Hitachi Virtual Storage Platform Gx00, Nx00, and Fx00

SVOS 7.4.1

SNMP Agent User Guide

This document describes and provides instructions for using the SNMP Agent on Hitachi Virtual Storage Platform G200, G400, G600, and G800, and Hitachi Virtual Storage Platform N400, N600, and N800 storage systems and Hitachi Virtual Storage Platform F400, F600, and F800 all-flash arrays.

MK-94HM8015-08
May 2019

© 2017, 2019 Hitachi Vantara Corporation. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara 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 Vantara Corporation at https://support.HitachiVantara.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 Vantara 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.

EXPORT CONTROLS - Licensee will comply fully with all applicable export laws and regulations of the United States and other countries, and Licensee shall not export, or allow the export or re-export of, the Software, API, or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

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, RS6000, 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 web site are properties of their respective owners.

Contents

Preface 5
Intended audience 6
Product version 6
Release notes 6
Changes in this revision 6
Referenced documents 6
Document conventions 7
Conventions for storage capacity values 8
Accessing product documentation 9
Getting help 9
Comments 9

1 Introduction 11
SNMP Manager overview 12
How SNMP works 12
Management Information Base overview 13
SNMP Agent configuration 13
SNMP Agent overview 14
SNMP traps 15
SNMP Agent operations 15
SNMP Agent reported errors 16
Component status information from SNMP Manager 16

2 Using SNMP 19
Editing alert settings 20
Managing SNMP trap notification 20
Adding trap notification for SNMP v1 and v2c 20
Adding trap notification for SNMP v3 22
Changing trap notification for SNMP v1 and v2c 23
Changing trap notification for SNMP v3 24
Deleting SNMP trap notification 25
Managing SNMP request authentication 26
Adding request authentication for SNMP v1 and v2c 26
Adding request authentication for SNMP v3 27

Changing request authentication for SNMP v1 and v2c..... 29
Changing request authentication for SNMP v3.....30
Deleting SNMP request authentication.....31
Testing SNMP trap reports.....32

3 SNMP supported MIBs.....33

SNMP Agent failure report trap contents..... 34
SNMP Agent extension trap types.....34
Standard MIB specifications..... 35
MIBs supported by SNMP Agent.....35
SNMP Agent MIB access mode.....36
Example object identifier system.....36
MIB mounting specifications supported by SNMP Agent.....37
Extension MIB specifications..... 38
Extension MIB configuration..... 38
raidExMibName..... 40
raidExMibVersion..... 40
raidExMibAgentVersion.....40
raidExMibDkcCount.....40
raidExMibRaidListTable.....40
raidExMibDKCHWTable.....41
raidExMibDKUHWTable.....42
raidExMibTrapListTable.....43

4 SNMP failure trap reference..... 45

SNMP failure trap reference codes.....46
Obtaining drive box and drive numbers.....60

5 Troubleshooting.....61

Getting help.....62
Solving SNMP problems..... 62

Glossary.....63

Index.....67

Preface

This document describes and provides instructions for using the SNMP Agent on VSP Gx00, VSP Nx00, and VSP Fx00 models.

Please read this document carefully to understand how to use this product, and maintain a copy for reference purposes.

- Intended audience
- Product version
- Release notes
- Changes in this revision
- Referenced 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 install, configure, and operate VSP Gx00, VSP Nx00, and VSP Fx00 models.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- Hitachi Virtual Storage Platform Gx00 or Fx00 models and the *Product Overview*.
- The Hitachi Device Manager - Storage Navigator software and the *System Administrator Guide*.

Product version

This document revision applies to:

- Firmware 83-04-6*x* or later
- SVOS 7.3 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

- Added support for VSP Nx00.

Referenced documents

- *Command Control Interface User and Reference Guide*, MK-90RD7010
- *System Administrator Guide*, MK-94HM8016

Document conventions

This document uses the following typographic conventions:

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

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

Icon	Label	Description
	Note	Calls attention to important or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions 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, cache memory capacity) are calculated based on the following values:

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

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

Accessing product documentation

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

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

Comments

Please send us your comments on this document to doc.comments@hitachivantara.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 Vantara Corporation.

Thank you!

1

Introduction

This chapter provides an overview of the SNMP implementation for monitoring Hitachi Virtual Storage Platform G200, G400, G600, G800 and N400, N600, and N800, and Hitachi Virtual Storage Platform F400, F600, F800 storage systems, including the agent and management functions.

- SNMP Manager overview
- SNMP Agent configuration
- SNMP Agent overview
- Component status information from SNMP Manager

SNMP Manager overview

SNMP Manager is installed in the network management station. It collects and manages information from SNMP agents installed in the managed devices on the network.

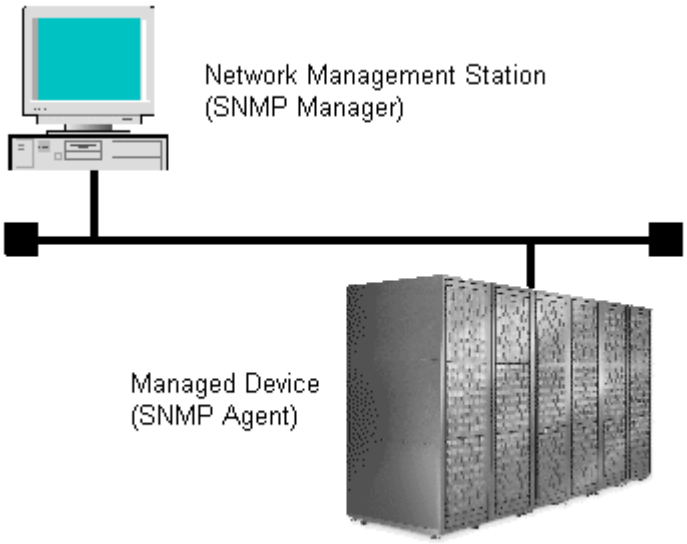
The SNMP Manager graphically displays information collected from two or more SNMP agents, accumulates the information in the database, and analyzes problems discovered while accumulating this information.

Note: SNMP versions v1, v2c, and v3 are supported.

How SNMP works

Simple Network Management Protocol (SNMP) is an industry-standard protocol for managing and monitoring network devices, including disk devices, routers, and hubs. SNMP uses Simple Gateway Management Protocol (SGMP) to manage TCP/IP gateways.

The following figure shows an example SNMP environment.



An SNMP manager monitors the devices, which are referred to as managed nodes. Typically, an SNMP Manager polls the SNMP agents on a periodic basis. The manager receives the reports from the agents and determines whether the devices are operating normally. If an abnormal event occurs, an SNMP Agent can report the condition without a request from the manager, by using a trap message.

When an SNMP manager polls an agent, the following dialogue takes place:

- An SNMP Manager sends a request packet to an SNMP Agent, which requests data regarding the status of the managed node.
- The SNMP Agent sends a response packet back to the SNMP Manager.
- SNMP uses the TCP/IP User Datagram Protocol (UDP). If the SNMP Agent does not respond within a specified time period, the SNMP Manager re-sends the request packet. That time period is set by the system administrator, taking into account the network traffic and operation policy.
- If an SNMP Agent again does not respond to the resent packet, the SNMP Manager assumes that an error has occurred. Depending on the times set for polling and response, this dialogue can take several seconds.

If an SNMP Agent detects an abnormal event, it sends a trap to the SNMP Manager. However, if a trap is dropped in transmission, the SNMP Manager does not know that it was sent. For this reason, you should use both polling and traps to determine whether an abnormal event has occurred.

Management Information Base overview

The standardized configuration and database of network management information is called a Management Information Base (MIB). A standard MIB is common to all SNMP interfaces. An extension MIB is defined by the particular managed device or protocol.

A MIB is a collection of standardized configuration and network management information that is contained in each device on the network. Each MIB contains a set of parameters called managed objects. Each managed object consists of a parameter name, one or more parameters, and a group of operations that can be executed with the object. The MIB defines the type of information that can be obtained from a managed device, and the device settings that can be controlled from a management system.

The MIB definition file, `VSPGx00MIB.txt`, is located in the `program\SNMP` folder of the software media kit.

For details about the MIB definition file of NAS modules, see the *Server and Cluster Administration Guide*.

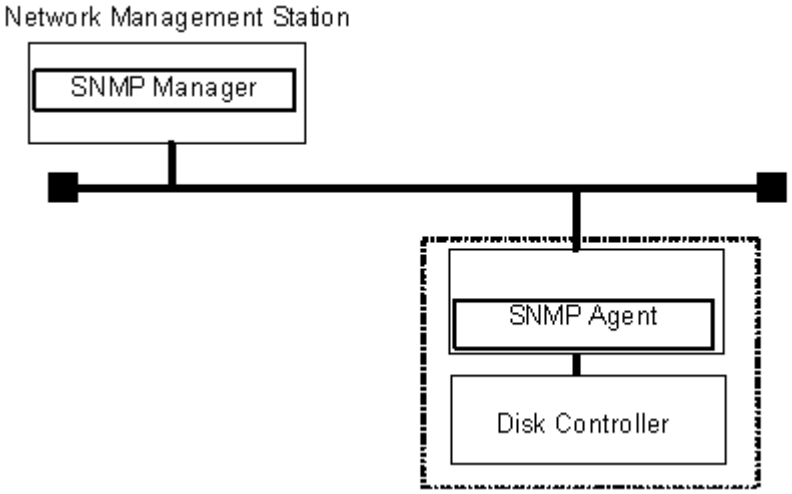
SNMP Agent configuration

The SNMP Agent runs on the storage system.

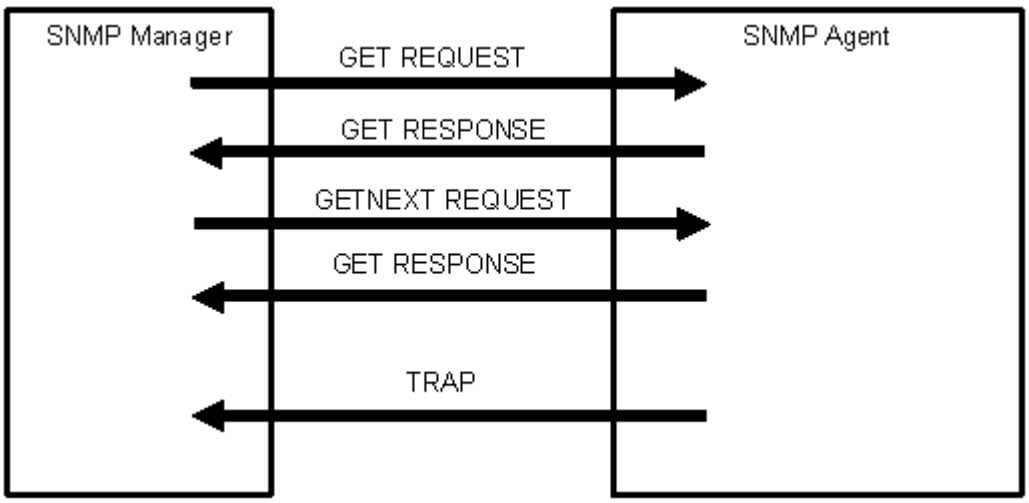
The SNMP Agent communicates with the SNMP manager through the LAN between the storage system and the SNMP manager.

Note: If you cannot input two or more MIB definition files for USP, USP V/VM, VSP, VSP G1000, VSP Gx00 models, or VSP Fx00 models because of the specifications of the SNMP manager software, use the MIB definition files for VSP Gx00 models or VSP Fx00 models. Error reports include storage system nicknames, which can be used to identify each storage system.

The following figure illustrates the SNMP environment.



The following figure shows an example of SNMP operations using an SNMP manager.



SNMP Agent overview

The SNMP Agent is mounted on a managed device (such as a hard disk) in the network. It collects error information, the usage condition, and other information about the device, and forwards the information to the SNMP Manager.

The SNMP Agent reports disk storage system failures to the manager using the SNMP trap function.

SNMP traps

An SNMP Agent reports storage system errors to the SNMP Manager using the SNMP trap function.

When an error occurs, the SNMP Agent issues an SNMP trap to the SNMP Manager that includes the product number, nickname, reference code, component where the failure occurred, failure date and time, and detailed information about the failure.

The following table lists the types of events that trigger an SNMP Agent trap.

Events	Description
Acute failure detected.	All operations in a storage system stopped.
Serious failure detected.	Operation in a component where a failure occurred stopped.
Moderate failure detected.	Partial failure.
Service failure detected.	Minor failure.

SNMP Agent operations

Operations that an SNMP Agent can perform fall into the categories GET REQUEST, GETNEXT REQUEST, GETBULK REQUEST, and TRAP.

The following table describes the types of SNMP Agent operations.

Operation	Description
GET REQUEST	Obtains a specific MIB object value. GET REQUEST is the request from an SNMP Manager, and GET RESPONSE is the agent's response to that request.
GETNEXT REQUEST	Continuously finds a MIB object. GETNEXT REQUEST is the request from an SNMP Manager, and GET RESPONSE is the agent's response to that request.
GETBULK REQUEST	Continuously finds specified MIB objects only. GETBULK REQUEST is the request from an SNMP Manager, and GET RESPONSE is the agent's response to that request.
TRAP	Reports an event (failure) to an SNMP Manager. TRAP occurs without a request from the SNMP Manager.

If you use SNMP version 3 in VSP G400, G600, G800 with NAS modules, specify VSPGx00 (fixed) as the context name when obtaining a MIB.

For details about obtaining MIBs of NAS modules and VSP G400, G600, G800 storage systems with NAS modules, see Example object identifier system on page 36

SNMP Agent reported errors

Several different types of errors can be reported when GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST operations are sent to an SNMP Agent.

The following table describes the errors that can be reported and suggests corrective action.

Error	Description	Corrective action
noError (0)	Normal	N/A
noSuchName (2)	• There are no MIB objects that are required. (Not supported.) • The GETNEXT REQUEST command that is specified for the following object identifier of the last supported MIB object is received.	Verify that the name of the requested object is correct.
	SET REQUEST is received.	SET REQUEST operation is not supported.
genErr (5)	Error occurred for other reasons.	Retry the operation.

Component status information from SNMP Manager

You can obtain the status information of certain storage system components from the SNMP Manager.

The following table lists the components for which the status can be obtained.

Area	Component name
Storage System	Processor(s)
	BUS
	Cache
	Power supplies
	Batteries
	Fans
	Others
DB	Power supplies
	Fans
	Environments
	Drives

The following table lists the status of storage system components, as well as the trap report functions.

Status	Description
Normal	Normal operation.
Acute failure detected	All operations in a storage system stopped.
Serious failure detected	Operation in a component where a failure occurred stopped.
Moderate failure detected	Partial failure.
Service failure detected	Minor failure.

2

Using SNMP

This chapter describes how to use to manage alert settings, SNMP trap notification, and SNMP request authentication, and how to test SNMP trap reports.

- Editing alert settings
- Managing SNMP trap notification
- Managing SNMP request authentication
- Testing SNMP trap reports

Editing alert settings

This topic describes how to set the Edit Alert Settings. If NAS modules are installed in your storage system, specify the alert notification settings in both the maintenance utility and NAS Manager. For details on how to configure NAS Manager, see the User Guide for your storage system.

Before you begin

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

For more information, see the **Set Up Alert Notifications** window in the *System Administrator Guide* .

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. For **Notification Alert**, select one of the following:
   - **All** (Sends alerts of all SIMs.)
   - **Host Report** (Sends alerts only of SIMs that report to hosts. Alert destinations are common to Syslog, SNMP, and Email.)
6. For **SNMP Agent**, select **Enable**.
7. In **System Group Information**, enter the Storage System Name, Contact, and Location. Changes made to information here are also reflected in the maintenance utility and shown in the **Storage System** window in Device Manager - Storage Navigator.
8. Confirm the settings, and then click **Apply**.

Managing SNMP trap notification

Adding trap notification for SNMP v1 and v2c

Follow this procedure to procedure to add IP addresses and communities to trap notification for SNMP versions v1 and v2c.

Before you begin

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

For more information, see the **Add Sending Trap Setting** window in the *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v1** or **v2c**.
7. Under **Registered Sending Trap Settings**, click **Add**.
8. In the **Add Sending Trap Setting** window, under **Community**, complete one of the following:
   - If you select an existing community, uncheck the **New** checkbox, and then select from the list of existing community names.
   - If you add a new community, check the **New** check box, and then enter a community name.

   You can enter up to 180 letters, numbers, and symbols, except the following:

   ```
   " \ ; : , * ? < > | / ^ & % '
   ```

   Do not use a space at the beginning or end of the name.
9. Under **Send Trap To**, complete the following:
   - If you enter a new IP address, check the **New** check box. Select **IPv4** or **IPv6** for the version of the IP address, and then enter an IP address.
   - If you use an existing IP address, uncheck the **New** check box. Select an existing IP address from the pull-down menu.
   - If you add more IP addresses, click **Add IP Address** to add input fields.
   - If you delete an IP address from **Send Trap to**, click the **-** button to delete the IP address.

   Note: Any IP address that has all values set to zero (0) cannot be specified for IPv4 and IPv6. The IPv6 address is specified by entering eight hexadecimal numbers that are separated by colons (:) using a maximum of 4 digits from zero (0) to FFFF inclusive. The default form of the IPv6 address can be specified.
10. Click **OK**.
    The IP address and community you entered are added to the **Registered Sending Trap Settings** table.
11. Confirm the settings, and then click **Apply**.

Adding trap notification for SNMP v3

This topic describes the procedure to add IP addresses and users to trap notification for SNMP v3.

Before you begin

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

For more information, see the **Add Sending Trap Setting** window in the *System Administrator Guide* .

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v3**.
7. Under **Registered Sending Trap Settings**, click **Add**.
8. In the **Add Sending Trap Setting** window, under **Send Trap To**, select **IPv4** or **IPv6** and enter an IP address.

   Note: Any IP address that has all values set to zero (0) cannot be specified for IPv4 and IPv6. The IPv6 address is specified by entering eight hexadecimal numbers that are separated by colons (:) using a maximum of 4 digits from zero (0) to FFFF inclusive. The default form of the IPv6 address can be specified.

9. Under **User Name**, enter a user name.

   Note: If you use a user name that has already been specified for **Sending Trap Setting** or **Request Authentication Setting**, specify the same settings for the following options that were specified for that name. Otherwise, SNMP traps might not be sent correctly.
   - Authentication
   - Authentication - Protocol
   - Authentication - Password
   - Encryption
   - Encryption - Protocol
   - Encryption - Key

You can enter up to 32 letters, numbers, and symbols, except the following:

```
" \ ; : , * ? < > | / ^ & %
```

Do not use a space at the beginning or end of the name.

10. Under **Authentication**, select whether to **Enable** or **Disable** authentication.
    If you select **Enable**, complete the following steps:
    a. For **Protocol**, select an authentication type.
    b. For **Password**, enter a password.
11. Under **Encryption**, select whether to **Enable** or **Disable** encryption.
    If you select **Enable**, complete the following steps:
    a. For **Protocol**, select an encryption type.
    b. For **Key**, enter a key.
    c. For **Re-enter Key**, enter the same key for confirmation.
12. Click **OK**.
    The IP address and user you entered are added to the **Registered Sending Trap Settings** table.
13. Confirm the settings, and then click **Apply**.

Changing trap notification for SNMP v1 and v2c

This topic describes the procedure to change the IP addresses and communities for trap notification for SNMP versions v1 and v2c.

Before you begin

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

For more information, see the **Change Sending Trap Setting** window in the *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v1** or **v2c**.
7. Under **Registered Sending Trap Settings**, select a trap setting that you want to change, and then click **Change**.
8. In the **Change Sending Trap Setting** window, under **Community**, enter a community name.

You can enter up to 180 letters, numbers, and symbols, except the following:

```
" \ ; : , * ? < > | / ^ & % '
```

Do not use a space at the beginning or end of the name.

9. Under **Send Trap To**, complete the following:
   - If you enter a new IP address, click **Add IP Address** to add input fields. Check the **New** check box, and then select **IPv4** or **IPv6** for the version of the IP address. Enter an IP address.
   - If you use an existing IP address, uncheck the **New** check box. Select an existing IP address from the pull-down menu.
   - If you delete an IP address from **Send Trap to**, click the **-** button to delete the IP address.
10. Click **OK**.
    The IP address and community that you entered are changed to the **Registered Sending Trap Settings** table.
11. Confirm the settings, and then click **Apply**.

Changing trap notification for SNMP v3

This topic describes the procedure to change the IP addresses and users for SNMP v3 trap notification.

Before you begin

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

For more information, see the **Change Sending Trap Setting** window in the *System Administrator Guide* .

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v3**.
7. Under **Registered Sending Trap Settings**, select a trap setting that you want to change, and then click **Change**.
8. In the **Change Sending Trap Setting** window, under **Send Trap To**, select **IPv4** or **IPv6** and enter an IP address.

Note: Any IP address that has all values set to zero (0) cannot be specified for IPv4 and IPv6. The IPv6 address is specified by entering eight hexadecimal numbers that are separated by colons

(:) using a maximum of 4 digits from zero (0) to FFFF inclusive. The default form of the IPv6 address can be specified.

9. Under **User Name**, enter a user name.

Note: If you use a user name that has already been specified for **Sending Trap Setting** or **Request Authentication Setting**, specify the same settings for the following options that were specified for that name. Otherwise, SNMP traps might not be sent correctly.

- Authentication
- Authentication - Protocol
- Authentication - Password
- Encryption
- Encryption - Protocol
- Encryption - Key

You can enter up to 32 letters, numbers, and symbols, except the following:

```
" \ ; : , * ? < > | / ^ & %
```

Do not use a space at the beginning or end of the name.

10. Under **Authentication**, select whether to **Enable** or **Disable** authentication.

    If you select **Enable**, complete the following steps:

    a. For **Protocol**, select an authentication type.
    b. If you change your password, check the **Change Password** checkbox and then enter a password.

11. Under **Encryption**, select whether to **Enable** or **Disable** encryption.

    If you select **Enable**, complete the following steps:

    a. For **Protocol**, select an encryption type.
    b. If you change a key, check the **Change Key** checkbox and then enter a key.
    c. For **Re-enter Key**, enter the same key for confirmation.

12. Click **OK**.
    The IP address and user you entered are changed to the **Registered Sending Trap Settings** table.
13. Confirm the settings, and then click **Apply**.

Deleting SNMP trap notification

This topic describes the procedure to delete IP addresses and communities or users from SNMP trap notification.

Before you begin

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

For more information, see the **Set Up Alert Notifications** window in the *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select your SNMP version.
7. Under **Registered Sending Trap Settings**, select one or more specific combinations of IP address and community or user, and then click **Delete**.
8. Confirm the settings, and then click **Apply**.

Managing SNMP request authentication

Adding request authentication for SNMP v1 and v2c

This topic describes how to add IP addresses and communities for request authentication for SNMP versions v1 and v2c.

Before you begin

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

For more information, see the **Add Request Authentication Setting** window in the *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v1** or **v2c**.
7. Under **Registered Request Authentication Settings**, click **Add**.
8. In the **Add Request Authentication Setting** window, under **Community**, complete one of the following:

- If you add a new community, check the **New** check box, and then enter a community name.
- If you select an existing community, uncheck the **New** check box, and then select from the list of existing community names.

You can enter up to 180 letters, numbers, and symbols, except the following:

```
" \ ; : , * ? < > | / ^ & % '
```

Do not use a space at the beginning or end of the name.

9. Under **Request Permitted**, complete the following:
   - If you want to allow REQUEST operations from all managers, select the **All** check box.
   - If you want to allow REQUEST operations only from specified managers, select **IPv4** or **IPv6** and enter an IP address, or select from the list of existing IP addresses.
   - If you enter a new IP address, check the **New** check box. Select **IPv4** or **IPv6** for the version of the IP address, and then enter an IP address.
   - If you use an existing IP address, uncheck the **New** check box. Select an existing IP address from the pull-down menu.
   - If you add more IP addresses, click **Add IP Address** to add input fields.
   - If you delete an IP address from **Request Permitted**, click the **-** button to delete the IP address.

Note: Any IP address that has all values set to zero (0) cannot be specified for IPv4 and IPv6. The IPv6 address is specified by entering eight hexadecimal numbers that are separated by colons (:) using a maximum of 4 digits from zero (0) to FFFF inclusive. The default form of the IPv6 address can be specified.

10. Click **OK**
    The community and IP address that you entered are added to the **Registered Request Authentication Settings** table.
11. Confirm the settings, and then click **Apply**.

Adding request authentication for SNMP v3

This topic describes how to add IP addresses and users for SNMP v3 request authentication.

Before you begin

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

For more information, see the **Add Request Authentication Setting** window in the *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v3**.
7. Under **Registered Request Authentication Settings**, click **Add**.
8. In the **Add Request Authentication Setting** window, under **User Name**, enter a user name.

   Note: If you use a user name that has already been specified for **Sending Trap Setting** or **Request Authentication Setting**, specify the same settings for the following options that were specified for that name. Otherwise, SNMP traps might not be sent correctly.
   - Authentication
   - Authentication - Protocol
   - Authentication - Password
   - Encryption
   - Encryption - Protocol
   - Encryption - Key

   You can enter up to 32 letters, numbers, and symbols, except the following:

   ```
   " \ ; : , * ? < > | / ^ & %
   ```

   Do not use a space at the beginning or end of the name.
9. Under **Authentication**, select whether to **Enable** or **Disable** authentication.

   If you select **Enable**, complete the following steps:

   a. For **Protocol**, select an authentication type.
   b. For **Password**, enter a password.
10. Under **Encryption**, select whether to **Enable** or **Disable** encryption.

    If you select **Enable**, complete the following steps:

    a. For **Protocol**, select an encryption type.
    b. For **Key**, enter a key.
    c. For **Re-enter Key**, enter the same key for confirmation.
11. Click **OK**.

The user you entered is added to the **Registered Request Authentication Settings** table.

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

Changing request authentication for SNMP v1 and v2c

This topic describes how to change IP addresses and communities for request authentication for SNMP versions v1 and v2c.

Before you begin

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

For more information, see the **Change Request Authentication Setting** window in the *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v1** or **v2c**.
7. Under **Registered Request Authentication Settings**, select an authentication setting that you want to change and then click **Change**.
8. In the **Change Request Authentication Setting** window, under **Community**, enter a community name.

   You can enter up to 180 letters, numbers, and symbols, except the following:

   ```
   " \ ; : , * ? < > | / ^ & % '
   ```

   Do not use a space at the beginning or end of the name.
9. Under **Request Permitted**, complete the following:
   - If you want to allow REQUEST operations from all managers, select the **All** check box.
   - If you want to allow REQUEST operations only from specified managers, select **IPv4** or **IPv6** and enter an IP address, or select from the list of existing IP addresses.
   - If you enter a new IP address, click **Add IP Address** to add input fields, and then check the **New** check box. Select **IPv4** or **IPv6** for the version of the IP address, and then enter an IP address.
   - If you use an existing IP address, uncheck the **New** check box. Select an existing IP address from the pull-down menu.

- If you delete an IP address from **Request Permitted**, click the **-** button to delete the IP address.

Note: Any IP address that has all values set to zero (0) cannot be specified for IPv4 and IPv6. The IPv6 address is specified by entering eight hexadecimal numbers that are separated by colons (:) using a maximum of 4 digits from zero (0) to FFFF inclusive. The default form of the IPv6 address can be specified.

10. Click **OK**.
    The community and IP address that you entered are changed to the **Registered Request Authentication Settings** table.
11. Confirm the settings, and then click **Apply**.

Changing request authentication for SNMP v3

This topic describes how to change IP addresses and users for SNMP v3 request authentication.

Before you begin

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

For more information, see the **Change Request Authentication Setting** window in the *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.
5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select **v3**.
7. Under **Registered Request Authentication Settings**, select an authentication setting that you want to change, and then click **Change**.
8. In the **Change Request Authentication Setting** window, under **User Name**, enter a user name.

Note: If you use a user name that has already been specified for **Sending Trap Setting** or **Request Authentication Setting**, specify the same settings for the following options that were specified for that name. Otherwise, SNMP traps might not be sent correctly.

- Authentication
- Authentication - Protocol

- Authentication - Password
- Encryption
- Encryption - Protocol
- Encryption - Key

You can enter up to 32 letters, numbers, and symbols, except the following:

```
" \ ; : , * ? < > | / ^ & %
```

Do not use a space at the beginning or end of the name.

9. Under **Authentication**, select whether to **Enable** or **Disable** authentication.
   If you select **Enable**, complete the following steps:
   a. For **Protocol**, select an authentication type.
   b. If you change your password, check the **Change Password** checkbox, and then enter a password.
10. Under **Encryption**, select whether to **Enable** or **Disable** encryption.
    If you select **Enable**, complete the following steps:
    a. For **Protocol**, select an encryption type.
    b. If you change a key, check the **Change Key** checkbox, and then enter a key.
    c. For **Re-enter Key**, enter the same key for confirmation.
11. Click **OK**.
    The user you entered is changed to the **Registered Request Authentication Settings** table.
12. Confirm the settings, and then click **Apply**.

Deleting SNMP request authentication

This topic describes how to delete IP addresses and communities or users from request authentication.

Before you begin

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

For more information, see the **Set Up Alert Notifications** window in the *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. In the **Alert Notifications** window, click **Set Up**.
4. In the **Set Up Alert Notifications** window, select the **SNMP** tab.

5. Under **SNMP Agent**, click **Enable**.
6. Under **SNMP Version**, select your SNMP version.
7. Under **Registered Request Authentication Settings**, select one or more specific combinations of IP address and community or user, and then click **Delete**.
8. Confirm the settings, and then click **Apply**.

Testing SNMP trap reports

This topic describes the procedure to test SNMP trap reporting by sending a test trap.

Before you begin

An IP address and community have been added in the **Set Up Alert Notifications** window.

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

For more information, see the *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Maintenance Utility** menu, select **Alert Notifications**.
3. Select the **SNMP** tab.
4. Click **Send Test SNMP Trap**.
   Reports the test SNMP trap to the community or user registered in the storage system. Reports the events registered in the storage system instead of the events that are set on the **SNMP** tab. If you want to test the events set on the **SNMP** tab, click **Finish** and apply to the storage system, and then report the test SNMP trap.
5. Verify whether the SNMP trap report (reference code 7fffff) is received by the SNMP manager that has the IP address specified for **Sending Trap Setting** in the **Alert Notifications** window.

3

SNMP supported MIBs

This chapter describes the standard and extension MIB specifications, and trap configuration.

- SNMP Agent failure report trap contents
- SNMP Agent extension trap types
- Standard MIB specifications
- Extension MIB specifications

SNMP Agent failure report trap contents

A standard extension trap protocol data unit (PDU) includes the product number of the device that experienced the failure, the device nickname, and a failure reference code. A failure report trap contains additional information about the failure, such as the area, date, and time of the failure.

If you obtain the information with the **GetRequest** command, access the MIB by using the product number of the device as an index.

The following table shows the failure report trap.

Name	Object identifier	Type	Description
eventTrapSerialNumber	.1.3.6.1.4.1.116.5.11.4.2.1	INTEGER	The product number of the device that experienced the failure.
eventTrapNickname	.1.3.6.1.4.1.116.5.11.4.2.2	DisplayString	The device nickname "HM800" is displayed.
eventTrapREFCODE	.1.3.6.1.4.1.116.5.11.4.2.3	DisplayString	The failure reference code.
eventTrapPartsID	.1.3.6.1.4.1.116.5.11.4.2.4	OBJECT IDENTIFIER	The area where the failure occurred.*
eventTrapDate	.1.3.6.1.4.1.116.5.11.4.2.5	DisplayString	Failure occurrence date.
eventTrapTime	.1.3.6.1.4.1.116.5.11.4.2.6	DisplayString	Failure occurrence time.
eventTrapDescription	.1.3.6.1.4.1.116.5.11.4.2.7	DisplayString	Detailed information of a failure.
*The object identifier for a failure in a storage system processor would be .1.3.6.1.4.1.116.5.11.4.1.1.6.1.2.			

The SNMP trap information that is output depends on whether the VSP G400, G600, G800 storage system includes NAS modules. For details about SNMP traps of NAS modules, see the *Server and Cluster Administration Guide*.

SNMP Agent extension trap types

SNMP Agent extension trap types are set according to the severity. The character strings following "RaidEventUser" indicate their severity.

The following table describes the SNMP Agent extension trap types.

Specific Trap Code	Trap	Description
1	RaidEventUserAcute	All operations in a storage system stopped.
2	RaidEventUserSerious	Operation in a component where a failure occurred stopped.
3	RaidEventUserModerate	Partial failure.
4	RaidEventUserService	Minor failure.

For details about types of traps for NAS modules, see the *Server and Cluster Administration Guide*q.

Standard MIB specifications

MIBs supported by SNMP Agent

SNMP Agent supports a limited number of MIBs. If you send a GET request for an object (MIB) that is not supported, you will receive `NoSuchName` as a GET RESPONSE.

The following table lists MIBs and indicates whether they are supported.

MIB		Without NAS modules	With NAS modules
Standard MIB: MIB-II	system group	Supported[1]	Supported[1]
	interface group	Not supported	Supported
	at group		
	ip group		
	icmp group		
	tcp group		
	udp group		
	egp group		
	oim group		
	transmission group		
	snmp group		
Extension MIB	hitachi(116)	Supported[1]	Supported[1]
	blueArc(11096)	Not supported	Supported[2]

Notes:
1. The maintenance utility responds.
2. The NAS unified firmware responds.

SNMP Agent MIB access mode

The access mode for MIB in all communities is read only. If you send a GET request for a SET REQUEST operation, you will receive `NoSuchName` as a RESPONSE.

Example object identifier system

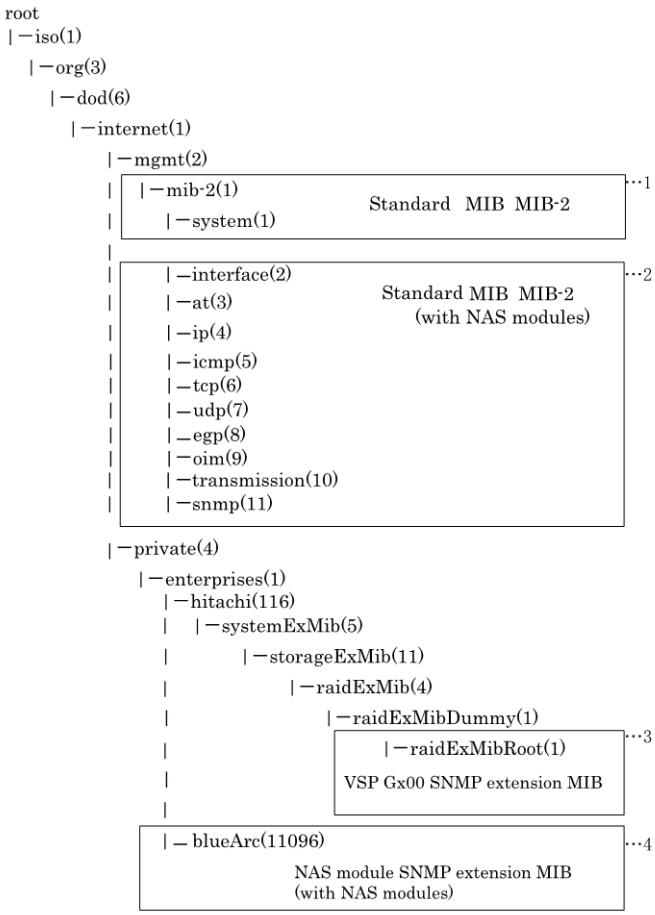
The following figure shows an example object system supported by SNMP Agent.

When NAS modules are not installed, obtain all MIB objects as follows:

1. Specify object identifier 1.3.6.1.2.1 to execute `snmpwalk`.
   The information in 1 and 3 in the figure below is obtained.

When NAS modules are installed, obtain all MIB objects as follows:

1. Specify object identifier 1.3.6.1.2.1 to obtain the information shown in 1. If NAS modules are installed, you will also need the information shown in 2.
2. Specify object identifier 1.3.6.1.4.1.116 to obtain the information shown in 3.
3. If NAS modules are installed, specify object identifier 1.3.6.1.4.1.11096 to obtain the information shown in 4.



Related references

- Extension MIB configuration on page 38

MIB mounting specifications supported by SNMP Agent

SNMP Agent supports two MIB mounting specifications.

The supported MIB mounting specifications are as follows:

- mgmt OBJECT IDENTIFIER ::= {iso(1) org(3) dod(6) internet(1) 2 }
- mib-2 OBJECT IDENTIFIER ::= {mgmt 1}

An SNMP Agent mounts only system groups in mib-2, as shown in the following table.

Name	Description	Mounted value
sysObjectID {system 2}	This is the product identification number.	Fixed value. See Example object identifier system on page 36. 1.3.6.1.4.1.116.3.11.4.1.1
sysUpTime {system 3}	An accumulated time from an SNMP agent.	Unit: 100 ms

Name	Description	Mounted value
sysContact {system 4}	A manager who manages an agent or a contact address.	Maximum 180 characters in an ASCII characters string. Input by a user from an SNMP setting window.*
sysName {system 5}	The name of an agent manager	Maximum 180 characters in an ASCII characters string. Input by a user from an SNMP setting window.*
sysLocation {system 6}	An agent setup location.	Maximum 180 characters in an ASCII characters string. Input by a user from an SNMP setting window.*
sysService {system 7}	Value indicating a service.	Fixed value 76 (decimal)
*The following symbols cannot be used: \ , / : ; * ? " < > | & % ^		

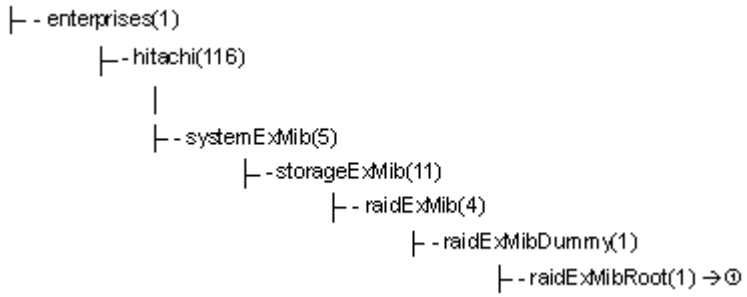
Extension MIB specifications

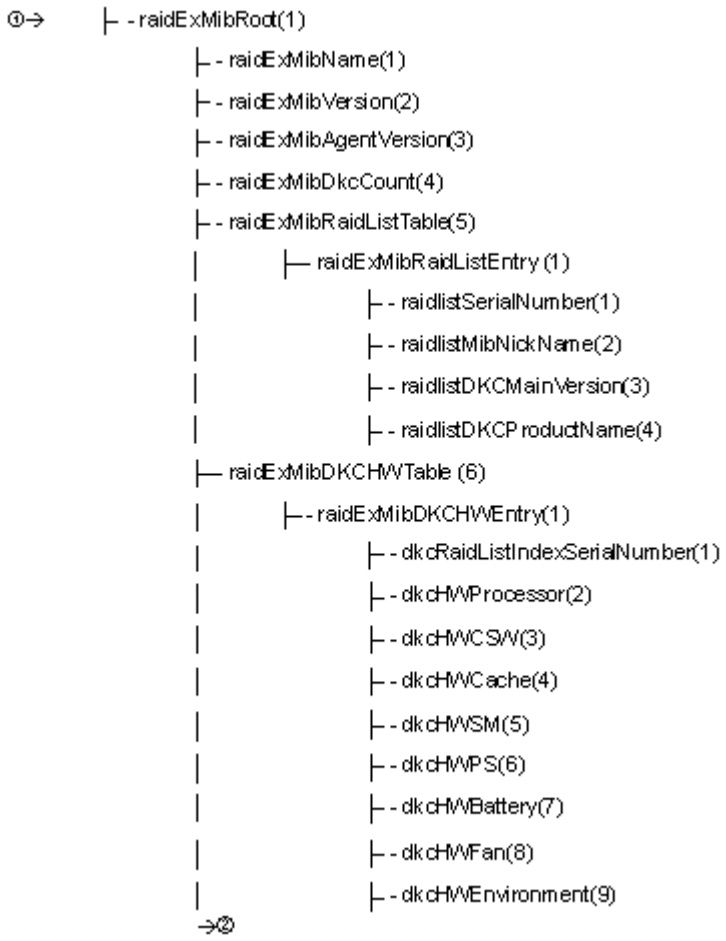
Extension MIB configuration

The following shows the extension MIB object system for the storage system. For details about extension MIB of NAS modules, see the *Server and Cluster Administration Guide*.

```
raidExMibRoot(1)
  ├--raidExMibName(1)           Maintenance utility product name
  ├--raidExMibVersion(2)        Maintenance utility firmware version
  ├--raidExMibAgentVersion(3)   Extension MIB internal version
  ├--raidExMibDkcCount(4)       Number of DKC
  ├--raidExMibRaidListTable(5)  List of DKC
  ├--raidExMibDKCHWTable(6)     Disk control device information
  ├--raidExMibDKUHWTable(7)     Disk device information
  ├--raidExMibTrapListTable(8)  Error information list
```

The following figures show an example extension MIB configuration.




①→
raidExMibRoot(1)
raidExMibName(1)
raidExMibVersion(2)
raidExMibAgentVersion(3)
raidExMibDkcCount(4)
raidExMibRaidListTable(5)
raidExMibRaidListEntry (1)
raidlistSerialNumber(1)
raidlistMibNickName(2)
raidlistDKCMainVersion(3)
raidlistDKCProductName(4)
raidExMibDKCHWTable (6)
raidExMibDKCHWEntry(1)
dkcRaidListIndexSerialNumber(1)
dkcHWProcessor(2)
dkcHWCSW(3)
dkcHWCache(4)
dkcHWSM(5)
dkcHWPS(6)
dkcHWBattery(7)
dkcHWFan(8)
dkcHWEnvironment(9)
→②
②→
raidExMibDKUHWTable (7)
raidExMibDKUHWEntry (1)
dkuRaidListIndexSerialNumber(1)
dkuHWPS(2)
dkuHWFan(3)
dkuHWEnvironment(4)
dkuHWDrive(5)
raidExMibTrapListTable (8)
raidExMibTrapListEntry (1)
eventListIndexSerialNumber(1)
eventListNickName(2)
eventListIndexRecorderNo(3)
eventListREFCODE(4)
eventListDate(5)
eventListTime(6)
eventListDescription(7)

raidExMibName

`raidExMibName` indicates the product name.

```
raidExMibName            OBJECT-TYPE
SYNTAX                   DisplayString
ACCESS                   read-only
STATUS                   mandatory
DESCRIPTION              "product name."
::={ raidExMibRoot 1 }
```

raidExMibVersion

`raidExMibVersion` indicates the maintenance utility firmware version.

```
raidExMibVersion         OBJECT-TYPE
SYNTAX                   DisplayString
ACCESS                   read-only
STATUS                   mandatory
DESCRIPTION              "GUM firmware version."
::= { raidExMibRoot 2 }
```

raidExMibAgentVersion

`raidExMibAgentVersion` indicates the internal version of the extension MIB.

```
raidExMibAgentVersion OBJECT-TYPE
SYNTAX              DisplayString
ACCESS              read-only
STATUS              mandatory
DESCRIPTION         "Extension agent version."
::= { raidExMibRoot 3 }
```

raidExMibDkcCount

`raidExMibDkcCount` suggests the number of a storage system.

```
raidExMibDkcCount        OBJECT TYPE
SYNTAX                   INTEGER
ACCESS                   read-only
STATUS                   mandatory
DESCRIPTION              "Number of DKC"
::={ raidExMibRoot 4}
```

raidExMibRaidListTable

`raidExMibRaidListTable` indicates the storage system.

```
raidExMibRaidListTable   OBJECT TYPE
SYNTAX                   SEQUENCE OF raidExMibRaidListEntry
ACCESS                   not-accessible
STATUS                   mandatory
DESCRIPTION              "List of DKC."
::={ raidExMibRoot 5}
```

```
raidExMibRaidListEntry   OBJECT TYPE
SYNTAX                   RaidExMibRaidListEntry
ACCESS                   not-accessible
STATUS                   mandatory
DESCRIPTION              "Entry of DKC list."
INDEX                    { raidlistSerialNumber }
::={ raidExMibRaidListTable 1}
```

The following table lists the information displayed for each storage system

Name	Type	Description	Mounted value	Attribute
raidlistSerialNumber ::=RaidExMibRaidListEntry(1)	INTEGER	Storage system product number (index).	400,001 - 499,999	read-only
raidlistMibNickName ::=RaidExMibRaidListEntry(2)	DisplayString	Storage system nickname.	(Max. 18 characters)	read-only
raidlistDKCMainVersion ::=RaidExMibRaidListEntry(3)	DisplayString	Software version.	Max. 14 characters	read-only
raidlistDKCProductName ::=RaidExMibRaidListEntry(4)	DisplayString	Storage system product type.	7 characters*	read-only
* RAID800 will be used as storage system product type raidlistDKCProductName.				

raidExMibDKCHWTable

`raidExMibDKCHWTable` indicates the status of the storage system components.

```
raidExMibDKCHWTable  OBJECT TYPE
SYNTAX               SEQUENCE OF RaidExMibDKCHWEntry
ACCESS               not-accessible
STATUS               mandatory
DESCRIPTION          "Error information of the DKC."
::={ raidExMibRoot 6}

raidExMibDKCHWEntry  OBJECT TYPE
SYNTAX               RaidExMibDKCHWEntry
ACCESS               not-accessible
STATUS               mandatory
DESCRIPTION          "Entry of DKC information."
INDEX                {dkcRaidListIndexSerialNumber}
::={ raidExMibDKCHWTable 1}
```

The following table lists the information displayed for each storage system component.

Name	Type	Description	MIB value	Attribute
dkcRaidListIndexSerialNumber ::=raidExMibDKCHWEntry(1)	INTEGER	Storage system product number (index).	400,001 - 499,999	read-only

Name	Type	Description	MIB value	Attribute
dkcHWProcessor ::=raidExMibDKCHWEntry(2)	INTEGER	Status of processor.	See Note	read-only
dkcHWCSW ::=raidExMibDKCHWEntry(3)	INTEGER	Status of internal star.	See Note	read-only
dkcHWCache ::=raidExMibDKCHWEntry(4)	INTEGER	Status of cache.	See Note	read-only
dkcHWSM ::=raidExMibDKCHWEntry(5)	INTEGER	This value is unused.	See Note	read-only
dkcHWPS ::=raidExMibDKCHWEntry(6)	INTEGER	Status of power supply.	See Note	read-only
dkcHWBattery ::=raidExMibDKCHWEntry(7)	INTEGER	Status of battery.	See Note	read-only
dkcHWFan ::=raidExMibDKCHWEntry(8)	INTEGER	Status of fan.	See Note	read-only
dkcHWEnvironment ::=raidExMibDKCHWEntry(9)	INTEGER	Information of an operational environment.	See Note	read-only
Note: The status of each component is a single digit which shows the following: 1: Normal. 2: Acute failure detected. 3: Serious failure detected. 4: Moderate failure detected. 5: Service failure detected.				

raidExMibDKUHWTable

`raidExMibDKUHWTable` indicates the status of the storage system components.

```
raidExMibDKUHWTable  OBJECT TYPE
SYNTAX               SEQUENCE OF RaidExMibDKUHWEntry
ACCESS               not-accessible
STATUS               mandatory
DESCRIPTION          "Error information of the DKU."
::={ raidExMibRoot 7}

raidExMibDKUHWEntry  OBJECT TYPE
SYNTAX               RaidExMibDKUHWEntry
ACCESS               not-accessible
STATUS               mandatory
DESCRIPTION          "Entry of DKU information."
INDEX                { dkuRaidListIndexSerialNumber }
::={ raidExMibDKUHWTable 1}
```

The following table lists the information displayed for each disk device component.

Name	Type	Description	MIB value	Attribute
dkuRaidListIndexSerialNumber ::=raidExMibDKUHWEntry(1)	INTEGER	Storage system product number (index).	400,001 - 499,999	read-only
dkuHWPS ::=raidExMibDKUHWEntry(2)	INTEGER	Status of power supply.	See Note	read-only
dkuHWFan ::=raidExMibDKUHWEntry(3)	INTEGER	Status of fan.	See Note	read-only
dkuHWEnvironment ::=raidExMibDKUHWEntry(4)	INTEGER	Status of environment monitor.	See Note	read-only
dkuHWDrive ::=raidExMibDKUHWEntry(5)	INTEGER	Status of drive.	See Note	read-only
Note: The status of each component is a single digit which shows the following: 1: Normal. 2: Acute failure detected. 3: Serious failure detected. 4: Moderate failure detected. 5: Service failure detected.				

raidExMibTrapListTable

raidExMibTrapListTable shows the history of the failure traps.

```
raidExMibTrapListTable  OBJECT TYPE
SYNTAX                  SEQUENCE OF RaidExMibTrapListEntry
ACCESS                  not-accessible
STATUS                  mandatory
DESCRIPTION             "Trap list table."
::={ raidExMibRoot 8 }

raidExMibTrapListEntry  OBJECT TYPE
SYNTAX                  RaidExMibTrapListEntry
ACCESS                  non-accessible
STATUS                  mandatory
DESCRIPTION             "Trap list table index."
INDEX                   { eventListIndexSerialNumber ,
                        eventListIndexRecordNo }
::={ raidExMibTrapListTable 1 }
```

The following table lists the information displayed for each failure.

Name	Type	Description	MIB value	Attribute
eventListIndexSerialNumber ::=raidExMibTrapListEntry(1)	INTEGER	Storage system product number (index).	400,001 - 499,999	read-only
eventListNickname ::=raidExMibTrapListEntry(2)	DisplayString	Storage system nickname.	18 characters maximum	read-only
eventListIndexRecordNo ::=raidExMibTrapListEntry(3)	Counter	Number of records.	1-256	read-only
eventListREFCODE ::=raidExMibTrapListEntry(4)	DisplayString	Reference code (index).	6 characters	read-only
eventListData ::=raidExMibTrapListEntry(5)	DisplayString	Date when the failure occurred.	*yyyy/mm/dd* (10 characters)	read-only
eventListTime ::=raidExMibTrapListEntry(6)	DisplayString	Time when the failure occurred.	*hh:mm:ss* (8 characters)	read-only
eventListDescription ::=raidExMibTrapListEntry(7)	DisplayString	Detailed information about the failure.	256 characters maximum	read-only

4

SNMP failure trap reference

This chapter describes the failure trap reference codes, including sections and alert levels.

- SNMP failure trap reference codes
- Obtaining drive box and drive numbers

SNMP failure trap reference codes

The following table lists and describes the SNMP failure trap reference codes.

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
18	00	00	Audit Log lost	DKC environment	MODERATE	Yes
1C	00	00	Detected a specific error code SSB	DKC environment	SERVICE	Yes
21	20	*xx*	Channel port blocking	DKC environment	MODERATE	Yes
21	30	*xx*	CHB blocking	DKC environment	MODERATE	Yes
21	40	*xx*	DKB blocking	DKC environment	MODERATE	Yes
21	50	*xx*	Unified NAS module blocking	DKC environment	MODERATE	No
21	51	*xy*	NAS SFP type error	DKC environment	MODERATE	No
21	52	*xy*	NAS SFP module error	DKC environment	MODERATE	No
21	53	*xx*	PECB blocking	DKC environment	MODERATE	Yes
21	54	*xx*	SWPK blocking	DKC environment	MODERATE	Yes
21	57	*xx*	PECB warning	DKC environment	MODERATE	Yes
21	80	*xx*	RIO path closed	DKC environment	MODERATE	Yes
21	90	*xx*	AL_PA value conflict	DKC environment	SERVICE	Yes
21	93	*xx*	Link failure1	DKC environment	SERIOUS	Yes
21	94	*xx*	Link failure2	DKC environment	SERIOUS	Yes
21	a8	*xx*	SFP wrong type	DKC environment	MODERATE	Yes
21	aa	*xx*	SFP TxFault	DKC environment	MODERATE	Yes
21	d0	*xx*	External storage system connection path blocking	DKC environment	MODERATE	Yes
21	d1	*xx*	External storage system connection path restore	DKC environment	SERVICE	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
21	d2	*xx*	External subsystem path response timeout	DKC environment	SERVICE	Yes
30	70	*xx*	CHK1A threshold over	Processor	SERVICE	Yes
30	71	*xx*	CHK1B threshold over	Processor	SERVICE	Yes
30	72	*xx*	CHK3 threshold over	Processor	SERVICE	Yes
30	73	*xx*	Processor blocking	Processor	MODERATE	Yes
30	75	*xx*	CFM Failure	Cache	MODERATE	Yes
30	76	*xx*	Incorrect SUM value of FM	Processor	SERVICE	Yes
30	77	*xx*	Processor memory temporary error	Processor	SERVICE	Yes
30	78	*xx*	BFM error	Processor	SERIOUS	Yes
30	7b	0*x*	Unified Hypervisor blocking	DKC environment	MODERATE	Yes
30	80	*xx*	WCHK1 dump	Processor	MODERATE	Yes
38	8f	00	PS OFF impossible	PS(DKC)	MODERATE	Yes
38	9f	00	PS OFF impossible (Device reserved)	PS(DKC)	MODERATE	Yes
39	90	*xx*	Undefined Package is mounted	Processor	MODERATE	Yes
39	91	*xx*	V-R or serial number is inconsistent	Processor	MODERATE	Yes
39	93	*xx*	Replace failed	Processor	MODERATE	Yes
39	9d	*xx*	Injustice dc voltage control	DKC environment	MODERATE	Yes
39	9e	*xx*	Injustice CEMODE	DKC environment	MODERATE	Yes
39	9f	*xx*	Injustice CEDT	DKC environment	MODERATE	Yes
39	a0	00	The upper temperature limit was exceeded	DKC environment	SERVICE	Yes
39	b0	*xx*	MP patrol check error	DKC environment	SERVICE	Yes
3a	0*x*	*xx*	LDEV Blockade (Effect of microcode error)	Drive	MODERATE	Yes
3c	95	00	CHB/DKB Type disagreement	DKC environment	MODERATE	Yes
3c	96	00	No CHB mounted	Processor	MODERATE	Yes
41	00	00	Format complete (Normal end)	Drive	SERVICE	Yes
41	00	01	Format complete (Abnormal end)	Drive	SERVICE	Yes
41	00	02	Format complete (Partial abnormal end)	Drive	SERVICE	Yes
41	01	00	Quick Format finish	Drive	SERVICE	Yes
43	4*x*	*xx*	Drive media error[2]	Drive	SERVICE	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
43	b*x*	*xx*	Drive blockade (media)(with redundancy)[2]	Drive	SERIOUS	Yes
43	c*x*	*xx*	Drive blockade (media)(without redundancy)[2]	Drive	SERIOUS	Yes
45	1*x*	*xx*	Correction copy start[2]	Drive	SERVICE	Yes
45	2*x*	*xx*	Correction copy normal end[2]	Drive	SERVICE	Yes
45	3*x*	*xx*	Correction copy abnormal end[2]	Drive	SERIOUS	Yes
45	4*x*	*xx*	Correction copy discontinued[2]	Drive	SERVICE	Yes
45	5*x*	*xx*	Correction copy warning end[2]	Drive	SERVICE	Yes
46	1*x*	*xx*	Dynamic sparing start(Drive copy)[2]	Drive	SERVICE	Yes
46	2*x*	*xx*	Dynamic sparing normal end(Drive copy)[2]	Drive	SERVICE	Yes
46	3*x*	*xx*	Dynamic sparing abnormal end (Drive copy)[2]	Drive	MODERATE	Yes
46	4*x*	*xx*	Dynamic sparing discontinued (Drive copy)[2]	Drive	SERVICE	Yes
46	5*x*	*xx*	Dynamic Sparing(Drive Copy) warning end[2]	Drive	SERVICE	Yes
46	8*x*	*xx*	Collection Copy/Copyback disabled(drive replace)	Drive	MODERATE	Yes
47	d*x*	*xx*	Shadow Image Copy abnormal end	DKC environment	MODERATE	Yes
47	e7	00	Forcible suspend by SM volatile	DKC environment	MODERATE	Yes
47	ec	e7	Forcible suspend by SM volatile	DKC environment	MODERATE	Yes
47	f*x*	*xx*	Volume Migration abnormal end	DKC environment	MODERATE	Yes
49	10	00	Cache overload condition	Cache	SERVICE	Yes
4a	80	*xx*	Expander Micro Exchange failed	DKC environment	MODERATE	Yes
4b	3*x*	*xx*	Thin Image Option abnormal end	DKC environment	MODERATE	Yes
4c	1*x*	*xx*	PDEV Erase Start	Drive	SERVICE	Yes
4c	2*x*	*xx*	PDEV Erase Normal End	Drive	SERVICE	Yes
4c	3*x*	*xx*	PDEV Erase Abnormal End	Drive	SERVICE	Yes
4C	4*x*	*xx*	Flash module drive initialization failed	Drive	MODERATE	Yes
4d	1*x*	*xx*	Differential area blocking	Drive	SERIOUS	Yes
50	1*x*	*xx*	Drive temporary error	Drive	SERVICE	Yes
50	2*x*	*xx*	Drive media error	Drive	SERVICE	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
50	5*x*	*xx*	Flash module drive internal battery error (ORM)[2]	Drive	SERVICE	Yes
50	8*x*	*xx*	Flash module drive internal battery error[2]	Drive	MODERATE	Yes
50	b*x*	*xx*	Flash drive End of life[2]	Drive	SERVICE	Yes
50	c*x*	*xx*	Flash module drive End of life[2]	Drive	SERVICE	Yes
50	d*x*	*xx*	Flash module drive battery warning[2]	Drive	SERVICE	Yes
50	e*x*	*xx*	Flash module drive battery capacity shortage[2]	Drive	MODERATE	Yes
50	f0	00	Flash module drive micro-program version warning	Drive	MODERATE	Yes
60	1*x*	*xx*	Pool utilization threshold excess	DKC environment	MODERATE	Yes
60	2*x*	*xx*	Pool blocking	DKC environment	MODERATE	Yes
60	2f	fe	Pools blocking by SM volatile	DKC environment	MODERATE	Yes
60	30	00	SM Space Warning	DKC environment	MODERATE	Yes
60	4*x*	*xx*	Exceeded Threshold of actual pool use rate	DKC environment	MODERATE	Yes
60	5*x*	*xx*	Actual pool use rate reaches upper limit	DKC environment	MODERATE	Yes
60	6*x*	*xx*	Exceeded Fixed outage Threshold of pool use rate	DKC environment	MODERATE	Yes
61	00	01	Backup/restore SM Information failed (Backup)	SM	MODERATE	Yes
61	00	02	Backup/restore SM Information failed (Restore)	SM	MODERATE	Yes
62	0*x*	*xx*	The DP POOL Warning Threshold was exceeded	DKC environment	MODERATE	Yes
62	2*x*	*xx*	The DP POOL FULL	DKC environment	MODERATE	Yes
62	3*x*	*xx*	The DP POOL error is detected	DKC environment	MODERATE	Yes
62	3f	fe	DP Pools blocking by Shared Memory volatile	DKC environment	MODERATE	Yes
62	40	00	SM Full	DKC environment	MODERATE	Yes
62	50	00	DP pool threshold continues to be exceeded	DKC environment	MODERATE	Yes
62	6*x*	*xx*	The DP POOL Depletion threshold was exceeded	DKC environment	MODERATE	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
62	7*x*	*xx*	The DP POOL LDEV blockade	DKC environment	MODERATE	Yes
62	80	00	DP Protect attribute setting of DRU	DKC environment	SERVICE	Yes
62	9*x*	*xx*	Exceeded Warning Threshold of DP pool use rate	DKC environment	MODERATE	Yes
62	a*x*	*xx*	Actual DP pool use rate reaches upper limit	DKC environment	MODERATE	Yes
62	b0	00	Threshold of DP pool use rate remains exceeded	DKC environment	MODERATE	Yes
62	c*x*	*xx*	Exceeded Depletion Threshold of DP pool use rate	DKC environment	MODERATE	Yes
62	d*x*	*xx*	Exceeded Fixed outage Threshold of DP pool use rate	DKC environment	MODERATE	Yes
62	e*x*	*xx*	Exceeded DP pool depletion threshold for TI pairs	DKC environment	MODERATE	Yes
64	1*x*	*xx*	Tier relocation is not completed	DKC environment	SERVICE	Yes
66	01	00	No free encryption key	DKC environment	MODERATE	Yes
66	02	00	Remaining free encryption key warning	DKC environment	SERVICE	Yes
66	10	00	Acquisition failure of the outside encryption key	DKC environment	MODERATE	Yes
67	00	00	Warning for depletion of cache management devices	Cache	MODERATE	Yes
68	00	*xx*	Dedupe and compression abnormality detect	DKC environment	MODERATE	Yes
76	00	00	CUDG detected error	DKC environment	MODERATE	Yes
79	00	*xx*	BOOT detected error	DKC environment	MODERATE	Yes
7d	00	0*x*	GUM error	DKC environment	MODERATE	Yes
7d	01	0*x*	LAN error (Internal Network)	DKC environment	MODERATE	Yes
7d	02	0*x*	LAN error (CTL1-CTL2)	DKC environment	MODERATE	Yes
7d	03	0*x*	GUM AuditLog lost	DKC environment	MODERATE	Yes
7d	04	0*x*	GUM AuditLog Warning Threshold was exceeded	DKC environment	MODERATE	Yes
7d	05	0*x*	Notification of Alert failed	DKC environment	MODERATE	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
7d	06	*xx*	MP error	Processor	MODERATE	Yes
7d	07	*xx*	GUM security error detected	DKC environment	MODERATE	Yes
7d	08	*xx*	Failed to recover GUM configuration information	DKC environment	MODERATE	Yes
7d	09	00	DKC warning	Processor	SERIOUS	Yes
7d	0a	*xx*	GUM version warning	DKC environment	MODERATE	Yes
7f	f1	02	SI	DKC environment	SERVICE	No
7f	f1	04	TI	DKC environment	SERVICE	No
7f	f1	06	Volume Migration Pair	DKC environment	SERVICE	No
7f	f7	*xx*	The term of validity is over	DKC environment	MODERATE	Yes
7f	f8	*xx*	The capacity of validity is over	DKC environment	MODERATE	Yes
7f	f9	*xx*	The PP is invalid by assumption PP invalidity	DKC environment	MODERATE	Yes
7f	fa	00	Synchronization time failure	DKC environment	SERVICE	Yes
ac	50	*xx*	DB power off	PS(DKU)	MODERATE	Yes
ac	51	*xx*	DB power recovered	PS(DKU)	SERVICE	Yes
ac	60	00	DKC was set to power error mode	PS(DKC)	MODERATE	Yes
ac	61	00	DKC was released from power error mode	PS(DKC)	SERVICE	Yes
ac	62	00	Destaging startup normal	PS(DKC)	SERVICE	Yes
ac	63	00	Destaging startup failed	PS(DKC)	MODERATE	Yes
ac	80	0*x*	Server failure	DKC environment	SERIOUS	Yes
af	00	*xx*	Injustice JP Warning	DKC environment	MODERATE	Yes
af	10	*xx*	MP Temperature abnormality warning	DKC environment	MODERATE	Yes
af	11	*xx*	External temperature warning	DKC environment	MODERATE	Yes
af	12	*xx*	External temperature alarm	DKC environment	MODERATE	Yes
af	13	*xx*	Thermal monitor warning	DKC environment	MODERATE	Yes
af	20	*xx*	DKCPS warning	PS(DKC)	MODERATE	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
af	21	*xx*	DKCPS input voltage abnormality	PS(DKC)	MODERATE	Yes
af	30	*xx*	Environmental microcomputer warning	DKC environment	MODERATE	Yes
af	31	*xx*	Device movement mode warning	DKC environment	MODERATE	Yes
af	32	*xx*	Environmental Firmware Update warning	DKC environment	MODERATE	Yes
af	33	*xx*	Voltage change setting warning	PS(DKC)	MODERATE	Yes
af	40	*xx*	BKM/BKMF warning	DKC environment	MODERATE	Yes
af	41	*xx*	Battery replacement should be scheduled	Battery	MODERATE	Yes
af	42	*xx*	CHBB environmental microcontroller warning	DKC environment	MODERATE	Yes
af	43	*xx*	SCM environmental microcontroller warning	DKC environment	MODERATE	Yes
af	44	*xx*	CHBB environmental firmware update warning	DKC environment	MODERATE	Yes
af	45	*xx*	SCM environmental firmware update warning	DKC environment	MODERATE	Yes
af	46	*xx*	SWPK temperature warning	DKC environment	MODERATE	Yes
af	48	*xx*	CHBB voltage change failure warning	DKC environment	MODERATE	Yes
af	49	*xx*	SCM voltage change failure warning	DKC environment	MODERATE	Yes
af	4a	*xx*	CHBBPS warning	DKC environment	MODERATE	Yes
af	4b	*xx*	CHBBPS abnormal input voltage	DKC environment	MODERATE	Yes
af	4c	*xx*	CHBBFAN warning	DKC environment	MODERATE	Yes
af	4d	*xx*	Panel switch warning	DKC environment	MODERATE	Yes
af	4e	*xx*	Invalid PS ON warning	DKC environment	MODERATE	Yes
af	50	*xx*	DBPS warning	PS(DKU)	MODERATE	Yes
af	60	*xx*	DBPS input voltage abnormality	PS(DKU)	MODERATE	Yes
af	70	00	DB External temperature warning	DKU environment	MODERATE	Yes
af	71	00	DB External temperature Alarm	DKU environment	MODERATE	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
af	80	*xx*	ENC warning	DKU environment	MODERATE	Yes
af	e4	*xx*	Life expiry warning for DB air filter	DKU environment	SERVICE	Yes
af	f0	*xx*	UPS warning	PS(DKC)	MODERATE	Yes
af	f1	*xx*	GUM warning	DKC environment	MODERATE	Yes
af	f2	*xx*	CFM error	Cache	MODERATE	Yes
af	f3	*xx*	FAN warning	Fan(DKC)	MODERATE	Yes
af	f4	00	Life expiry warning for DKC air filter	DKC environment	SERVICE	Yes
bf	c0	10	DKC ALARM LED light on	Processor	SERIOUS	Yes
cf	10	*xx*	SAS CTL blocking	DKC environment	MODERATE	Yes
cf	11	*xx*	SAS Port (WideLink) is partially blocked	DKC environment	SERVICE	Yes
cf	12	*xx*	SAS PORT BLOCK[3]	DKC environment	MODERATE	Yes
cf	13	*xx*	SAS-CTL Error detection	DKC environment	SERIOUS	Yes
cf	14	*xx*	Recovered from ENC temporary failure successfully[3]	DKC environment	SERVICE	Yes
cf	88	*xx*	CTL blocking	DKC environment	MODERATE	Yes
cf	8a	*xx*	CTL blockade due to CTL interconnect path failure	DKC environment	MODERATE	Yes
d0	0*x*	*xx*	Remote Copy start	DKC environment	SERVICE	Yes
d0	1*x*	*xx*	Remote Copy normal end	DKC environment	SERVICE	Yes
d0	2*x*	*xx*	Pair end	DKC environment	SERVICE	Yes
d1	0*x*	*xx*	HRC pair status change(MCU command), SMPL -> COPY	DKC environment	SERVICE	Yes
d1	1*x*	*xx*	HRC pair status change(MCU command), SMPL -> PAIR	DKC environment	SERVICE	Yes
d1	2*x*	*xx*	HRC pair status change(MCU command), COPY -> PAIR	DKC environment	SERVICE	Yes
d1	3*x*	*xx*	HRC pair status change(MCU command), COPY -> PSUx	DKC environment	SERVICE	Yes
d1	4*x*	*xx*	HRC pair status change(MCU command), PAIR -> PSUx	DKC environment	SERVICE	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
d1	5*x*	*xx*	HRC pair status change(MCU command), PAIR -> SMPL	DKC environment	SERVICE	Yes
d1	6*x*	*xx*	HRC pair status change(MCU command), COPY -> SMPL	DKC environment	SERVICE	Yes
d1	7*x*	*xx*	HRC pair status change(MCU command), PSUx -> SMPL	DKC environment	SERVICE	Yes
d1	8*x*	*xx*	HRC pair status change(MCU command), PSUx -> COPY	DKC environment	SERVICE	Yes
d1	9*x*	*xx*	HRC pair status change(MCU command), COPY -> PSUx	DKC environment	SERVICE	Yes
d1	a*x*	*xx*	HRC pair status change(MCU command), COPY -> PSUx	DKC environment	SERVICE	Yes
d1	b*x*	*xx*	HRC pair status change(MCU command), PSUx -> PSUx	DKC environment	SERVICE	Yes
d4	0*x*	*xx*	Pair suspend(RIO path closed)	DKC environment	SERIOUS	Yes
d4	1*x*	*xx*	Pair suspend(P-VOL error)	DKC environment	SERIOUS	Yes
d4	2*x*	*xx*	Pair suspend(S-VOL error)	DKC environment	SERIOUS	Yes
d4	4*x*	*xx*	Pair suspend(RVOL Suspend report)	DKC environment	SERIOUS	Yes
d4	5*x*	*xx*	Pair suspend(S-VOL Simplex report)	DKC environment	SERIOUS	Yes
d4	6*x*	*xx*	Pair suspend(Communication error at RCU)	DKC environment	SERIOUS	Yes
d4	7*x*	*xx*	Pair suspend(Error detected at RCU)	DKC environment	SERIOUS	Yes
d4	f*x*	*xx*	Pair status incorrect	DKC environment	SERIOUS	Yes
d8	0*x*	*xx*	Volume to be used by UR was defined	DKC environment	SERVICE	Yes
d8	1*x*	*xx*	Volume used by UR began copying	DKC environment	SERVICE	Yes
d8	2*x*	*xx*	Volume used by UR completed copying	DKC environment	SERVICE	Yes
d8	3*x*	*xx*	Volume used by UR received suspension request	DKC environment	SERVICE	Yes
d8	4*x*	*xx*	Volume used by UR completed suspension transaction	DKC environment	SERVICE	Yes
d8	5*x*	*xx*	Volume used by UR received request for deletion	DKC environment	SERVICE	Yes
d8	6*x*	*xx*	Volume used by UR completed deletion	DKC environment	SERVICE	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
d8	7*x*	*xx*	Volume used by UR was defined	DKC environment	SERVICE	Yes
d8	8*x*	*xx*	Volume used by UR was defined in hold	DKC environment	SERVICE	Yes
d8	9*x*	*xx*	PVOL used by UR was defined in hold	DKC environment	SERVICE	Yes
d9	0*x*	*xx*	Change to SVOL was received from MCU, SMPL -> COPY	DKC environment	SERVICE	Yes
d9	1*x*	*xx*	Change to SVOL was received from MCU, SMPL -> PAIR	DKC environment	SERVICE	Yes
d9	2*x*	*xx*	Change to SVOL was received from MCU, COPY -> PAIR	DKC environment	SERVICE	Yes
d9	3*x*	*xx*	Change to SVOL was received from MCU, COPY -> PSUx	DKC environment	SERVICE	Yes
d9	4*x*	*xx*	Change to SVOL was received from MCU, PAIR -> PSUx	DKC environment	SERVICE	Yes
d9	5*x*	*xx*	Change to SVOL was received from MCU, PAIR -> SMPL	DKC environment	SERVICE	Yes
d9	6*x*	*xx*	Change to SVOL was received from MCU, COPY -> SMPL	DKC environment	SERVICE	Yes
d9	7*x*	*xx*	Change to SVOL was received from MCU, PSUx -> SMPL	DKC environment	SERVICE	Yes
d9	8*x*	*xx*	Change to SVOL was received from MCU, PSUx -> COPY	DKC environment	SERVICE	Yes
d9	9*x*	*xx*	Change to SVOL was received from MCU, HOLD -> PAIR	DKC environment	SERVICE	Yes
d9	a*x*	*xx*	Change to SVOL was received from MCU, HOLD -> COPY	DKC environment	SERVICE	Yes
d9	b*x*	*xx*	Change to SVOL was received from MCU, HOLD -> SMPL	DKC environment	SERVICE	Yes
d9	c*x*	*xx*	Change to SVOL was received from MCU, SMPL -> PSUx	DKC environment	SERVICE	Yes
d9	d*x*	*xx*	Change to SVOL was received from MCU, SMPL -> HOLD	DKC environment	SERVICE	Yes
d9	e*x*	*xx*	Change to SVOL was received from MCU, PSUx -> HOLD	DKC environment	SERVICE	Yes
d9	f*x*	*xx*	Change to SVOL was received from MCU, PAIR -> COPY	DKC environment	SERVICE	Yes
da	0*x*	*xx*	Change to SVOL was received from RCU, SUSPEND REQ.	DKC environment	SERVICE	Yes
da	1*x*	*xx*	Change to SVOL was received from RCU, SUSPEND END	DKC environment	SERVICE	Yes
da	2*x*	*xx*	Change to SVOL was received from RCU, PSUx -> SMPL	DKC environment	SERVICE	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
da	3*x*	*xx*	Change to SVOL was received from RCU, COPY -> SMPL	DKC environment	SERVICE	Yes
da	4*x*	*xx*	Change to SVOL was received from RCU, PAIR -> SMPL	DKC environment	SERVICE	Yes
da	5*x*	*xx*	Change to SVOL was received from RCU, DELETING END	DKC environment	SERVICE	Yes
da	6*x*	*xx*	Change to SVOL was received from RCU, HOLD -> SMPL	DKC environment	SERVICE	Yes
dc	0*x*	*xx*	Pair suspend(RIO path closed)	DKC environment	SERIOUS	Yes
dc	1*x*	*xx*	Pair suspend(M-VOL error)	DKC environment	SERIOUS	Yes
dc	2*x*	*xx*	Pair suspend(R-VOL error)	DKC environment	SERIOUS	Yes
dc	4*x*	*xx*	Pair suspend(Suspend report)	DKC environment	SERIOUS	Yes
dc	5*x*	*xx*	Pair suspend(Simplex report)	DKC environment	SERIOUS	Yes
dc	6*x*	*xx*	Pair suspend(Communication error at RCU)	DKC environment	SERIOUS	Yes
dc	7*x*	*xx*	Pair suspend(Error detected at RCU)	DKC environment	SERIOUS	Yes
dc	8*x*	*xx*	Pair suspend(MCU P/S OFF)	DKC environment	SERVICE	Yes
dc	9*x*	*xx*	Pair suspend(Delta volume error)	DKC environment	SERIOUS	Yes
dc	a*x*	*xx*	Pair suspend(Spread by error of another affiliate)	DKC environment	SERIOUS	Yes
dc	e0	*xx*	UR M-JNL Meta overflow warning	DKC environment	MODERATE	Yes
dc	e1	*xx*	UR M-JNL Data overflow warning	DKC environment	MODERATE	Yes
dc	e2	*xx*	UR R-JNL Meta overflow warning	DKC environment	MODERATE	Yes
dc	e3	*xx*	UR R-JNL Data overflow warning	DKC environment	MODERATE	Yes
dc	f0	*xx*	HUR read JNL was interrupted for 1 minute (at MCU)	DKC environment	MODERATE	Yes
dc	f1	*xx*	HUR read JNL was interrupted for 5 minute (at MCU)	DKC environment	SERIOUS	Yes
dc	f2	*xx*	HUR read JNL was interrupted for 1 minute (at RCU)	DKC environment	MODERATE	Yes
dc	f3	*xx*	HUR read JNL was interrupted for 5 minute (at RCU)	DKC environment	SERIOUS	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
dc	f4	*xx*	URxUR M-JNL Meta full Warning	DKC environment	MODERATE	Yes
dc	f5	*xx*	URxUR M-JNL Data full Warning	DKC environment	MODERATE	Yes
dd	0*x*	*xx*	GAD for this volume was suspended (Due to an unrecoverable failure on the remote copy connections)	Failure with paired volumes	SERIOUS	Yes
dd	1*x*	*xx*	GAD for this volume was suspended (Due to a failure on the volume)	Failure with paired volumes	SERIOUS	Yes
dd	2*x*	*xx*	GAD for this volume was suspended (Due to an internal error condition detected)	Failure with paired volumes	SERIOUS	Yes
dd	3*x*	*xx*	Status of the P-VOL was not consistent with the S-VOL	Failure with paired volumes	SERIOUS	Yes
de	e0	*xx*	Quorum Disk Restore	Drive	SERVICE	Yes
de	f0	*xx*	Quorum Disk Blocked	Drive	SERIOUS	Yes
df	6*x*	*xx*	Drive port temporary error(Drive path: Boundary 0)[2]	Drive	SERVICE	Yes
df	7*x*	*xx*	Drive port temporary error(Drive path: Boundary 1)[2]	Drive	SERVICE	Yes
df	8*x*	*xx*	Drive port blockade(Drive path: Boundary 0)[2]	Drive	MODERATE	Yes
df	9*x*	*xx*	Drive port blockade(Drive path: Boundary 1)[2]	Drive	MODERATE	Yes
df	a*x*	*xx*	LDEV blockade(Path 0 / Drive port blockade)[2]	Drive	SERIOUS	Yes
df	b*x*	*xx*	LDEV blockade(Path 1 / Drive port blockade)[2]	Drive	SERIOUS	Yes
df	c*x*	*xx*	Drive Link Rate Abnormality (Path 0)[2]	Drive	SERVICE	Yes
df	d*x*	*xx*	Drive Link Rate Abnormality (Path 1)[2]	Drive	SERVICE	Yes
df	f*x*	*xx*	Response late Drive[2]	Drive	SERVICE	Yes
e0	00	0*x*	Unified Hypervisor failure (S/W failure)	DKC environment	SERIOUS	No
e0	01	*x*2	NASFW failure (Unified Hypervisor failure)	DKC environment	SERIOUS	No
e0	02	0*x*	Hypervisor Network Module failure	DKC environment	MODERATE	No
e0	04	0*x*	NASFW persistent failure	DKC environment	SERIOUS	No

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
e0	05	*x*2	NASFW failure (S/W failure)	DKC environment	SERIOUS	No
e0	06	0*x*	Unified Hypervisor partial failure (S/W failure)	DKC environment	SERIOUS	No
e0	07	*x*2	NASFW boot failure (MBR corruption)	DKC environment	SERIOUS	No
e0	08	*x*2	Unified Hypervisor failure (Boot disk access error)	DKC environment	SERIOUS	No
e0	09	0*x*	NASFW boot failure (S/W failure)	DKC environment	SERIOUS	No
ef	0*x*	*xx*	Drive blockade (drive)(with redundancy)[2]	Drive	SERIOUS	Yes
ef	1*x*	*xx*	Drive blockade (drive)(without redundancy)[2]	Drive	SERIOUS	Yes
ef	2*x*	*xx*	Drive blockade(Effect of Drive Copy normal end)[2]	Drive	SERVICE	Yes
ef	4*x*	*xx*	Pinned slot	Drive	MODERATE	Yes
ef	5*x*	*xx*	External VOL Write Error	Drive	MODERATE	Yes
ef	9*x*	*xx*	LDEV blockade (Effect of drive blockade)[2]	Drive	SERIOUS	Yes
ef	a*x*	*xx*	Drive temporary error[2]	Drive	SERVICE	Yes
ef	c*x*	*xx*	Correction access occurred[2]	Drive	SERIOUS	Yes
ef	d0	00	External storage system connection device blockade	Drive	SERIOUS	Yes
ef	e*x*	*xx*	Reboot stopped due to much write pending data	Drive	SERVICE	Yes
ef	fc	*xx*	PCI cable connection error	DKC environment	MODERATE	Yes
ef	fd	*xx*	Expander failure	DKC environment	SERIOUS	Yes
ef	fe	*xx*	UNIT connection error	DKC environment	MODERATE	Yes
fe	00	00	Cache battery is being charged	Cache	SERIOUS	Yes
fe	01	00	End of Cache Write Through	Cache	SERVICE	Yes
fe	02	00	Start of Cache Write Through	Cache	MODERATE	Yes
fe	03	0*x*	CFM type error or CFM shortage	Cache	SERIOUS	Yes
fe	04	0*x*	Mounting Battery shortage	Battery	SERIOUS	Yes
ff	21	*xx*	LANB blocking	DKC environment	MODERATE	Yes
ff	4*x*	*xx*	Pinned slot	Cache	MODERATE	Yes
ff	5*x*	*xx*	External VOL Read Error	Drive	MODERATE	Yes

Trap reference code			Description	Section	Alert level (Severity)	Host report[1]
SIM 22	SIM 23	SIM 13				
ff	c3	0*x*	Cache Package Blockade Processing end	Cache	SERVICE	Yes
ff	cc	*xy*	CFM patrol check error	Cache	MODERATE	Yes
ff	cd	0*x*	Area is volatilized	Cache	SERVICE	Yes
ff	cf	*xx*	Module group is volatilized	Cache	SERVICE	Yes
ff	d4	00	Hard implementation out of the definition	DKC environment	MODERATE	Yes
ff	e2	0*x*	SM area blocking	SM	SERIOUS	Yes
ff	e4	0*x*	Replace failed	SM	SERIOUS	Yes
ff	e7	00	Shared memory is volatiled	SM	SERIOUS	Yes
ff	e8	00	Definition/Installation mismatch	Cache	ACUTE	Yes
ff	ea	0*x*	Recovery of area blocked temporarily was completed	SM	SERVICE	Yes
ff	ee	0*x*	Area temporary blocking	SM	SERVICE	Yes
ff	ef	00	Rebooted without volatilization	SM	SERVICE	Yes
ff	f0	*xx*	Cache correctable error	Cache	SERVICE	Yes
ff	f4	00	Area blocking	Cache	SERIOUS	Yes
ff	f5	0*x*	Both area failed	Cache	MODERATE	Yes
ff	f7	*xx*	GUM blocking	DKC environment	MODERATE	Yes
ff	f9	0*x*	Replace failed	Cache	SERVICE	Yes
ff	fa	*xx*	Battery warning	Battery	MODERATE	Yes
ff	fe	*xx*	Warning for forcible volatile mode	DKC environment	MODERATE	Yes

Legend:

- **Yes:** This SIM performs the host report.
- **No:** This SIM does not perform the host report.
- *x*: A hexadecimal number from 0 to f.

1. If you select All for Notification Alert in the **Set Up Alert Notifications** window, the SNMP agent reports all SIMs. If you select Host Report, the SNMP agent reports only SIMs that perform the host report.
2. *xxx*: The right-hand digit of SIM 23 and both digits of SIM 13 can be converted to the number of the drive box and drive where the error occurred. For details, see Obtaining drive box and drive numbers on page 60.
3. "Recovered from ENC temporary failure successfully" (cf14*xx*) indicates that "SAS PORT BLOCK" (cf12*xx*) occurred due to a temporary failure of ENC at the location indicated by the SAS-PORT number (*xx*) was recovered automatically. Therefore, no action by service personnel is required. However, if the SAS-PORT number indicated by SAS PORT BLOCK (cf12*xx*) is different from the one in cf14*xx*, action must be taken by service personnel.

Obtaining drive box and drive numbers

For certain trap reference codes, the right-hand digit of SIM 23 and both digits of SIM 13 form a three-digit hexadecimal number that can be converted to the number of the drive box and drive where the error occurred.

Procedure

1. Combine the right-hand digit of SIM 23 and both digits of SIM 13 form a three-digit hexadecimal number.
2. Convert the number in step 1 to decimal.

   For example, A9E in hexadecimal is 2,718 in decimal.
3. Divide the the number in step 2 by 64. The quotient is the drive box number and the remainder is the drive number.

   For example, 2,718 / 64 = 42 with a remainder of 30. Therefore, The drive box number is 42 and the drive number is 30.

Examples

The following table provides examples of trap reference codes and their corresponding drive box and drive numbers.

Hexadecimal trap value	Decimal value	Decimal value / 64		Drive box number	Drive number
		Quotient	Remainder		
A9E	2,718	42	30	DB-42	HDD42-30
436	1,078	16	54	DB-16	HDD16-54
BFB	3,067	47	59	DB-47	HDD47-59

5

Troubleshooting

This chapter provides troubleshooting information for the Hitachi SNMP Agent.

- Getting help
- Solving SNMP problems

Getting help

If you have difficulty with any of the procedures included in this document, or if a procedure does not provide the answer or results you expect, please contact customer support.

See https://hdssupport.hds.com for more details.

Solving SNMP problems

This topic describes some problems that can occur with SNMP.

Problem	Causes and solutions
Information cannot be received by GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST operations.	Causes: • An SNMP Manager IP address and community or user have not been added. • GUM failure occurred. • A network environment error occurred. Solutions: • Add an IP address and community or user. (See Adding request authentication for SNMP v1 and v2c on page 26 or Adding request authentication for SNMP v3 on page 27.) • Restore GUM. • Contact your network administrator.
Trap cannot be received.	Causes: • An SNMP Manager IP address and community or user have not been added. • GUM failure occurred. • A network environment error occurred. Solutions: • Add an IP address and community or user. (See Adding trap notification for SNMP v1 and v2c on page 20 or Adding trap notification for SNMP v3 on page 22.) • Enable a license. • Restore GUM. • Contact your network administrator.

Glossary

C

community name

An SNMP entity in which up to 32 names and up to 32 IP addresses can be registered.

E

extension trap

An error message generated by a third-party node and sent to the SNMP agent.

F

failure trap

An error message that indicates a problem within a managed node.

I

IPv4

Internet Protocol, Version 4

IPv6

Internet Protocol, Version 6

M

managed device

A network node on which the SNMP Agent software is installed. Using the agent, managed devices exchange node-specific information with the SNMP management software.

managed node

See managed device.

management information base (MIB)

A virtual database of objects that can be monitored by a network management system. SNMP uses standardized MIBs that allow any SNMP-based tool to monitor any device defined by a MIB file.

MIB

See management information base.

S

Simple Network Management Protocol (SNMP)

An industry-standard protocol that is used to manage and monitor network-attached devices for conditions that warrant administrative attention. The devices can include disk devices, routers, and hubs. SNMP uses Simple Gateway Management Protocol (SGMP) to manage TCP/IP gateways.

SNMP

See *Simple Network Management Protocol*.

SNMP Agent

Software that is installed on the maintenance utility and responds to queries from SNMP Manager.

SNMP Manager

Software that is installed on the network management station that collects and manages information from SNMP agents installed in the managed devices on the network.

SNMP trap

An event generated by an SNMP agent from the managed resource that communicates an event, such as an error or failure.

U

UDP

See user datagram protocol.

user datagram protocol (UDP)

Software that requests data regarding the status of a managed node.

Index

A

access mode
  MIB 36
adding
  request authentication for SNMP v1 and v2c 26
  request authentication for SNMP v3 27
  trap notification for SNMP v1 and v2c 20
  trap notification for SNMP v3 22
alerts
  editing settings 20
architecture
  SNMP environment 13

C

changing
  request authentication for SNMP v1 and v2c 29
  request authentication for SNMP v3 30
  trap notification for SNMP v1 and v2c 23
  trap notification for SNMP v3 24
codes
  SNMP failure trap reference 46
cold trap function, troubleshooting 62
components
  storage system 16
configuration
  extension MIB 38
  SNMP Agent 13
configuring
  alert settings 20

D

definition files, trouble inputting 62
deleting
  SNMP request authentication 31
  SNMP trap notification 25

E

editing
  alert settings 20
environment
  SNMP 13
errors
  REQUEST operation 16
  SNMP Agent, reported by 16
extension trap
  supported types 34
extension traps
  protocol data unit 34

F

failure
  SNMP trap reference codes 46
  trap report 34

H

help
  getting support 62

I

interaction
  SNMP Manager and SNMP Agent 12
introduction 11

M

Management Information Base
  overview 13
MIB
  access mode 36
  configuration
    MIB 36
  extension configuration 38
  extension specifications 38
  mounting specifications 37
  object identifier system 36
  overview 13
  raidExMibAgentVersion 40
  raidExMibDkcCount 40
  raidExMibDKCHWTable 41
  raidExMibDKUHWTable 42
  raidExMibName 40

raidExMibRaidListTable 40
raidExMibTrapListTable 43
raidExMibVersion 40
supported types 35
MIB definition files, trouble inputting 62
mounting
MIB specifications 37
system groups 37

O

objects
identifier system 36
operations
REQUEST 16
SNMP Agent 15
overview
Management Information Base 13
MIB 13
Simple Network Management Protocol 12
SNMP 12
SNMP Agent 14
SNMP Manager 12

P

PDU 34
protocol data unit 34

R

raidExMibAgentVersion 40
raidExMibDkcCount 40
raidExMibDKCHWTable 41
raidExMibDKUHWTable 42
raidExMibName 40
raidExMibRaidListTable 40
raidExMibTrapListTable 43
raidExMibVersion 40
reports
testing, for SNMP traps 32
request authentication
deleting 31
requests
adding authentication for SNMP v1 and v2c 26
adding authentication for SNMP v3 27
changing authentication for SNMP v1 and v2c 29
changing authentication for SNMP v3 30

S

security function, troubleshooting 62
Simple Network Management Protocol
overview 12
SNMP
architecture 13
environment 13
failure trap reference codes 46
interaction of manager and agent 12
overview 12
traps 14, 15
SNMP Agent
configuration 13
environment 13
errors reported 16
operations, types of 15
overview 14
traps 15
SNMP Manager
components, status of 16
environment 13
overview 12
status of components 16
specifications
extension MIB 38
MIB mounting 37
status
storage system components 16
support
getting help 62
system groups
mounting 37

T

testing
SNMP trap report 32
trap notification
deleting 25
traps
failure report 34
SNMP 14
SNMP Agent 15
SNMP failure reference codes 46
SNMP v1 and v2c, adding notification for 20
SNMP v1 and v2c, changing notification for 23
SNMP v3, adding notification for 22
SNMP v3, changing notification for 24
supported types 34
testing, of SNMP trap reports 32
triggers 15
troubleshooting
abnormal response to SNMP commands 62
inputting MIB definition files 62
SNMP cold trap function 62
SNMP security function 62

Hitachi Vantara

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 95050-2639 USA
www.HitachiVantara.com
community.HitachiVantara.com

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