Hitachi Virtual Storage Platform 5000 Series
SVOS RF 9.8.6

Hitachi Alert Notification Guide

The Alert Notification feature provides failure monitoring functions (which include monitoring of your storage systems by using SNMP), enabling you to recognize and fix failures in your storage system.

Contents

Contents

Preface

The Alert Notification feature provides failure monitoring functions (which include monitoring of your storage systems by using SNMP), enabling you to recognize and fix failures in your storage system.

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

Intended audience

This document is intended for system administrators, Hitachi Vantara representatives, and authorized service providers who install, configure, and operate Hitachi Virtual Storage Platform 5000 series storage systems.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- Hitachi Virtual Storage Platform 5000 series storage systems and the *Product Overview*.
- The Device Manager - Storage Navigator software for the Hitachi Virtual Storage Platform 5000 series, and the *System Administrator Guide*.

Product version

This document revision applies to the following product versions:

- VSP 5000 series: microcode 90-09-01 or later
- SVOS RF 9.8.6 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 the Hitachi Vantara Support Website: https://knowledge.hitachivantara.com/Documents.

Changes in this revision

▪ Added SIM codes of performance degradation alert.

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 additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Important	Highlights information that is essential to the completion of a task.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	CAUTION	Warns the user of a hazardous situation that, if not avoided, could result in major or minor injury.
	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
1 EB	1,024 PB or $1,024^6$ bytes

Accessing product documentation

Product user documentation is available on the Hitachi Vantara Support Website: 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

The Hitachi Vantara Support Website is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website 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 comments 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 LLC.

Thank you!

Chapter 1: Failure monitoring

You can use alert notification email, Syslog, and SNMP for failure monitoring.

Alert notification email

The following example shows an alert notification email that is sent from the storage system to the mail server.

```
VSP 5100 Report
//RAID900 //VSP ////////////////////////////////
//e-Mail Report
////////////////////////////////
Date : 20/04/2020
Time : 00:20:00
Machine : VSP 5100(Serial# 64019)
RefCode : 7fffff
Detail: This is Test Report.
```

The following table describes the components of an alert notification email.

Component	Item in the example	Description
Title	VSP 5100 Report	*product-name-of-the-storage-system* Report

Additional information	//RAID900 //
	VSP ////////////////////////////////
	//e-Mail Report
	////////////////////////////
		The information set in Editing alert notification email settings (on page 16)
		
		Nothing appears if no information is set.

Date	Date : 20/04/2021	The date when the error occurred
Time	Time : 00:20:00	The time when the error occurred
Hardware identification	Machine : VSP 5100 (serial# 400102)	*storage-system-name-set-in-Storage-Navigator*(serial# *serial-number*)
Failure code	RefCode : 7fffff	The reference code that appears in the alert window

Component	Item in the example	Description
Failure detail	Detail: This is Test Report.	Information of failure locations that need maintenance
		Information of a maximum of eight failure locations appears.
		Each information item includes the following items: action code, assumed failure part, and location.

Syslog message

The following examples show Syslog messages that are sent from the storage system to the syslog server.

You can use Hitachi Device Manager - Storage Navigator to select either of the following message formats: RFC3164-compliant or RFC5424-compliant.

For details, see

Syslog file format (RFC3164-compliant)

```
<149> Jan 24 18:10:30 GUM Storage: 0000001571,Service,H2(Serial#400102),Japan-Tokyo,
   1       2           3    4          5           6        7                8

RefCode:7FFA00,Synchronization time failure
                     9
```

No.	Item	Description
1	Priority	The priority of a syslog message is determined according to the following formula, enclosed by angle brackets (< >):
		Priority = 8 × *Facility* + *Severity*
		Facility is 18 (fixed).
		Severity depends on the type of log information:
		▪ 3: Error (abnormal end)
		▪ 4: Warning (partially abnormal end, or an operation was canceled before it could be completed)
		▪ 5: Notice (normal end)
		For example, if *Severity* is 3 (Error), <147> is output as the priority value.

Chapter 1: Failure monitoring

No.	Item	Description
2	Date, time[1]	The date and time in the format of "*MMM DD HH*:*MM*:*SS*" *MMM*: first three letters of the month (Jan to Dec) *DD*: date If *DD* is a single digit (for example, 1), it is displayed as " 1" (with a blank space before "1") and not as "01". *HH*: hour *MM*: minute *SS*: second
3	Detected location	"SVP" (fixed)
4	Program name	"Storage" (fixed)
5	Message identification	The serial number (0000000000 to 4294967295)
6	Event type	Any of the following event category names. (The event category corresponds to *Severity*.) - Acute *Severity* is 3 (Error). - Serious *Severity* is 3 (Error). - Moderate *Severity* is 4 (Warning). - Service *Severity* is 5 (Notice).
7	Hardware identification[2]	The storage system name and serial number
8	Related information	The location identification information set in the Syslog tab in the **Edit Alert Settings** window of Device Manager - Storage Navigator
9	Detailed information	The SIM reference code and failure information that are displayed in the alert window

Notes:

1. A date and time being set on SVP are output as log data. If a failure, such as a SVP failure and a LAN failure, occurs in the storage system, the date and time may be output of the accumulated date and time since January 01, 1970.

Chapter 1: Failure monitoring

No.	Item	Description
2.		While the controller model is being upgraded, information before upgrade might be output. While the controller model is being downgraded, information before downgrade might be output.

Syslog file format (RFC5424-compliant)

```
<149>1 2017-01-24T18:17:09.0+09:00 GUM Storage - - - 0000001572,Service,H2(Serial#400102),
  1  2          3                    4    5   678  9         10              11

Japan-Tokyo,RefCode:7FFA00,Synchronization time failure
     12                    13
```

No.	Item	Description
1	Priority	The priority of a syslog message is determined according to the following formula, enclosed by angle brackets (< >): *Priority = 8 × Facility + Severity* *Facility* is 18 (fixed). *Severity* depends on the type of log information: ▪ 3: Error (abnormal end) ▪ 4: Warning (partially abnormal end, or an operation was canceled before it could be completed) ▪ 5: Notice (normal end) For example, if *Severity* is 3 (Error), <147> is output as the priority value.
2	Version	"1" (fixed)
3	Date, time[1]	The date, time, and the time difference between UTC (Coordinated Universal Time) and the local time in the format of "*YYYY-MM-DD*T*hh*:*mm*:*ss.s*±*hh*:*mm*" ▪ *YYYY*: year, *MM*: month, *DD*: date ▪ *hh*: hour, *mm*: minute, *ss.s*: second in one decimal place ▪ ±*hh*:*mm*: hours and minutes of the time difference. "Z" is written instead of "± *hh*:*mm*" when there is no time difference between UTC and the local time, such as "2018-12-26T23:06:58.0Z".
4	Detected location	"SVP" (fixed)
5	Program name	"Storage" (fixed)
6	Process name	"-" (fixed.)

Chapter 1: Failure monitoring

No.	Item	Description
7	Message ID	"-" (fixed.)
8	Structured data	"-" (fixed.)
9	Message identification	The serial number (0000000000 to 4294967295)
10	Event type	Any of the following event category names. (The event category corresponds to *Severity*.) ▪ Acute *Severity* is 3 (Error). ▪ Serious *Severity* is 3 (Error). ▪ Moderate *Severity* is 4 (Warning). ▪ Service *Severity* is 5 (Notice).
11	Hardware identification[2]	The storage system name and serial number
12	Related information	The location identification information set in the Syslog tab in the **Edit Alert Settings** window of Device Manager - Storage Navigator
13	Detailed information	The SIM reference code and failure information that are displayed in the alert window

Notes:

1. A date and time being set on SVP are output as log data. If a failure, such as a SVP failure and a LAN failure, occurs in the storage system, the date and time may be output of the accumulated date and time since January 01, 1970.

2. While the controller model is being upgraded, information before upgrade might be output. While the controller model is being downgraded, information before downgrade might be output.

SNMP

SNMP data is sent from a storage system to the SNMP agent. The following table describes an example of event details that are contained in SNMP data.

Component	Example	Description
TRAP type	raideventUsermoderate	Failure level
eventTrapSerialNumber	1	Serial number of the product
eventTrapNickname	RAID900	Product name
eventTrapREFCODE	212051	The reference code that appears in the alert window
eventTrapPartsID	dkcHWProcessor	Failure location
eventTrapDate	2018/12/21	The date the SNMP Agent received the SNMP data
eventTrapTime	08:27:50	The time the SNMP Agent received the SNMP data
eventTrapDescription	"Channel port blocking"	Information of the failure locations that need maintenance

Chapter 2: Setting alert notification email

By using the Hitachi Device Manager - Storage Navigator, you can manage the alert notificatrion email settings.

Editing alert notification email settings

This topic describes how to specify the email settings necessary to report failure trap reference codes (SIMs).

Before you begin

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

- You must have installed a mail server that supports Simple Mail Transfer Protocol (SMTP). The SVP uses PLAIN or LOGIN of SMTP authentication (SMTP-AUTH) to connect to the mail server. CRAM-MD5 and DIGEST-MD5 of SMTP-AUTH are not supported.

- You must release Port 25 if a firewall is used (because Port 25 is used for communication between the SVP and the mail server).

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Settings** menu, select **Environmental Setting > Edit Alert Settings**.
3. 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.

4. Click the **Email** tab.
5. For **Mail Notice**, select **Enable** to enable that option.

6. In **Email Settings**, enter the destination email address and the attribute (To, Cc, Bcc).

   ▪ To add an email address, click **Add** and then specify the email address and attribute in the **Add Address** window.

   ▪ To change an email address and the attribute, select the check box for the email address you want to change, and then click **Change**. You can change the email address and attribute in the **Change Settings** window.

   You can select multiple email addresses. If you select multiple email addresses, you can change their attributes only.

   ▪ To delete email addresses, select the check boxes for the email addresses you want to delete, and then click **Delete**.

   Make sure that you specify these settings if **Mail Notice** is set to **Enable**.

7. Enter the source email address (required) and the return email address (option).

   You can enter up to 255 characters of alphabets, numerals, and symbols (!, #, $, %, &, `, +, -, *, /, ', ^, {, }, _, and .).

8. Enter the information of the email server.

   ▪ **Identifier**

   To specify the host name, select **Identifier** and then enter up to 63 characters of alphabets, numerals, and symbols (! $ % ( ) ' - _ . @ ~).

   ▪ **IPv4**

   To specify an IPv4 address, select **IPv4** and then enter four numbers (0 to 255) in the following format:

   XXX.XXX.XXX.XXX (Each *XXX* indicates a number.)

   ▪ **IPv6**

   To specify an IPv6 address, select **IPv6** and then enter eight hexadecimal numbers (0 to FFFF) in the following format:

   YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY (Each *YYYY* indicates a hexadecimal number.)

   You can also specify the abbreviated format of IPv6 addresses.

   Make sure that you specify these settings if **Mail Notice** is set to **Enable**.

9. In **SMTP Authentication**, select **Enable** (to use SMTP authentication) or **Disable** (to not to use SMTP authentication). If you select **Enable**, also enter the account name and password that you use for SMTP authentication.

   You can enter up to 255 characters of alphabets, numerals, and symbols (! $ % ( ) ' - _ . @ ~).

   Make sure that you specify these settings if **Mail Notice** is set to **Enable**.

10. Click **Send Test Email**, if necessary, to test the settings.

11. Confirm that you received the test email.

12. Click **Finish**.

13. Confirm the settings in the **Confirm** window, and then enter the task name in **Task Name**.

14. Click **Apply**.

The task is registered. If the check box for **Go to tasks window for status** is selected, the **Tasks** window opens.

Chapter 3: Setting Syslog

By using the Hitachi Device Manager - Storage Navigator, you can manage Syslog settings.

Editing Syslog settings

This topic describes how to specify the Syslog settings necessary to report a failure in the storage system.

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must install a server that supports Syslog.
- You must release the port to be used for sending Syslog data if a firewall is used.
- If you use the new Syslog protocol (TLS1.2/RFC5424), you must specify, for subjectAltName or CommonName in the syslog server certificate, the host name or IP address of the syslog server.
- If you specify the host name of the syslog server as the transfer destination, you must register the host name and domain name of the syslog server in the DNS server.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Settings** menu, select **Environmental Setting > Edit Alert Settings**.
3. 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.

4. Click the **Syslog** tab.
5. For **Transfer Protocol**, select the protocol you want to use for sending Syslog data.

6. To send Syslog data to the primary server, select **Enable** for **Primary Server** and then specify the following items:

   - IP Address/Host Name

     Specify the IPv4 address, IPv6 address, or host name of the syslog server to which you want to send syslog data. To specify the host name, select **Identifier** and then enter up to 255 characters of alphabets, numerals, and symbols (! $ % - . @ _ ` ~).

   - Port Number

   - Client Certificate File Name, Password, and Root Certificate File Name

     Specify this setting only when **New Syslog Protocol (TLS1.2/RFC5424)** is selected for **Transfer Protocol**.

7. To send Syslog data to the alternative server (secondary server), select **Enable** for **Secondary Server** and then specify the following items:

   - IP Address/Host Name

   - Port Number

   - Client Certificate File Name, Password, and Root Certificate File Name

     Specify this setting only when **New Syslog Protocol (TLS1.2/RFC5424)** is selected for **Transfer Protocol**.

8. Specify a name you want for **Location Identification Name** to identify the storage system.

9. If **New Syslog Protocol (TLS1.2/RFC5424)** is selected for **Transfer Protocol**, specify the values for **Timeout**, **Retry Interval**, and **Number of Retries**.

10. Click **Send Test Message to Syslog Server**, if necessary, to test the settings.

11. Confirm that the Syslog server received the log message (detailed data: "RefCode: 7FFFFF, This is Test Report.").

12. Click **Finish**.

13. Confirm the settings in the **Confirm** window, and then enter the task name in **Task Name**.

14. Click **Apply**.

    The task is registered. If the check box for **Go to tasks window for status** is selected, the **Tasks** window opens.

Chapter 4: Setting SNMP

By using the Hitachi Device Manager - Storage Navigator, you can manage alert settings, SNMP trap notification, SNMP request authentication, and test SNMP trap reports.

Editing alert settings

This topic describes how to set the Edit Alert Settings.

> ⚠ **Caution:** Be sure to document your storage system name before this process, because the settings will be cleared when the SVP is replaced.

Before you begin

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 **Settings** menu, select **Environmental Setting > Edit Alert Settings**.
3. 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.)
4. Click the **SNMP** tab.
5. For **Extension SNMP**, select **Enable** to enable that option.
6. In **System Group Information**, enter the **Storage System Name**, **Contact**, and **Location**.

   Changes made to information here are also reflected in the **Storage System** window in Device Manager - Storage Navigator.
7. Click **Finish**.
8. Enter a name for the task in the **Confirm** window, confirm the settings, and then click **Apply**.

Managing SNMP trap notification

Use the procedure for the SNMP version you use to set SNMP trap notification. The items to specify are different depending on the SNMP version.

> 📄 **Note:**
>
> **Required operations on the SNMP Manager after maintenance**
>
> If you are using SNMP v3, and authentication and encryption are enabled for traps, the following operations are required on the SNMP Manager after maintenance operations (including replacement of controller boards). If you are asked by maintenance personnel, perform the following operations.
>
> To check whether the SNMP version is SNMP v3, in the maintenance utility, check the setting for SNMP version in the SNMP tab in the **Alert Notifications** window. To check whether authentication or encryption is enabled for traps, check the setting for Sending Trap Setting in the SNMP tab in the **Set Up Alert Notifications** window.
>
> - Restart the SNMP Manager, or reregister the storage systems to be monitored on the SNMP Manager.
>
> - Test trap reports. (See Testing the SNMP trap report (on page 32).)
>
> - Obtain the trap history in MIB raidExMibTrapListTable from the SNMP Manager, and then perform proper storage management for traps that are not yet confirmed. For details about the format of the trap history, see raidExMibTrapListTable (on page 51).

Adding trap notification for SNMP v1 and SNMP v2c

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

Before you begin

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 **Settings** menu, select **Environmental Setting > Edit Alert Settings**.
3. Click the **SNMP** tab.
4. Under **SNMP Agent**, select **Enable**.
5. Under **SNMP Version**, select **v1** or **v2c**.
6. Under **Registered Sending Trap Settings**, click **Add**.
7. In the **Add Sending Trap Setting** window, under **Community**, enter a community name or select from the list of existing community names.

   You can enter up to 180 alphanumeric characters. The following special characters are not allowed: **"**, \, **;**, **:**, **,**, *, ?, <, >, |, /, ^, &, **'**, and %.

   Do not use a space either at the beginning or the end.

8. Under **Send Trap To**, perform one or more of the following steps:

   - To enter a new IP address, select **IPv4** or **IPv6**, and then enter the IP address.

   - To use an existing IP address, select from the list of existing IP addresses.

   - To add more than one IP address, click **Add IP Address** to add additional input fields.

   - To delete an IP address from **Send Trap To**, click the minus (-) button next to 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.

9. Click **OK**.
   The IP address and community you entered are added to the **Registered Sending Trap Settings** table.

10. Click **Finish**.

11. In the **Confirm** window, enter a name for the task, 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 *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Settings** menu, select **Environmental Setting > Edit Alert Settings**.
3. Click the **SNMP** tab.
4. Under **SNMP Agent**, select **Enable**.
5. Under **SNMP Version**, select **v3**.
6. Under **Registered Sending Trap Settings**, click **Add**.
7. 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.

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

   You can enter up to 32 alphanumeric characters. The following special characters are not allowed: ", \, ;, :, ,, *, ?, <, >, |, /, ^, &, and %.

   Do not use a space either at the beginning or the end.

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.

    Note: If you select **Disable** for **Authentication**, **Encryption** is automatically disabled.

    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 IP address and user you entered are added to the **Registered Sending Trap Settings** table.

12. Click **Finish**.

13. In the **Confirm** window, enter a name for the task, confirm the settings, and then click **Apply**.

Changing trap notification for SNMP v1 and SNMP v2c

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

Before you begin

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 **Settings** menu, select **Environmental Setting > Edit Alert Settings**.

3. Click the **SNMP** tab.

4. Under **SNMP Agent**, select **Enable**.

5. Under **SNMP Version**, select **v1** or **v2c**.

6. Under **Registered Sending Trap Settings**, select the trap setting you want to change, and then click **Change**.
   The **Change Sending Trap Setting** window opens.

7. If you want to change the **Community**, select the **Community** check box, and then enter a community name or select from the list of existing community names.

   You can enter up to 180 alphanumeric characters. The following special characters are not allowed: **"**, \, ;, :, ,, *, ?, <, >, |, /, ^, &, ', and %.

   Do not use a space either at the beginning or the end.

8. If you want to make changes under **Send Trap to**, select the **Send Trap to** check box, and then perform one or more of the following steps:

   ▪ To enter a new IP address, select **IPv4** or **IPv6**, and then enter the IP address.

   ▪ To use an existing IP address, select from the list of existing IP addresses.

   ▪ To add more than one IP address, click **Add IP Address** to add additional input fields.

   ▪ To delete an IP address from **Send Trap To**, click the minus (-) button next to 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.

9. Click **OK**.
   The IP address and community you entered are changed in the **Registered Sending Trap Settings** table.

10. Click **Finish**.

11. In the **Confirm** window, enter a name for the task, 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 *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Settings** menu, select **Environmental Setting > Edit Alert Settings**.
3. Click the **SNMP** tab.
4. Under **SNMP Agent**, select **Enable**.
5. Under **SNMP Version**, select **v3**.

6. Under **Registered Sending Trap Settings**, select the trap setting you want to change, and then click **Change**.
   The **Change Sending Trap Setting** window opens.

7. If you want to make changes under **Send Trap to**, select the **Send Trap to** check box, select **IPv4** or **IPv6**, and then 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 8 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.

8. If you want to change the **User Name**, select the **User Name** check box, and then enter a user name.

   You can enter up to 32 alphanumeric characters. The following special characters are not allowed: **"**, \, ;, :, ,, *, ?, <, >, |, /, ^, &, and %.

   Do not use a space either at the beginning or the end.

9. If you want to make changes under **Authentication**, select the **Authentication** check box, and then select whether to **Enable** or **Disable** authentication.

   If you select **Enable**, perform the following steps:
   a. To change the **Protocol**, select the **Protocol** check box, and then select an authentication type.
   b. To change the **Password**, select the **Password** check box, and then enter a password.

10. If you want to make changes under **Encryption**, select the **Encryption** check box, and then select whether to **Enable** or **Disable** encryption.

    Note: If you select **Disable** for **Authentication**, **Encryption** is automatically disabled.

    If you select **Enable**, perform the following steps:
    a. To change the **Protocol**, select the **Protocol** check box, and then select an encryption type.
    b. To change the **Key**, select the **Key** check box, enter a key, and then enter the key again under **Re-enter Key** for confirmation.

11. Click **OK**.
    The IP address and user you entered are changed in the **Registered Sending Trap Settings** table.

12. Click **Finish**.

13. In the **Confirm** window, enter a name for the task, 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 *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Settings** menu, select **Environmental Setting > Edit Alert Settings**.
3. Click the **SNMP** tab.
4. Under **SNMP Agent**, select **Enable**.
5. Under **SNMP Version**, select your SNMP version.
6. Under **Registered Sending Trap Settings**, select one or more specific combinations of IP address and community or user, and then click **Delete**.
7. Click **Finish**.
8. In the **Confirm** window, enter a name for the task, confirm the settings, and then click **Apply**.

Managing SNMP request authentication

Use the procedure for the SNMP version you use to set SNMP request authentication. The items to specify are different depending on the SNMP version.

Adding request authentication for SNMP v1 and SNMP v2c

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

Before you begin

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 **Settings** menu, select **Environmental Setting > Edit Alert Settings**.
3. Click the **SNMP** tab.
4. Under **SNMP Agent**, select **Enable**.
5. Under **SNMP Version**, select **v1** or **v2c**.
6. Under **Registered Request Authentication Settings**, click **Add**.
7. In the **Add Request Authentication Setting** window, under **Community**, enter a community name or select from the list of existing community names.

   You can enter up to 180 alphanumeric characters. The following special characters are not allowed: ", \, ;, :, ,, *, ?, <, >, |, /, ^, &, ', and %.

   Do not use a space either at the beginning or the end.

Chapter 4: Setting SNMP

8. Under **Request Permitted**, complete one of the following steps:

    ▪ 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, perform one or more of the following steps:

      - To enter a new IP address, select **IPv4** or **IPv6**, and then enter the IP address.

      - To use an existing IP address, select from the list of existing IP addresses.

      - To add more than one IP address, click **Add IP Address** to add additional input fields.

      - To delete an IP address from **Send Trap To**, click the minus (-) button next to 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.

9. Click **OK**
    The community and IP address that you entered are added to the **Registered Request Authentication Settings** table.

10. Click **Finish**.

11. In the **Confirm** window, enter a name for the task, confirm the settings, and then click **Apply**.

Adding request authentication for SNMP v3

This topic describes how to add 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 *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.
2. From the **Settings** menu, select **Environmental Setting > Edit Alert Settings**.
3. Click the **SNMP** tab.
4. Under **SNMP Agent**, select **Enable**.
5. Under **SNMP Version**, select **v3**.
6. Under **Registered Request Authentication Settings**, click **Add**.

7. In the **Add Request Authentication Setting** window, under **User Name**, enter a user name.

    You can enter up to 32 alphanumeric characters. The following special characters are not allowed: **"**, \, ;, :, ,, *, ?, <, >, |, /, ^, &, and %.

    Do not use a space either at the beginning or the end.

8. 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.

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

    > 📄 **Note:** If you select **Disable** for **Authentication**, **Encryption** is automatically disabled.

    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.

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

11. Click **Finish**.

12. In the **Confirm** window, enter a name for the task, confirm the settings, and then click **Apply**.

Changing request authentication for SNMP v1 and SNMP v2c

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

Before you begin

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 **Settings** menu, select **Environmental Setting > Edit Alert Settings**.

3. Click the **SNMP** tab.

4. Under **SNMP Agent**, select **Enable**.

5. Under **SNMP Version**, select **v1** or **v2c**.

6. Under **Registered Request Authentication Settings**, select the authentication setting you want to change, and then click **Change**.
    The **Change Request Authentication Setting** window opens.

7. If you want to make changes under **Community**, select the **Community** check box, and then enter a community name or select from the list of existing community names.

   You can enter up to 180 alphanumeric characters. The following special characters are not allowed: **"**, \, ;, :, ,, *, ?, <, >, |, /, ^, &, ', and %.

   Do not use a space either at the beginning or the end.

8. If you want to make changes under **Request Permitted**, select the **Request Permitted** check box, and then complete one of the following steps:

   ▪ 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, perform one or more of the following steps:

   - To enter a new IP address, select **IPv4** or **IPv6**, and then enter the IP address.

   - To use an existing IP address, select from the list of existing IP addresses.

   - To add more than one IP address, click **Add IP Address** to add additional input fields.

   - To delete an IP address from **Send Trap To**, click the minus (-) button next to 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 8 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. Click **OK**.
   The community and IP address that you entered are changed in the **Registered Request Authentication Settings** table.

10. Click **Finish**.

11. In the **Confirm** window, enter a name for the task, confirm the settings, and then click **Apply**.

Changing request authentication for SNMP v3

This topic describes how to change users and authentication settings 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 *System Administrator Guide*.

Procedure

1. Display the Device Manager - Storage Navigator main window.

2. From the **Settings** menu, select **Environmental Setting > Edit Alert Settings**.

3. Click the **SNMP** tab.

Chapter 4: Setting SNMP

4. Under **SNMP Agent**, select **Enable**.

5. Under **SNMP Version**, select **v3**.

6. Under **Registered Request Authentication Settings**, click **Change**.
   The **Change Request Authentication Setting** window opens.

7. If you want to change the **User Name**, select the **User Name** check box, and then enter a user name.

   You can enter up to 32 alphanumeric characters. The following special characters are not allowed: ", \, ;, :, , , *, ?, <, >, |, /, ^, &, and %.

   Do not use a space either at the beginning or the end.

8. If you want to make changes under **Authentication**, select the **Authentication** check box, and then select whether to **Enable** or **Disable** authentication.

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

   a. To change the **Protocol**, select the **Protocol** check box, and then select an authentication type.

   b. To change the **Password**, select the **Password** check box, and then enter a password.

9. If you want to make changes under **Encryption**, select the **Encryption** check box, and then select whether to **Enable** or **Disable** encryption.

   > **Note:** If you select **Disable** for **Authentication**, **Encryption** is automatically disabled.

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

   a. To change the **Protocol**, select the **Protocol** check box, and then select an encryption type.

   b. To change the **Key**, select the **Key** check box, enter a key, and then enter the key again under **Re-enter Key** for confirmation.

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

11. Click **Finish**.

12. In the **Confirm** window, enter a name for the task, 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 (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 **Settings** menu, select **Environmental Setting > Edit Alert Settings**.
3. Click the **SNMP** tab.
4. Under **SNMP Agent**, select **Enable**.
5. Under **SNMP Version**, select your SNMP version.
6. Under **Registered Request Authentication Settings**, select one or more specific combinations of IP address and community or user, and then click **Delete**.
7. Click **Finish**.
8. In the **Confirm** window, enter a name for the task, confirm the settings, and then click **Apply**.

Testing the SNMP trap report

This topic describes the procedure to test the SNMP trap report.

After you perform this procedure, the test SNMP trap (reference code: 7fffff) is sent to the SNMP Manager registered in the community.

Before you begin

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 **Settings** menu, select **Environmental Setting > Edit Alert Settings**.
3. Click the **SNMP** tab.
4. Click **Send Test SNMP Trap**.
   The test SNMP trap is reported to the IP address registered in the storage system. The events registered in the storage system are reported 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 the changes to the storage system, and then report the test SNMP trap.
5. Verify that the SNMP trap report (reference code 7fffff) is received by the SNMP manager registered in the community.

Required operations on the SNMP Manager after maintenance

If authentication and encryption are enabled for traps while you are using SNMP v3, the following operations are required on the SNMP Manager after maintenance operations (including SVP replacement, SVP microcode exchange, and SVP failover). If you are asked by maintenance personnel, perform the following operations.

To check the SNMP version and whether authentication and encryption are enabled for traps, see SNMP Version and Sending Trap Setting on the SNMP tab in the **Edit Alert Settings** window in the *System Administrator Guide*.

- Restart the SNMP Manager, or reregister the storage systems to be monitored on the SNMP Manager.

- Test the trap report. (See Testing the SNMP trap report (on page 32).)

- Obtain the trap history in MIB raidExMibTrapListTable from the SNMP Manager, and then perform proper storage management for traps that are not yet confirmed. For details about the format of the trap history, see raidExMibTrapListTable (on page 51).

Chapter 5: Troubleshooting

This chapter provides troubleshooting information for the Hitachi SNMP Agent.

Solving SNMP problems

The following problems can occur:

SNMP security function

If the SNMP security function is working, and a command is executed from an IP address that is not entered, you will get a "no reply" return, and a certification error is received for a trap.

SNMP cold trap function

- Depending on your network environment, you might not receive SNMP agent cold traps when the SVP is rebooted.

- The SNMP agent might report Link up/Link down Trap when the SVP reboots.

- A number of Link up/Link down Traps may be reported when the SVP OS is Windows 7.

Abnormal response to SNMP command

If an error occurs in the SVP, traps might not be sent.

While SVP High Reliability Kit is installed (by maintenance personnel)

- Traps might not be reported for errors that occur during installation.

- SNMP commands might not respond normally.

- Cold traps might be reported repeatedly.

- Traps could be reported to an IP address that is not specified in SNMP settings.

Traps cannot be reported

Perform the following:

- Restart the SNMP Manager, or reregister the storage systems to be monitored on the SNMP Manager.

- Confirm that traps can be reported. (See Testing the SNMP trap report (on page 32).)

- Obtain the trap history in MIB raidExMibTrapListTable from the SNMP Manager, and then perform proper storage management for traps that are not yet confirmed. For details about the format of the trap history, see raidExMibTrapListTable (on page 51).

Chapter 6: SNMP overview

This chapter provides an overview of the SNMP implementation for monitoring Hitachi Virtual Storage Platform 5000 series storage systems, including the agent and management functions.

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.
> - An RFC-compliant encryption algorithm is adopted for User-based Security Model (USM) authentication.

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.

Chapter 6: SNMP overview
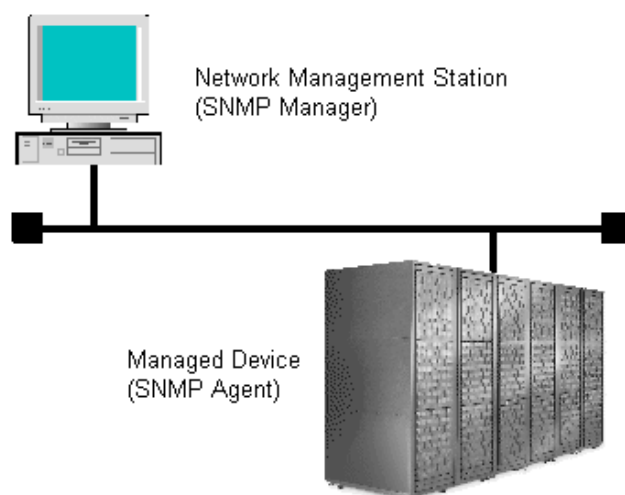
An SNMP manager monitors the devices, which are referred to as managed nodes. Typically, an SNMP Manager polls the SNMP agents on a periodic basis. The manager receives the reports from the agents and determines whether the devices are operating normally. If an abnormal event occurs, an SNMP Agent can 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, `VSP5KMIB.txt`, is located in the `program\SNMP` folder of the software media kit.

SNMP Agent configuration

The SNMP Agent is installed on the service processor (SVP), which is the computer within the storage system that manages the storage system.

The storage system has an exclusive LAN for communications with the SVP and a separate LAN for SNMP. The configuration of each Network Management Station is determined by the type of SNMP manager.

The following figure illustrates the SNMP environment.
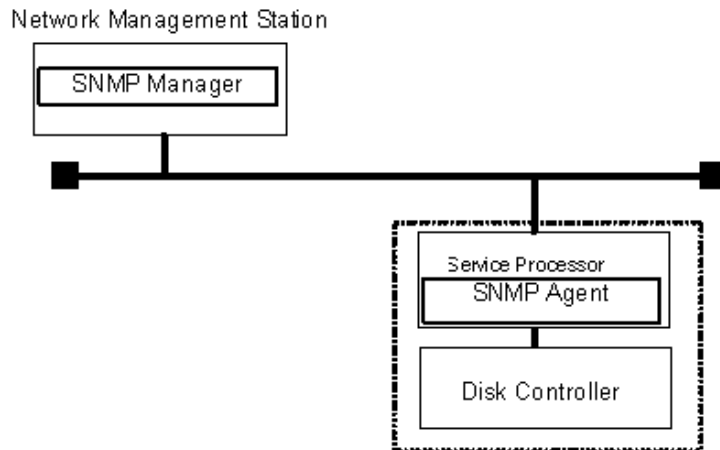
> 📝 **Note:** If you cannot enter multiple MIB definition files in the SNMP Manager software, use the MIB definition file for VSP 5000 series. In this case, determine the storage system model by referring to the storage system nickname displayed in an error report.

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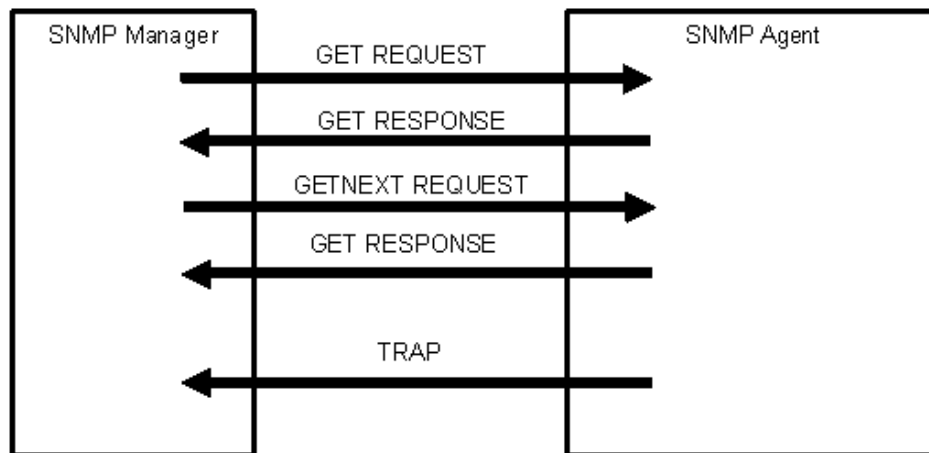
SNMP Agent overview

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 sends traps 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, and an identifier of the component.

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.

An SNMP Agent logs the most recent 10,000 traps, so you can see the trap history of a particular device.

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.

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	Processors
	BUS
	Cache
	Shared memory
	Power supplies
	Batteries
	Fans
	Others
Disk Unit	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.

Chapter 7: SNMP supported MIBs

You can use the SNMP supported MIBs reference to find information on the standard and extension MIB specifications and trap configuration.

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 nickname of the device where the failure occurred.
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.

Name	Object identifier	Type	Description
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.			

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	Object Identifier	Description
1	RaidEventUserAcute	1.3.6.1.4.1.116.3.1 1.4.1.1.0.1	All operations in a storage system stopped.
2	RaidEventUserSerious	1.3.6.1.4.1.116.3.1 1.4.1.1.0.2	Operation in a component where a failure occurred stopped.
3	RaidEventUserModerate	1.3.6.1.4.1.116.3.1 1.4.1.1.0.3	Partial failure.
4	RaidEventUserService	1.3.6.1.4.1.116.3.1 1.4.1.1.0.4	Minor failure.

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		Supported?
Standard MIB: MIB-II	system group	Yes

Chapter 7: SNMP supported MIBs

MIB		Supported?
	interface group	No
	at group	No
	ip group	No
	icmp group	No
	tcp group	No
	udp group	No
	egp group	No
	snmp group	No
Extension MIB		Yes

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.

Execute `snmpwalk` as follows to obtain all MIB objects:

1. Specify object identifier 1.3.6.1.2.1 to obtain the information shown in 1.
2. Specify object identifier 1.3.6.1.4.1.116 to obtain the information shown in 2.

```
root
|―iso(1)
  |―org(3)
    |―dod(6)
      |―internet(1)
        |―mgmt(2)
        |  |  |―mib-2(1)          Standard  MIB  MIB-2          …1
        |  |     |―system(1)
        |
        |―private(4)
          |―enterprises(1)
            |―hitachi(116)
            |  |―systemExMib(5)
            |      |―storageExMib(11)
            |          |―raidExMib(4)
            |              |―raidExMibDummy(1)
            |                  |―raidExMibRoot(1)          …2
            |                     SNMP extension MIB
            |
```

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.	1.3.6.1.4.1.116.3.11.4.1.1 (fixed)
sysUpTime {system 3}	An accumulated time from an SNMP agent.	Unit: 100 ms
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.

```
raidExMibRoot(1)
 ├─raidExMibName(1)          SVP product name
 ├─raidExMibVersion(2)       SVP Micro-program version
 ├─raidExMibAgentVersion(3)  Extension MIB internal version
 ├─raidExMibDkcCount(4)      Number of DKC under the control of SVP
 ├─raidExMibRaidListTable(5) List of DKC under the control of SVP
 ├─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 supported by SNMP agents, which list all extension MIBs that can be obtained from storage systems.

```
├- - enterprises(1)
     ├- hitachi(116)
          |
          ├- - systemExMib(5)
                  ├- -storageExMib(11)
                        ├- - raidExMib(4)
                              ├- - raidExMibDummy(1)
                                     ├- - raidExMibRoot(1) →①
```

```
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)
```
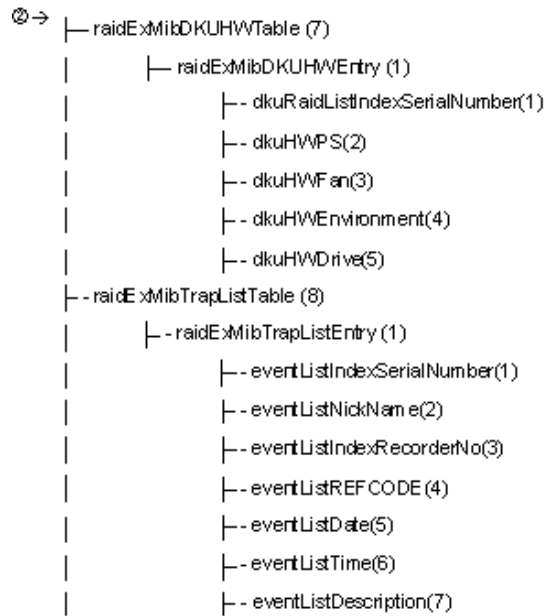
raidExMibName

`raidExMibName` indicates the SVP product name.

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

raidExMibVersion

`raidExMibVersion` indicates the micro-program version.

```
raidExMibVersion      OBJECT-TYPE
SYNTAX                DisplayString
ACCESS                read-only
STATUS                mandatory
DESCRIPTION           "SVP Micro-program 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 under the control of the SVP.

```
raidExMibDkcCount       OBJECT TYPE
SYNTAX                  INTEGER
ACCESS                  read-only
STATUS                  mandatory
DESCRIPTION             "Number of DKC which is registered
                        on the SVP"
::={ raidExMibRoot 4}
```

raidExMibRaidListTable

`raidExMibRaidListTable` indicates the storage system under the control of the SVP.

```
raidExMibRaidListTable   OBJECT TYPE
SYNTAX                   SEQUENCE OF raidExMibRaidListEntry
ACCESS                   not-accessible
STATUS                   mandatory
DESCRIPTION              "List of DKC which is registered
                         on the SVP."
::={ 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).	1 - 999,999	read-only
raidlistMibNickName ::=RaidExMibRaidListEntry(2)	DisplayString	Storage system nickname.	(Max. 18 characters)	read-only
raidlistDKCMainVersion ::=RaidExMibRaidListEntry(3)	DisplayString	Microcode version.	Max. 10 characters	read-only
raidlistDKCProductName ::=RaidExMibRaidListEntry(4)	DisplayString	Storage system product type.	7 characters*	read-only
* VSP5000 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).	1 - 999,999	read-only
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	Status of shared memory.	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.

Name	Type	Description	MIB value	Attribute
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).	1 - 999,999	read-only
dkuHWPS ::=raidExMibDKUHWEntry(2)	INTEGER	Status of power supply.	See Note 1.	read-only
dkuHWFan ::=raidExMibDKUHWEntry(3)	INTEGER	Status of fan.	See Note 1.	read-only
dkuHWEnvironment ::=raidExMibDKUHWEntry(4)	INTEGER	Status of environment monitor. (See Note 2.)	See Note 1.	read-only
dkuHWDrive ::=raidExMibDKUHWEntry(5)	INTEGER	Status of drive. (See Note 3.)	See Note 1.	read-only
Notes:				

Name	Type	Description	MIB value	Attribute
1. 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. 2. The status of environment monitor indicates the status of drives and ENCs in the drive box, and returns a value indicating the highest failure level. 3. Indicates the drive status in the controller chassis.				

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).	1 - 999,999	read-only

Name	Type	Description	MIB value	Attribute
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

Chapter 8: SIM codes

You can use the failure trap reference to identify trap reference codes (SIM codes) to see what section it affects and the alert levels.

Failure trap reference codes

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

For details on alert levels, see the *System Administrator Guide*.

Trap reference code						
SIM 22	SIM 23	SIM 13	Description	Section	Alert level	Host report [1]
14	02	00	Communication error between MP and SVP	SVP failure	MODERATE	Yes
14	20	*xx*	Transmitted data abnormality between MP and GUM	Processor	MODERATE	Yes
18	00	00	AuditLog lost	DKC environment	MODERATE	Yes
21	20	*xx*	Channel port blocking	Processor	MODERATE	Yes
21	30	*xx*	CHB blocking	Environmental error	MODERATE	Yes
21	60	*xx*	HIE blocking	Cache	MODERATE	Yes
21	61	*xx*	ISW blocking	Cache	MODERATE	Yes
21	62	*xx*	X path blocking	Cache	MODERATE	Yes
21	63	*xx*	HIE warning	Cache	MODERATE	Yes

Trap reference code						
SIM 22	**SIM 23**	**SIM 13**	**Description**	**Section**	**Alert level**	**Host report** [1]
21	64	*xx*	X path warning	Cache	MODERATE	Yes
21	80	*xx*	Logical path(s) on the remote copy connections was logically blocked (Due to an error condition)	Processor	MODERATE	Yes[2]
21	81	*xx*	RIO PATH AUTOMATICALLY RECOVERED	Processor	SERVICE	No
21	90	*xx*	AL_PA VALUE CONFLICT	Processor	SERVICE	No
21	93	*xx*	LINK FAILURE	Processor	SERIOUS	Yes
21	94	*xx*	LINK FAILURE2	Processor	SERIOUS	Yes
21	a3	*xx*	HTP/Channel port blocking	Processor	MODERATE	Yes
21	a8	*xx*	SFP wrong type	Processor	MODERATE	No
21	aa	*xx*	SFP TxFault	Processor	MODERATE	No
21	ab	*xx*	SFP warning	Processor	MODERATE	Yes
21	ac	*xx*	SFP alarm	Processor	MODERATE	Yes
21	b*x*	*xx*	HTP hard error	Processor	MODERATE	Yes
21	d0	*xx*	External storage system connection path blocking	Processor	MODERATE	Yes
21	d1	*xx*	External storage system connection path restore	Processor	SERVICE	No
21	d2	*xx*	External storage system response delay	Processor	SERVICE	Yes
21	d4	*xx*	Blocking the Data Migration path	Processor	MODERATE	No
21	d5	*xx*	Data Migration Path Recovery	Processor	SERVICE	No

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
30	70	*xx*	CHK1A THRESHOLD OVER	Processor	SERVICE	No
30	71	*xx*	CHK1B THRESHOLD OVER	Processor	SERVICE	No
30	72	*xx*	CHK3 THRESHOLD OVER	Processor	SERVICE	No
30	73	*xx*	PROCESSOR BLOCKING	Processor	MODERATE	Yes
30	75	*xx*	FM ERROR	Processor	MODERATE	Yes
30	76	*xx*	Incorrect SUM value of FM	Processor	SERVICE	No
30	77	*xx*	PROCESSOR MEMORY TEMPORARY ERROR	Processor	SERVICE	No
30	78	*xx*	BFM error	Processor	SERIOUS	Yes
30	80	*xx*	WCHK1 dump	Processor	MODERATE	No
30	a1	00	DKC Blockade	Processor	ACUTE	Yes
38	8f	00	P/S OFF IMPOSSIBLE	PS(DKC)	MODERATE	No
38	9f	00	P/S OFF IMPOSSIBLE(DEVICE RESERVED)	PS(DKC)	MODERATE	No
39	90	*xx*	Undefined Package is mounted	Processor	MODERATE	No
39	91	*xx*	V-R OR SERIAL NUMBER IS INCONSISTENT	Processor	MODERATE	No
39	93	*xx*	REPLACE FAILED	Processor	MODERATE	No
39	9d	*xx*	Injustice DC voltage control	Processor	MODERATE	Yes
39	9e	*xx*	Injustice CEMODE	Processor	MODERATE	Yes
39	9f	*xx*	Injustice CEDT	Processor	MODERATE	Yes
39	b0	*xx*	SMA SLAVE ERROR	Processor	SERVICE	No

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
3a	0*x*	*xx*	LDEV Blockade (Effect of microcode error)	Processor	MODERATE	Yes
3c	95	00	CHB/DKB Type disagreement	Processor	MODERATE	No
3c	96	00	No CHB mounted	CHB/DKB error	MODERATE	No
3c	97	*xx*	ISCF microcode exchange warning	CHB/DKB error	MODERATE	Yes
3c	98	00	ACLF type mismatch detected	ACLF error	MODERATE	No
41	00	*xx*	Format complete	Drive	SERVICE	No
41	01	00	Quick Format finish	Drive	SERVICE	No
41	02	00	Parity consistency check completed	Environment	SERVICE	No
41	02	01	Parity consistency check suspended	Environment	SERVICE	No
41	03	00	Parity consistency check abnormality detection	Environment	MODERATE	No
43	4*x*	*xx*	DRIVE MEDIA ERROR[6]	Drive	SERVICE	No
43	5*x*	*xx*	Drive media error	Drive	SERVICE	No
43	a*x*	*xx*	Drive blockade (media)(with redundancy)	Drive	SERIOUS	Yes
43	b*x*	*xx*	Drive blockade (media)(with redundancy)[6]	Drive	SERIOUS	Yes
43	c*x*	*xx*	Drive blockade (media)(without redundancy)[6]	Drive	SERIOUS	Yes
43	d*x*	*xx*	Drive blockade (media)(without redundancy)	Drive	SERIOUS	Yes
46	8*x*	*xx*	Collection Copy/Copyback disabled(drive replace)	Drive	MODERATE	No

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
46	9x	xx	Collection Copy/Copyback disabled(drive replace)	Drive	MODERA TE	No
46	ax	xx	Drive Copy/Correction Copy delay	Drive	MODERA TE	Yes
46	bx	xx	Drive Copy/Correction Copy delay	Drive	MODERA TE	Yes
46	cx	xx	Drive Copy/Correction Copy copy skip	Drive	MODERA TE	Yes
46	dx	xx	Drive Copy/Correction Copy copy skip	Drive	MODERA TE	Yes
47	dx	xx	SIMF/SI Copy abnormal end	Failure with paired volumes	MODERA TE	Yes
47	e5	00	All FlashCopy(R) Option abnormal end by SM volatile	Failure with paired volumes	MODERA TE	Yes
47	e7	00	Forcible suspend by SM volatile (SIMF/SI)	Failure with paired volumes	MODERA TE	Yes
47	ec	00	Thin Image ABNORMAL END BY SM VOLATILE	Failure with paired volumes	MODERA TE	Yes
47	fx	xx	Volume Migration Abnormal End	Volume Migration	MODERA TE	Yes[3]
49	10	00	CACHE WRITE PENDING RATIO IS OVER 65%	Cache	SERVICE	No
49	3x	xx	Cache Write Pending warning threshold exceeded	Cache	MODERA TE	No
4a	80	xx	Expander Micro Exchange failed	Processor	MODERA TE	No
4b	2x	xx	Compatible FlashCopy(R) ABNORMAL END	Failure with paired volumes	MODERA TE	Yes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
4b	3*x*	*xx*	Thin Image ABNORMAL END	Failure with paired volumes	MODERATE	Yes
4b	4*x*	*xx*	FlashCopy(R) Hierarchical memory access error	Failure with paired volumes	MODERATE	Yes
4b	6*x*	*xx*	Correction copy start	Failure with paired volumes	SERVICE	Yes
4b	7*x*	*xx*	Correction copy start	Failure with paired volumes	SERVICE	Yes
4b	8*x*	*xx*	Correction copy normal end	Failure with paired volumes	SERVICE	Yes
4b	9*x*	*xx*	Correction copy normal end	Failure with paired volumes	SERVICE	Yes
4b	a*x*	*xx*	Correction copy abnormal end	Failure with paired volumes	SERIOUS	Yes
4b	b*x*	*xx*	Correction copy abnormal end	Failure with paired volumes	SERIOUS	Yes
4b	c*x*	*xx*	Correction copy discontinued	Failure with paired volumes	SERVICE	No
4b	d*x*	*xx*	Correction copy discontinued	Failure with paired volumes	SERVICE	No
4b	e*x*	*xx*	Correction copy warning end (With blockade LDEV or some error)	Failure with paired volumes	SERVICE	Yes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
4b	f*x*	*xx*	Correction copy warning end (With blockade LDEV or some error)	Failure with paired volumes	SERVICE	Yes
4c	4*x*	*xx*	Flash module drive initialization failed	Drive	MODERATE	Yes
4c	5*x*	*xx*	Flash module drive initialization failed	Drive	MODERATE	Yes
4c	6*x*	*xx*	Dynamic sparing start (Drive copy)	Drive	SERVICE	Yes
4c	7*x*	*xx*	Dynamic sparing start (Drive copy)	Drive	SERVICE	Yes
4c	8*x*	*xx*	Dynamic sparing normal end (Drive copy)	Drive	SERVICE	Yes
4c	9*x*	*xx*	Dynamic sparing normal end (Drive copy)	Drive	SERVICE	Yes
4c	a*x*	*xx*	Dynamic sparing abnormal end (Drive copy)	Drive	MODERATE	Yes
4c	b*x*	*xx*	Dynamic sparing abnormal end (Drive copy)	Drive	MODERATE	Yes
4c	c*x*	*xx*	Dynamic sparing discontinued (Drive copy)	Drive	SERVICE	No
4c	d*x*	*xx*	Dynamic sparing discontinued (Drive copy)	Drive	SERVICE	No
4c	e*x*	*xx*	Dynamic sparing warning end (With blockade LDEV or some error) (Drive copy)	Drive	SERVICE	Yes
4c	f*x*	*xx*	Dynamic sparing warning end (With blockade LDEV or some error) (Drive copy)	Drive	SERVICE	Yes
4d	1*x*	*xx*	Differential area blocking	Drive	SERIOUS	Yes
4d	6*x*	*xx*	PDEV Erase Start	Drive	SERVICE	No
4d	7*x*	*xx*	PDEV Erase Start	Drive	SERVICE	No

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
4d	8x	xx	PDEV Erase Normal End	Drive	SERVICE	No
4d	9x	xx	PDEV Erase Normal End	Drive	SERVICE	No
4d	ax	xx	PDEV Erase Abnormal End	Drive	SERVICE	No
4d	bx	xx	PDEV Erase Abnormal End	Drive	SERVICE	No
4e	0x	xx	Drive blockade due to Media Sanitization start	Drive	SERVICE	Yes
4e	1x	xx	Drive blockade due to Media Sanitization start	Drive	SERVICE	Yes
4e	2x	xx	Media Sanitization start	Drive	SERVICE	Yes
4e	3x	xx	Media Sanitization start	Drive	SERVICE	Yes
4e	4x	xx	Media Sanitization normal end	Drive	SERVICE	Yes
4e	5x	xx	Media Sanitization normal end	Drive	SERVICE	Yes
4e	6x	xx	Media Sanitization abnormal end	Drive	MODERATE	Yes
4e	7x	xx	Media Sanitization abnormal end	Drive	MODERATE	Yes
4e	8x	xx	Media Sanitization warning end	Drive	MODERATE	Yes
4e	9x	xx	Media Sanitization warning end	Drive	MODERATE	Yes
50	0x	xx	Drive temporary error	Drive	SERVICE	No
50	1x	xx	DRIVE TEMPORARY ERROR	Drive	SERVICE	No
50	2x	xx	DRIVE MEDIA ERROR[6]	Drive	SERVICE	No
50	3x	xx	Drive media error	Drive	SERVICE	No
50	ax	xx	Flash drive End of life	Drive	SERVICE	Yes
50	bx	xx	Flash drive End of life[6]	Drive	SERVICE	Yes
50	cx	xx	Flash module drive End of life[6]	Drive	SERVICE	Yes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
50	d*x*	*xx*	Flash module drive battery warning[6]	Drive	SERVICE	No
60	2*x*	*xx*	Pool blocking[7]	Thin Image pool	MODERATE	Yes
60	30	00	SM Space Warning	SM	MODERATE	Yes[4]
60	4*x*	*xx*	Exceeded Threshold of pool use rate	Thin Image pool	MODERATE	Yes
60	5*x*	*xx*	Actual pool use rate reaches upper limit	Thin Image pool	MODERATE	Yes
60	6*x*	*xx*	Exceeded Fixed outage Threshold of pool use rate	Thin Image pool	MODERATE	Yes
61	00	*xx*	BACKUP/RESTORE SM INFORMATION FAILED	SM	MODERATE	No
62	3*x*	*xx*	The DP POOL error is detected (XXX : Pool ID)	Dynamic Provisioning pool	MODERATE	Yes
62	40	00	SM(DP/TI) AREA DEPLETION	Dynamic Provisioning pool	MODERATE	Yes
62	7*x*	*xx*	The DP POOL LDEV blockade	Dynamic Provisioning pool	SERIOUS	Yes
62	80	00	DP Protect attribute setting of DRU	Dynamic Provisioning pool	SERIOUS	Yes
62	9*x*	*xx*	Exceeded Warning Threshold of DP pool use rate	Dynamic Provisioning pool	MODERATE	Yes
62	a*x*	*xx*	DP pool use rate reaches upper limit	Dynamic Provisioning pool	MODERATE	Yes

Trap reference code						
SIM 22	SIM 23	SIM 13	Description	Section	Alert level	Host report [1]
62	b0	00	Threshold of DP pool use rate remains exceeded	Dynamic Provisioning pool	MODERATE	Yes
62	c*x*	*xx*	Exceeded Depletion Threshold of DP pool use rate	Dynamic Provisioning pool	MODERATE	Yes
62	d*x*	*xx*	Exceeded Fixed outage Threshold of DPpool use rate	Dynamic Provisioning pool	MODERATE	Yes
62	e*x*	*xx*	Exceeded DP pool depletion threshold for TI pairs	Dynamic Provisioning pool	MODERATE	Yes
63	1*x*	*xx*	Auto pool expansion failed due to system error	Dynamic Provisioning pool	MODERATE	Yes
63	2*x*	*xx*	Auto pool expansion failed due to pool error	Dynamic Provisioning pool	MODERATE	Yes
63	3*x*	*xx*	Failed to create, expand, or delete pools	Pool error	MODERATE	Yes
63	4*x*	*xx*	Auto pool expansion failed due to no more LDEV IDs	Dynamic Provisioning pool	MODERATE	Yes
64	1*x*	*xx*	Tier relocation is not completed	Dynamic Tiering pool	SERVICE	Yes
66	01	00	No free encryption key	Encryption key	MODERATE	Yes
66	02	00	Remaining free encryption key warning	Encryption key	SERVICE	Yes
66	10	*xx*	Acquisition of encryption key from KMS failed	Encryption key	MODERATE	Yes
66	20	*xx*	Encryption key setting abnormality	Processor	SERIOUS	Yes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
67	00	00	Warning for depletion of cache management devices	Thin Image	MODERATE	Yes
68	00	xx	Dedupe and compression abnormality detect	dedupe and compression failure	MODERATE	Yes
68	1x	xx	dedupe system volume deletion abnormal end	dedupe and compression failure	MODERATE	Yes
68	20	00	dedupe system volume deletion suspended	dedupe and compression failure	MODERATE	Yes
68	3x	xx	Log structured area depletion alert	dedupe and compression	MODERATE	Yes
68	4x	xx	Log structured area depletion is solved	dedupe and compression	SERVICE	Yes
68	9x	xx	dedupe system volume change comp_acl abnormal end	dedupe and compression failure	MODERATE	Yes
68	a0	xx	performance degradation alert	dedupe and compression	MODERATE	Yes
68	bx	xx	dedupe and compression meta data access failure	dedupe and compression failure	MODERATE	Yes
70	xx	00	Logical inconsistency	SVP failure	MODERATE	No
71	xx	00	Heap error	SVP failure	MODERATE	No
72	xx	00	File error	SVP failure	MODERATE	No
73	xx	xx	LAN error	SVP failure	MODERATE	No

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
74	*xx*	*xx*	SSVP error	SVP failure	MODERATE	Yes
75	*xx*	00	Windows error	SVP failure	MODERATE	No
76	00	00	CUDG3 detected error	SVP failure	MODERATE	No
7b	00	03	ISDN Router failure	SVP failure	MODERATE	Yes
7c	00	00	SVP reboot stop (FD Inserted)	SVP failure	MODERATE	No
7c	02	00	Audit Log failure of Host instruction configuration change	SVP failure	MODERATE	No
7c	03	00	Audit Log FTP Transfer failed	SVP failure	MODERATE	Yes
7c	04	00	Dump Tool failed	SVP failure	SERVICE	Yes
7c	05	00	Invalid SIM data detection	SVP failure	SERVICE	No
7c	08	00	Dump collection starts	SVP failure	SERVICE	No
7c	09	00	Dump collection ends normally	SVP failure	SERVICE	No
7c	0a	00	Dump collection ends abnormally	SVP failure	SERVICE	No
7c	0b	00	Cancellation of the dump collection completed	SVP failure	SERVICE	No
7d	00	*xx*	GUM error	GUM detection error	MODERATE	No
7d	01	*xx*	LAN error(Internal Network)	GUM detection error	MODERATE	Yes
7d	02	*xx*	LAN error(CTL1-CTL2)	GUM detection error	MODERATE	Yes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
7d	06	*xx*	MP error	GUM detection error	MODERATE	Yes
7d	07	*xx*	GUM security error detected	GUM detection error	MODERATE	Yes
7d	08	*xx*	Failed to recover GUM configuration information	GUM detection error	MODERATE	Yes
7d	09	0*x*	DKC warning	GUM detection error	SERIOUS	Yes
7d	0a	*xx*	GUM version warning	GUM detection error	MODERATE	Yes
7e	12	*xx*	MP usage threshold exceeded	Monitor	MODERATE	Yes
7e	20	*xx*	Loss Of Signal Count(Fibre) Excess	Monitor	MODERATE	No
7e	21	*xx*	Bad Received Character Count(Fibre) Excess	Monitor	MODERATE	No
7e	22	*xx*	Loss Of Synchronization Count(Fibre) Excess	Monitor	MODERATE	No
7e	23	*xx*	Link Failure Count(Fibre) Excess	Monitor	MODERATE	No
7e	24	*xx*	Received EOFa Count(Fibre) Excess	Monitor	MODERATE	No
7e	25	*xx*	Discarded Frame Count(Fibre) Excess	Monitor	MODERATE	No
7e	26	*xx*	Bad CRC Count(Fibre) Excess	Monitor	MODERATE	No
7e	27	*xx*	Protocol Error Count(Fibre) Excess	Monitor	MODERATE	No

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
7e	28	*xx*	Expired Frame Count (Fibre) Excess	Monitor	MODERATE	No
7e	29	*xx*	HTP/FNP Multiplicity Excess	Monitor	MODERATE	No
7e	2a	*xx*	FEC Un-correctable Count(Fibre) threshold exceeded	Monitor	MODERATE	No
7e	2c	*xx*	HTP/FNP read data transfer threshold exceeded	Monitor	MODERATE	No
7e	2d	*xx*	HTP/FNP write data transfer threshold exceeded	Monitor	MODERATE	No
7e	2e	*xx*	HTP/FNP usage threshold exceeded	Monitor	MODERATE	No
7e	30	00	Read Hit Ratio Excess	Monitor	MODERATE	No
7e	50	*xx*	MAC CRC Error Count(iSCSI) threshold exceeded	Monitor	MODERATE	No
7e	51	*xx*	IP Error Packet Count(iSCSI) threshold exceeded	Monitor	MODERATE	No
7e	52	*xx*	IPv6 Error Packet Count(iSCSI) threshold exceeded	Monitor	MODERATE	No
7e	53	*xx*	TCP Retransmit Timer Expired Count(iSCSI) exceeded	Monitor	MODERATE	No
7e	54	*xx*	iSCSI Header Digest Error Count(iSCSI) exceeded	Monitor	MODERATE	No
7e	55	*xx*	iSCSI Data Digest Error Count(iSCSI) exceeded	Monitor	MODERATE	No
7e	a*x*	*xx*	Cache Use threshold exceeded	Monitor	MODERATE	No
7e	b*x*	*xx*	Cache Write Pending threshold exceeded	Monitor	MODERATE	No
7e	c*x*	*xx*	Cache MCU Side File Use threshold exceeded	Monitor	MODERATE	No

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
7f	f1	00	TCMF/TC	SVP failure	SERVICE	No
7f	f1	02	SIMF/SI	SVP failure	SERVICE	No
7f	f1	03	URMF/UR	SVP failure	SERVICE	No
7f	f1	04	TI	SVP failure	SERVICE	No
7f	f1	05	FlashCopy(R)	SVP failure	SERVICE	No
7f	f1	06	Volume Migration	SVP failure	SERVICE	No
7f	f2	*xx*	STANDBY SVP FAIL	SVP failure	MODERATE	No
7f	f3	*xx*	SVP FAIL OVER	SVP failure	MODERATE	No
7f	f7	*xx*	The term of validity is over	License key	MODERATE	Yes
7f	f8	*xx*	The capacity of validity is over	License key	MODERATE	Yes
7f	f9	*xx*	The PP is invalid by assumption PP invalidity	License key	MODERATE	Yes
7f	fa	0*x*	Synchronization time failure	SVP failure	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	No
ac	61	00	DKC was released from power error mode	PS(DKC)	SERVICE	No
ac	62	00	When DKC was set to power error mode, Urgent Destaging start succeeded	PS(DKC)	SERVICE	No
ac	63	00	When DKC was set to power error mode, Urgent Destaging start failed.	PS(DKC)	MODERATE	No

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
ac	91	00	Open host reservation	DKC environment	MODERATE	Yes
af	00	xx	Injustice JP Warning	Environmental error	MODERATE	Yes
af	10	xx	MP Temperature abnormality warning	Environmental error	MODERATE	Yes
af	11	xx	External temperature warning	Environmental error	MODERATE	Yes
af	12	xx	External temperature alarm	Environmental error	MODERATE	Yes
af	13	xx	Thermal monitor warning	Environmental error	MODERATE	Yes
af	20	xx	DKCPS warning	Environmental error	MODERATE	Yes
af	21	xx	DKCPS input voltage abnormality	Environmental error	MODERATE	Yes
af	30	xx	Environmental microcontroller warning	Environmental error	MODERATE	Yes
af	31	xx	Device movement mode warning	Environmental error	MODERATE	Yes
af	32	xx	Environmental Firmware Update warning	Environmental error	MODERATE	Yes
af	33	xx	Voltage change setting warning	Environmental error	MODERATE	Yes
af	40	xx	BKM/BKMF warning	Environmental error	MODERATE	Yes
af	41	xx	Battery replacement should be scheduled	Environmental error	MODERATE	Yes
af	4d	xx	Panel switch warning	Environmental error	MODERATE	Yes
af	4e	xx	Invalid PS ON warning	Environmental error	MODERATE	Yes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
af	51	*xx*	DBPS-1 warning	PS(DKU)	MODERATE	Yes
af	52	*xx*	DBPS-2 warning	PS(DKU)	MODERATE	Yes
af	61	*xx*	DBPS-1 input voltage abnormality	PS(DKU)	MODERATE	Yes
af	62	*xx*	DBPS-2 input voltage abnormality	PS(DKU)	MODERATE	Yes
af	70	00	DB External temperature warning	Environmental error	MODERATE	Yes
af	71	00	DB External temperature Alarm	Environmental error	MODERATE	Yes
af	81	*xx*	ENC-1 warning	Environmental error	MODERATE	Yes
af	82	*xx*	ENC-2 warning	Environmental error	MODERATE	Yes
af	b0	*xx*	HSNBX ambient temperature warning	Environmental error	MODERATE	Yes
af	b1	*xx*	ISW PS warning	Environmental error	MODERATE	Yes
af	b2	*xx*	ISW FAN warning	Environmental error	MODERATE	Yes
af	b3	*xx*	ISW PS input voltage abnormality	Environmental error	MODERATE	Yes
af	b4	*xx*	ISW warning	Environmental error	MODERATE	Yes
af	b5	*xx*	HSNBX thermal monitor warning	Environmental error	MODERATE	Yes
af	b6	*xx*	HSNBX PANEL JP setting abnormality	Environmental error	MODERATE	Yes
af	b7	*xx*	HSNBX PANEL JP setting warning	Environmental error	MODERATE	Yes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
af	b8	*xx*	HSNBX PSONOFF I/F inconsistent	Environmental error	MODERATE	Yes
af	f0	*xx*	SSW data disagreement	DKC environment	MODERATE	No
af	f1	*xx*	GUM warning	Environmental error	MODERATE	Yes
af	f2	*xx*	CFM error	Processor	MODERATE	Yes
af	f3	*xx*	FAN warning	Environmental error	MODERATE	Yes
bf	85	a3	JP remains	Environment	MODERATE	Yes
bf	86	a3	JP remains	Environment	MODERATE	Yes
bf	b*x*	*xx*	HSNPANEL error	Environmental error	MODERATE	No
bf	e3	a2	Duplex SVP Setup fail	SVP failure	MODERATE	Yes
bf	e4	00	SVP FAN0 error	SVP failure	MODERATE	No
bf	e4	04	SVP disk error (SMART)	Environmental error	MODERATE	No
bf	e4	07	USB interface error	Environmental error	MODERATE	No
cf	10	*xx*	SAS CTL blocking	Processor	MODERATE	Yes
cf	11	*xx*	SAS Port (WideLink) is partially blocked	Processor	SERVICE	No
cf	12	*xx*	SAS PORT blocked	Processor	MODERATE	Yes
cf	13	*xx*	Abnormal error detection	Processor	SERIOUS	Yes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
cf	20	*xx*	PSW blockade	Processor	MODERATE	Yes
cf	22	*xx*	NVMe port blockade	Processor	MODERATE	Yes
cf	88	*xx*	CTL blocking	Processor	MODERATE	Yes
d0	0*x*	*xx*	TCMF/TC started the initial copy or out of sync for this volume	Failure with paired volumes	SERVICE	Yes
d0	1*x*	*xx*	TCMF/TC completed the initial copy for this volume	Failure with paired volumes	SERVICE	Yes
d0	2*x*	*xx*	TCMF/TC for this volume was deleted(Operation from an SVP/Web Console or a host processor)	Failure with paired volumes	SERVICE	Yes
d0	6*x*	*xx*	TCMF completed the Create pair (No copy suspend)	Pair volume status error	SERVICE	Yes
d1	0*x*	*xx*	Remote Copy pair status change (MCU Command) (From Simplex to Duplex Pending)	Failure with paired volumes	SERVICE	Yes
d1	1*x*	*xx*	Remote Copy pair status change (MCU Command) (From Simplex to Duplex)	Failure with paired volumes	SERVICE	Yes
d1	2*x*	*xx*	Remote Copy pair status change (MCU Command) (From Duplex Pending to Duplex)	Failure with paired volumes	SERVICE	Yes
d1	3*x*	*xx*	Remote Copy pair status change (MCU Command) (From Duplex Pending to Suspend)	Failure with paired volumes	SERVICE	Yes
d1	4*x*	*xx*	Remote Copy pair status change (MCU Command) (From Duplex to Suspend)	Failure with paired volumes	SERVICE	Yes

Trap reference code						
SIM 22	**SIM 23**	**SIM 13**	**Description**	**Section**	**Alert level**	**Host report** [1]
d1	5x	xx	Remote Copy pair status change (MCU Command) (From Duplex to Simplex)	Failure with paired volumes	SERVICE	Yes
d1	6x	xx	Remote Copy pair status change (MCU Command) (From Duplex Pending to Simplex)	Failure with paired volumes	SERVICE	Yes
d1	7x	xx	Remote Copy pair status change (MCU Command) (From Suspend to Simplex)	Failure with paired volumes	SERVICE	Yes
d1	8x	xx	Remote Copy pair status change (MCU Command) (From Suspend to Duplex Pending)	Failure with paired volumes	SERVICE	Yes
d1	9x	xx	Remote Copy pair status change (MCU Command) (From Duplex Pending to Suspend(continue))	Failure with paired volumes	SERVICE	Yes
d1	ax	xx	Remote Copy pair status change (MCU Command) (From Duplex Pending to Suspend(complete))	Failure with paired volumes	SERVICE	Yes
d1	bx	xx	Remote Copy pair status change (MCU Command) (From Suspend (continue) to Suspend)	Failure with paired volumes	SERVICE	Yes
d4	0x	xx	TCMF/TC for this volume was suspended (Due to an unrecoverable failure on the remote copy connections)	Failure with paired volumes	SERIOUS	Yes
d4	1x	xx	TCMF/TC for this volume was suspended (Due to an unrecoverable failure on the P-VOL or the remote copy connections)	Failure with paired volumes	SERIOUS	Yes
d4	2x	xx	TCMF/TC for this volume was suspended (Due to an unrecoverable failure on the S-VOL)	Failure with paired volumes	SERIOUS	Yes

Trap reference code						
SIM 22	SIM 23	SIM 13	Description	Section	Alert level	Host report [1]
d4	3x	xx	TCMF for this volume was suspended (Caused by DFW to the S-VOL was prohibited)	Pair volume status error	SERIOUS	Yes
d4	4x	xx	TCMF/TC for this volume was suspended (Due to an internal error condition detected by the RCU)	Failure with paired volumes	SERIOUS	Yes
d4	5x	xx	TCMF/TC for this volume was suspended (Caused by Delete pair operation was issued to the S-VOL)	Failure with paired volumes	SERIOUS	Yes
d4	6x	xx	The S-VOL has suspended. (Due to an unrecoverable failure on the remote copy connections)	Failure with paired volumes	SERIOUS	Yes
d4	7x	xx	The S-VOL has suspended (Due to an unrecoverable failure on the S-VOL)	Failure with paired volumes	SERIOUS	Yes
d4	fx	xx	Status of the P-VOL was not consistent with the S-VOL	Failure with paired volumes	SERIOUS	Yes
d5	7x	xx	Command device operation execution of command device in state of ONLINE	Drive	SERVICE	No
d8	0x	xx	A volume to be used by the URMF/UR was defined	Failure with paired volumes	SERVICE	Yes[5]
d8	1x	xx	The volume being used by the URMF/UR began a copying	Failure with paired volumes	SERVICE	Yes[5]
d8	2x	xx	The volume being used by the URMF/UR completed a copying	Failure with paired volumes	SERVICE	Yes[5]
d8	3x	xx	The volume being used by the URMF/UR received a request for suspension	Failure with paired volumes	SERVICE	Yes[5]

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
d8	4x	xx	The volume being used by the URMF/UR completed a suspension transaction	Failure with paired volumes	SERVICE	Yes[5]
d8	5x	xx	The volume being used by the URMF/UR received a request for deletion	Failure with paired volumes	SERVICE	Yes[5]
d8	6x	xx	The volume being used by the URMF/UR completed the deletion	Failure with paired volumes	SERVICE	Yes[5]
d8	7x	xx	The volume being used by the URMF/UR was defined (placed in the PSUS status immediately)	Failure with paired volumes	SERVICE	Yes[5]
d8	8x	xx	A Delta volume to be used by the URMF/UR was defined	Failure with paired volumes	SERVICE	Yes[5]
d8	9x	xx	A Delta volume to be used by the URMF/UR was redefined	Failure with paired volumes	SERVICE	Yes[5]
d9	0x	xx	A change to an S-VOL was received from the MCU (From Simplex to Duplex Pending)	Failure with paired volumes	SERVICE	Yes[5]
d9	1x	xx	A change to an S-VOL was received from the MCU (From Simplex to Duplex)	Failure with paired volumes	SERVICE	Yes[5]
d9	2x	xx	A change to an S-VOL was received from the MCU (From Duplex Pending to Duplex)	Failure with paired volumes	SERVICE	Yes[5]
d9	3x	xx	A change to an S-VOL was received from the MCU (From Duplex Pending to Suspend)	Failure with paired volumes	SERVICE	Yes[5]
d9	4x	xx	A change to an S-VOL was received from the MCU (From Duplex to Suspend)	Failure with paired volumes	SERVICE	Yes[5]

Trap reference code						
SIM 22	SIM 23	SIM 13	Description	Section	Alert level	Host report [1]
d9	5x	xx	A change to an S-VOL was received from the MCU (From Duplex to Simplex)	Failure with paired volumes	SERVICE	Yes[5]
d9	6x	xx	A change to an S-VOL was received from the MCU (From Duplex Pending to Simplex)	Failure with paired volumes	SERVICE	Yes[5]
d9	7x	xx	A change to an S-VOL was received from the MCU (From Suspend to Simplex)	Failure with paired volumes	SERVICE	Yes[5]
d9	8x	xx	A change to an S-VOL was received from the MCU (From Suspend to Duplex Pending)	Failure with paired volumes	SERVICE	Yes[5]
d9	9x	xx	A change to an S-VOL was received from the MCU (HOLD -> PAIR)	Failure with paired volumes	SERVICE	Yes[5]
d9	ax	xx	A change to an S-VOL was received from the MCU (HOLD -> COPY)	Failure with paired volumes	SERVICE	Yes[5]
d9	bx	xx	A change to an S-VOL was received from the MCU (HOLD -> SMPL)	Failure with paired volumes	SERVICE	Yes[5]
d9	cx	xx	A change to an S-VOL was received from the MCU (From Simplex to Suspend)	Failure with paired volumes	SERVICE	Yes[5]
d9	dx	xx	A change to an S-VOL was received from the MCU (SMPL -> HOLD)	Failure with paired volumes	SERVICE	Yes[5]
d9	ex	xx	A change to an S-VOL was received from the MCU (PSUx(Suspend) -> HOLD)	Failure with paired volumes	SERVICE	Yes[5]
d9	fx	xx	A change to an S-VOL was received from the MCU (From Duplex to Duplex Pending)	Failure with paired volumes	SERVICE	Yes[5]

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
da	0*x*	*xx*	A change to an S-VOL was received from the RCU (A request for suspension was received.)	Failure with paired volumes	SERVICE	No
da	1*x*	*xx*	A change to an S-VOL was received from the RCU (A suspension transaction was completed.)	Failure with paired volumes	SERVICE	No
da	2*x*	*xx*	A change to an S-VOL was received from the RCU (An instruction to delete a pair was received in the Suspend status.)	Failure with paired volumes	SERVICE	No
da	3*x*	*xx*	A change to an S-VOL was received from the RCU (An instruction to delete a pair was received in the Duplex Pending status.)	Failure with paired volumes	SERVICE	No
da	4*x*	*xx*	A change to an S-VOL was received from the RCU (An instruction to delete a pair was received in the Duplex status.)	Failure with paired volumes	SERVICE	No
da	5*x*	*xx*	A change to an S-VOL was received from the RCU (A pair deletion was completed.)	Failure with paired volumes	SERVICE	No
da	6*x*	*xx*	A change to an S-VOL was received from the RCU (An instruction to delete a pair was received in the Hold status.)	Failure with paired volumes	SERVICE	No
db	0*x*	*xx*	Drive port temporary error	Drive error	SERVICE	No
db	1*x*	*xx*	Drive port temporary error	Drive error	SERVICE	No
db	2*x*	*xx*	Drive port temporary error	Drive error	SERVICE	No
db	3*x*	*xx*	Drive port temporary error	Drive error	SERVICE	No
db	4*x*	*xx*	Drive port blockade	Drive error	MODERATE	Yes

Trap reference code						
SIM 22	**SIM 23**	**SIM 13**	**Description**	**Section**	**Alert level**	**Host report** [1]
db	5*x*	*xx*	Drive port blockade	Drive error	MODERA TE	Yes
db	6*x*	*xx*	Drive port blockade	Drive error	MODERA TE	Yes
db	7*x*	*xx*	Drive port blockade	Drive error	MODERA TE	Yes
db	8*x*	*xx*	LDEV blockade (Effect of Drive port blockade)	Drive error	SERIOUS	Yes
db	9*x*	*xx*	LDEV blockade (Effect of Drive port blockade)	Drive error	SERIOUS	Yes
db	a*x*	*xx*	LDEV blockade (Effect of Drive port blockade)	Drive error	SERIOUS	Yes
db	b*x*	*xx*	LDEV blockade (Effect of Drive port blockade)	Drive error	SERIOUS	Yes
db	c*x*	*xx*	Drive Link Rate Abnormality	Drive error	SERVICE	Yes
db	d*x*	*xx*	Drive Link Rate Abnormality	Drive error	SERVICE	Yes
db	e*x*	*xx*	Drive Link Rate Abnormality	Drive error	SERVICE	Yes
db	f*x*	*xx*	Drive Link Rate Abnormality	Drive error	SERVICE	Yes
dc	0*x*	*xx*	PAIR SUSPEND(RIO PATH CLOSE)	Failure with paired volumes	SERIOUS	Yes[5]
dc	1*x*	*xx*	PAIR SUSPEND(MVOL ERROR)	Failure with paired volumes	SERIOUS	Yes[5]
dc	2*x*	*xx*	PAIR SUSPEND(RVOL ERROR)	Failure with paired volumes	SERIOUS	Yes[5]
dc	4*x*	*xx*	PAIR SUSPEND(SUSPEND REPORT)	Failure with paired volumes	SERIOUS	Yes[5]
dc	5*x*	*xx*	PAIR SUSPEND(SIMPLEX REPORT)	Failure with paired volumes	SERIOUS	Yes[5]

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
dc	6x	xx	PAIR SUSPEND(COMMUNICATION ERROR AT RCU)	Failure with paired volumes	SERIOUS	Yes[5]
dc	7x	xx	PAIR SUSPEND(ERROR DETECTED AT RCU)	Failure with paired volumes	SERIOUS	Yes[5]
dc	8x	xx	A volume being used by an S-VOL was suspended (PS OFF on the MCU side was detected)	Failure with paired volumes	SERVICE	No
dc	9x	xx	ERASE FAIL	Failure with paired volumes	SERIOUS	Yes[5]
dc	ax	xx	Pair suspend (Spread by error of another Affiliate)	Failure with paired volumes	SERIOUS	Yes[5]
dc	e0	xx	URMF/UR M-JNL Meta overflow warning	Failure with paired volumes	MODERATE	No
dc	e1	xx	URMF/UR M-JNL Data overflow warning	Failure with paired volumes	MODERATE	No
dc	e2	xx	URMF/UR R-JNL Meta overflow warning	Failure with paired volumes	MODERATE	No
dc	e3	xx	URMF/UR R-JNL Data overflow warning	Failure with paired volumes	MODERATE	No
dc	f0	xx	The URMF/UR Read JNL was interrupted for one minute (A failure on the MCU side was detected)	Failure with paired volumes	MODERATE	No
dc	f1	xx	The URMF/UR Read JNL was interrupted for five minutes (A failure on the MCU side was detected)	Failure with paired volumes	SERIOUS	No

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
dc	f2	*xx*	The URMF/UR Read JNL was interrupted for one minute (A failure on the RCU side was detected)	Failure with paired volumes	MODERATE	No
dc	f3	*xx*	The URMF/UR Read JNL was interrupted for five minutes (A failure on the RCU side was detected)	Failure with paired volumes	SERIOUS	No
dc	f4	*xx*	URMFxURMF/URxUR M-JNL Meta full Warning	Failure with paired volumes	MODERATE	No
dc	f5	*xx*	URMFxURMF/URxUR M-JNL Data full Warning	Failure with paired volumes	MODERATE	No
dc	f6	*xx*	Unassigned remote command device warning in 3DC	Failure with paired volumes	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	e*x*	*xx*	Response late Drive	Drive	SERVICE	No
df	f*x*	*xx*	Response late Drive[6]	Drive	SERVICE	No

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
eb	0x	xx	Drive blockade (drive)(with redundancy)	Drive	SERIOUS	Yes
eb	1x	xx	Drive blockade (drive)(with redundancy)	Drive	SERIOUS	Yes
eb	2x	xx	Drive blockade (drive)(without redundancy)	Drive	SERIOUS	Yes
eb	3x	xx	Drive blockade (drive)(without redundancy)	Drive	SERIOUS	Yes
eb	4x	xx	Drive blockade (Effect of Dynamic sparing normal end)	Drive	SERVICE	Yes
eb	5x	xx	Drive blockade (Effect of Dynamic sparing normal end)	Drive	SERVICE	Yes
eb	6x	xx	Correction access occurred	Drive	SERIOUS	Yes
eb	7x	xx	Correction access occurred	Drive	SERIOUS	Yes
eb	8x	xx	Reboot stopped due to much write pending data	Drive	SERVICE	No
eb	9x	xx	Reboot stopped due to much write pending data	Drive	SERVICE	No
ee	00	00	Volume I/O upper limit reached	QoS alert	SERVICE	Yes
ee	10	00	Volume I/O lower limit not reached	QoS alert	SERVICE	Yes
ee	20	00	Volume I/O response delay	QoS alert	SERVICE	Yes
ee	30	00	QoS group I/O upper limit reached	QoS alert	SERVICE	Yes
ee	50	00	QoS group I/O response delay	QoS alert	SERVICE	Yes
ef	4x	xx	PINNED SLOT	Drive	MODERATE	No
ef	5x	xx	Abnormal end of Write processing in External storage system	Drive	MODERATE	No

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
ef	8x	xx	LDEV blockade (Effect of drive blockade)	Drive	SERIOUS	Yes
ef	9x	xx	LDEV blockade (Effect of drive blockade)[6]	Drive	SERIOUS	Yes
ef	ax	xx	DRIVE TEMPORARY ERROR[6]	Drive	SERVICE	No
ef	bx	xx	Drive temporary error	Drive	SERVICE	No
ef	d0	00	External storage system connection device blockade	Drive	SERIOUS	Yes
ef	d4	00	Blocking the Data Migration source device	Drive	MODERATE	No
ef	fd	xx	Expander failure	Environmental error	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	0x	End of Cache Write Through	Cache	SERVICE	No
fe	02	0x	Start of Cache Write Through	Cache	MODERATE	Yes
fe	03	0x	Cache SSD mounting capacity shortage	Cache	SERIOUS	No
fe	04	xx	No CHB mounted	Cache	SERIOUS	Yes
ff	21	xx	LANB blocking	Processor	MODERATE	Yes
ff	4x	xx	PINNED SLOT	Cache	MODERATE	No
ff	5x	xx	Abnormal end of Read processing in External storage system	Drive	MODERATE	No
ff	c3	0x	CACHE PACKAGE BLOCKADE PROCESSING END	Cache	SERVICE	Yes

Chapter 8: SIM codes

Trap reference code			Description	Section	Alert level	Host report [1]
SIM 22	SIM 23	SIM 13				
ff	cb	*xx*	CTL patrol check error	Cache	SERVICE	No
ff	cc	*xx*	CFM patrol check error	Cache	MODERATE	No
ff	cd	0*x*	Area is volatilized	Cache	SERVICE	No
ff	cf	*xx*	Package is volatilized	Cache	SERVICE	No
ff	d4	*xx*	Constitution definition error	Processor	MODERATE	No
ff	de	*xx*	WDCP loss of duplicated information	SM	SERVICE	No
ff	e4	0*x*	REPLACE FAILED	Cache	SERIOUS	No
ff	e7	00	Rebooted with volatilization after an instantaneous down	SM	SERIOUS	Yes
ff	e8	00	Definition/Installation mismatch	SM	SERIOUS	No
ff	ea	0*x*	RECOVERY OF AREA BLOCKED TEMPORARILY WAS COMPLETED	SM	SERVICE	Yes
ff	eb	00	Configuration information restore by backup failed	SM	SERIOUS	Yes
ff	ee	0*x*	AREA TEMPORARY BLOCKING	SM	SERVICE	Yes
ff	ef	00	Rebooted without volatilization after an instantaneous down	SM	SERVICE	No
ff	f0	*xx*	DIMM Correctable error	Cache	SERVICE	No
ff	f3	0*x*	PACKAGE BLOCKING	Cache	MODERATE	Yes
ff	f4	00	AREA BLOCKING	Cache	SERIOUS	Yes
ff	f4	01	AREA BLOCKING	Cache	SERIOUS	Yes
ff	f5	0*x*	Both areas failed	Cache	MODERATE	No
ff	f7	*xx*	GUM blocking	Cache	MODERATE	Yes

Trap reference code						Host report [1]
SIM 22	SIM 23	SIM 13	Description	Section	Alert level	
ff	f9	0x	REPLACE FAILED	Cache	SERVICE	No
ff	fa	xx	Battery warning	Battery	MODERATE	Yes
ff	fb	xx	Cache Uncorrectable error	Cache	MODERATE	Yes
ff	fe	xx	Warning for forcible volatile mode	Cache	MODERATE	Yes

Legend:

- **Yes:** This SIM performs the host report.

- **No:** This SIM does not perform the host report.

- **x:** A hexadecimal number between 0 and f.

1. If you select All for Notification Alert in the **Edit Alert Settings** window, the SNMP agent reports all SIMs. If you select Host Report, the SNMP agent reports only SIMs that perform the host report.

2. If the DKC emulation type is I-2105 or I-2107, SIMs are reported to the host only if SOM 308 is enabled. However, SOM 308 is disabled by default.

3. This SIM is not reported to mainframe hosts, but an alert is reported by Syslog, SNMP, and email.

4. The SNMP agent does not report this SIM when Host Report is selected for Notification Alert in the **Edit Alert Settings** window, because the SIM is reported to the host, but not to the SVP.

5. SIMs are not reported to the host by default. To enable reporting of service SIMs, see the *Hitachi Universal Replicator for Mainframe User Guide*.

6. *xxx*: Drive location. For details, see Converting DB and RDEV numbers to the HDD location number (on page 83).

7. If the value that consists of the lower 1 byte of SIM Byte 23 and 2 bytes of SIM Byte 13 is ffe, it means that multiple pools are blocked due to SM volatile.

Converting DB and RDEV numbers to the HDD location number

To identify the location of an error, convert drive box (DB) and RDEV numbers to the HDD location number.

Chapter 8: SIM codes

The following describes the bit alignment of DB and RDEV numbers (which are expressed by 13 bits of a SIM reference code) and the relationship between the DB and RDEV numbers and the HDD location.

- Format of the DB and RDEV numbers

W (4 bits)				X (4 bits)				Y (4 bits)				Z (4 bits)			
w	w	w	w	x	x	x	x	y	y	y	y	z	z	z	z
				DB number (8 bits)								RDEV number (5 bits)			

Example:

When SIM code = eb75a5 (Correction access occurred [eb7*xxx*]):

WXYZ = 75a5 (hexadecimal)

7				5				a				5			
0	1	1	1	0	1	0	1	1	0	1	0	0	1	0	1
				DB number = AD (hexadecimal) 173 (decimal)								RDEV number = 05 (hex) 5 (decimal)			

- Relationship between the DB and RDEV numbers and the HDD location number

HDD*xxx-yy*
└─── RDEV# (decimal)
└─── DB# (decimal)
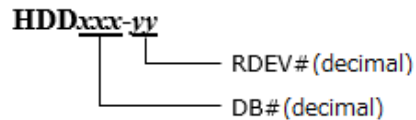
Example:

When *WXYZ* = 75a5 (hexadecimal):

HDD location number: HDD173-05

The following table describes the relationship between the DB and RDEV numbers (13 bits of a reference code), drive box number, RDEV number, and HDD location number, taking the example of drive boxes DB-000, DB-001, DB-190, and DB-191.

Reference code (DB#/RDEV#(hex))	Drive box number (DB#)	RDEV number (R#)	HDD location number
0000	DB-000	00	HDD000-00
0001		01	HDD000-01

Chapter 8: SIM codes

Reference code (DB#/RDEV#(hex))	Drive box number (DB#)	RDEV number (R#)	HDD location number
0002		02	HDD000-02
0003		03	HDD000-03
0004		04	HDD000-04
0005		05	HDD000-05
0006		06	HDD000-06
0007		07	HDD000-07
0008		08	HDD000-08
0009		09	HDD000-09
000A		10	HDD000-10
000B		11	HDD000-11
0020	DB-001	00	HDD001-00
0021		01	HDD001-01
0022		02	HDD001-02
0023		03	HDD001-03
0024		04	HDD001-04
0025		05	HDD001-05
0026		06	HDD001-06
0027		07	HDD001-07
0028		08	HDD001-08
0029		09	HDD001-09
002A		10	HDD001-10
002B		11	HDD001-11
...	...	...	...
17C0	DB-190	00	HDD190-00
17C1		01	HDD190-01
17C2		02	HDD190-02
17C3		03	HDD190-03

Chapter 8: SIM codes

Reference code (DB#/RDEV#(hex))	Drive box number (DB#)	RDEV number (R#)	HDD location number
17C4		04	HDD190-04
17C5		05	HDD190-05
17C6		06	HDD190-06
17C7		07	HDD190-07
17C8		08	HDD190-08
17C9		09	HDD190-09
17CA		10	HDD190-10
17CB		11	HDD190-11
17E0	DB-191	00	HDD191-00
17E1		01	HDD191-01
17E2		02	HDD191-02
17E3		03	HDD191-03
17E4		04	HDD191-04
17E5		05	HDD191-05
17E6		06	HDD191-06
17E7		07	HDD191-07
17E8		08	HDD191-08
17E9		09	HDD191-09
17EA		10	HDD191-10
17EB		11	HDD191-11

Hitachi Vantara