189
creating
  user accounts 148
Creating a keypair 206
creating a report 123, 245
creating a user account 159
CSV files 295

D

dashboard 21
  analyzing data 24
data compression 75
Data Retention Utility license
  removal 236
date 121
deduplication 96
deleting a report 245
deleting a user account 154
Device Manager - Storage Navigator 26
  accessing 89
  using 89

Device Manager- Storage Navigator
client setup for 41
disabling a user account 153
disabling user accounts 137
displaying
RADIUS servers 200
displaying RADIUS servers 197
DKU 299, 303
Dump files
collecting 246

E

EVS
details 107
inventory 106
EVSs
creating 106
exports
creating 110
details 110
updating 110
external parity groups 75

F

fabric switches
adding 52, 64
supported models 66
system requirements 66
file pool
details 105
file pools
creating 104
expanding 105
inventory 103
managing 102
file storage
configuring 102
file system
inventory 107
file systems
creating 108
deleting 108
expanding 109
managing 107
mounting/unmounting 108
updating 109
viewing details 108
Firefox
configuring 45
firewall setup 44, 117
force release system lock 119

G

general 219

H

HCS certificates 204
deleting 204
registering 204
HduInfo.csv 308
HDvM - SN configuration files
restoring 115
HDvM SN configuration files
backing up 114
hosts
updating 96
Hosts report 265
HTTP communication to SVP 132
blocking 132

I

installation
in a DHCP environment 33
in a static environment 35
using the application installer 32
installation verification 38
Internet Explorer
configuring 45
inventory 25
IPv6, configuring communications 117

K

Kerberos configuration file 172

L

LDAP configuration file 166
license capacities
unlicensed software 232
license keys
expiration 238
overview 230
permanent 230
term 231
types 230
viewing information 237
License keys 229
disabling 235
emergency 231
enabling 235
installing 235
managing 232, 233
removing a software license 236
temporary 231
logging in 39, 47
Logical Devices report 266
login message 119
LUNs report 268

M
maintenance utility 27
starting 56
management client
setup 41
management software architecture 18
modules 121
MP Unit Details report 269
MP Units report 268

N
NAS 121
NAS Manager 28
accessing 91
using for advanced file storage configuration 91
network communication settings 117
Network permissions 118
Network settings 117

O
onboard
workflow 51
overview
Hitachi Storage Advisor 19

P
parity groups
creating 54, 67
initializing 72
inventory 72
reserved for NAS firmware 72
status 72
Parity Groups report 270, 277
parity groups, creating
advanced method 70
basic method 68
password
allowable characters and symbols 148
changing a user's 151
local, changing 21
passwords
changing 180
permissions, changing 152
Physical Devices report 271
Physical View report 289
PKCS#12 format 210
pool creation
basic method, calculation of pool sizes 80
pools
creating 76
creating with advanced method 80
expanding 82
inventory 76
updating 82
viewing details 82
pools, creating 78
ports
enabling security 64
Ports report 273
Power Consumption report 275
primary SVP 120

R
RADIUS configuration file 169
RADIUS server
adding 198
RADIUS server, accessing 164
RADIUS servers
displaying 197, 200
raidinf add relocationlog 256
raidinf add report 252
raidinf delete relocationlog 258
raidinf delete report 253, 254, 259, 260
raidinf download relocationlog 257
raidinf get relocationloginfo 258
raidinf get reportinfo 255
releasing 132
removing user accounts 141
Report Configuration Tool Command Reference 249
Report Viewer window 245
reports
Cache Memories 283
Channel Boards 285
CHAP Users 262
Disk Boards 263
downloading 244
Host Groups 264
Hosts 265
iSCSI Targets 264
Logical Devices 266
LUNs 268
MP Unit Details 269
MP Units 268
Parity Groups 270, 277
Physical Devices 271
Physical View 289
Ports 273
power consumption 275
Spare Drives 276
Storage System Summary 278
table view 262
requirements
management clients 41
resetting passwords 180
resource groups 156
Resource groups
changing 161
resources 25
restoring user account information 144
roles 134, 156
Roles 90, 155

root password
changing 38

S

Security certificates 213
self-signed certificate 208
servers
adding 53, 93
attach existing volumes 94
create and attach volumes 94
delete 94
details 95
edit 94
inventory 94
Servers
connecting authentication and authorization servers 165
setting up management client 41
setting up user accounts 135
Settings menu 21
shares
adding AD groups to 111
creating 110
details 111
updating 112
shares and exports
inventory 109
managing 109
signed certificates 208
updating 210
Signed certificates 208
notes 211
returning to default 211
signed private key 208
signed public key 208
Spare Drives report 276
spares
managing 72
SsdDriveInfo.csv 327
SSdDriveInfo.csv 327
ssl certificate 40
SSL certificate passphrase 209
SSL certificates 205
converting 210
SSL communication settings 205
SSL-encrypted communications
creating a private keypair 206
creating a public key 207
starting
maintenance utility 56
Storage Navigator
creating a user account 159
storage system
editing 93
updating 93
storage system information 113
Storage system reports 244
Storage System Summary report 278
storage systems
adding 51
deleting 87
details 87
editing 87
inventory 86
managing 86
SVP
host name 120
SVP, adding to trusted sites 49
Syslog server
send test message 242
setup 240
system 121
System administration overview 17
system architecture 18
System configuration 61
system lock 119

T

Test messages 222
email 223
SNMP 224
Syslog 223
There is a problem with this website's security certificate 213
tiers
managing 92
time 121

U

unified management
overview 20
UNIX
requirements 43
user accounts
creating 148, 159
deleting 154
disabling 153
managing 147
user administration 134, 146
overview 146
user groups
deleting 161
managing 155
names 160
roles 90, 155, 156, 158
User groups
permissions 160

V

viewing a report 244
virtual file server
deleting 106
details 107

enabling/disabling 106
inventory 106
renaming 107
virtual file servers
creating 106
volumes
attaching 85, 98
create and attach 83
expanding 100
inventory 101
managing 96
updating 100
volumes, creating 83, 97

W

web browser
configuring Firefox 45
configuring Internet Explorer 45
Web browser
configuring 44
Windows requirements 42

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

Contact Us
www.hds.com/en-us/contact.html

Hitachi Data Systems

MK-94HM8016-06
October 2016