HITACHI
DATA SYSTEMS

Hitachi TagmaStore®
Adaptable Modular Storage
and Workgroup Modular Storage

Audit Log User's Guide

MK-96DF795-02

Trademarks

Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Contact the Hitachi Data Systems Legal Department for any export compliance questions.

Document Revision Level

Revision	Date	Description
MK-96DF795-0P	October 2006	Preliminary release
MK-96DF795-01	January 2007	Initial release
MK-96DF795-02	May 2007	Revision 2, supersedes and replaces MK-96DF795-01

Preface

This document assumes the following:

- The user is familiar with the operating system and web browser software on the system hosting the Storage Navigator Modular software.
- The user has a background in data processing and understands storage subsystems and their basic functions.
- The user is familiar with the AMS/WMS subsystem and has read and understands the manuals for the subsystem.

Notes:

- In this document the term "Storage Navigator" refers to the Storage Navigator Modular GUI, unless otherwise noted.
- In this document instructions with a "CAUTION" label indicate that failure to follow the instructions could result in damage to the subsystem or potential loss of data.
- The Storage Navigator windows shown in this document were captured on a Windows® system with the Internet Explorer web browser. The Storage Navigator screens may display differently on other operating systems and browsers.
- For further information, please contact your Hitachi Data Systems account team, or visit the Hitachi Data Systems worldwide web site at http://www.hds.com.

Notice: The use of the Storage Navigator Modular program and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

Software Version

This document revision applies to Hitachi TagmaStore® Adaptable Modular Storage and Workgroup Modular Storage Products version 7.0 and higher.

Convention for Storage Capacity Values

Storage capacity values for hard disk drives (HDDs) are calculated based on the following values:

1 KB (kilobyte) = 1,000 bytes
1 MB (megabyte) = $1,000^2$ bytes
1 GB (gigabyte) = $1,000^3$ bytes
1 TB (terabyte) = $1,000^4$ bytes

Storage capacity values for logical units (LUs) are calculated based on the following values:

1 KB (kilobyte) = 1,024 bytes
1 MB (megabyte) = $1,024^2$ bytes
1 GB (gigabyte) = $1,024^3$ bytes
1 TB (terabyte) = $1,024^4$ bytes

Referenced Documents

- *Hitachi TagmaStore AMS and WMS LUN Management User's Guide*, MK-95DF703
- *Hitachi TagmaStore AMS and WMS SNMP Agent User's Guide*, MK-95DF705
- *Hitachi TagmaStore AMS and WMS Password Protection User's Guide*, MK-95DF704
- *Hitachi TagmaStore AMS and WMS Error Codes*, MK-95DF788

Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please refer to specific section(s) and paragraph(s) whenever possible.

- **E-mail:** doc.comments@hds.com
- **Fax:** 858-695-1186
- **Mail:**
  Technical Writing, M/S 35-10
  Hitachi Data Systems
  10277 Scripps Ranch Blvd.
  San Diego, CA 92131

Thank you! (All comments become the property of Hitachi Data Systems Corporation.

Contents

List of Figures

List of Tables

Chapter 1 Overview of Audit Log

This chapter discusses the following topics:

- Introduction to Audit Log (see section 1.1)
- Introduction to the Syslog server (see section 1.2)

1.1 Introduction to Audit Log

The practice of logging and log management using Syslog has been around for many years, however, using storage technology as part of the process is new. The TagmaStore AMS/WMS Audit Log function allows you to record the access, activity, and configuration changes made to your storage subsystem.

Audit Logging has two primary functions:

- Helping ensure data security by alerting management and administrators to unusual or suspicious network and system behavior. This includes providing security auditors with the information required to validate security policy enforcement and proper segregation of duties.
- Helping with regulatory compliance, by allowing you to implement centralized aggregation of log data and formal data retention policies.

1.1.1 Increasing Data Security

Unfortunately, security incidents perpetrated by both internal and external sources are a real possibility that cannot be ignored. It is becoming increasingly common for data protection and privacy regulations to hold firms accountable for safeguarding their data. The general legal standard is “due care”, which means doing at least what is considered to be industry-standard, such as following security best practices frameworks (e.g., COBIT, BITS, COSO) and standards (e.g., ISO 17799 and NIST SP 800-53).

Audit Logging helps you with root-cause analysis following security breaches or other incidents. This allows you to monitor changes to the subsystem and take corrective actions where necessary.

1.1.2 Providing an Audit Trail for Regulatory Compliance

Using Audit log allows you to maintain and provide evidentiary information that will satisfy the ever-growing body of laws and regulations. Businesses are required to maintain certain types of data in a format that will withstand an outside audit. At a minimum, these regulations require you to prove chain of custody of the data, and provide long-term protection and retention of the log data. Audit Log helps businesses meet the increasingly strict and complex regulatory requirements, and avoid civil and criminal liability.

Some examples of specific statutory requirements are as follows:

- In the United States, the Health Insurance Portability and Accountability Act (HIPAA) requires hospitals, physicians, and managed care companies to adopt security, privacy, and data standards for medical information. It requires organizations to "audit and monitor system and user activity across the entire network, identify and investigate security breaches and suspicious behavior, and maintain an audit trail of user and network activity." HIPAA also specifies that companies should "Retain and protect log data as evidence…up to 6 years."
- In the United States, the Sarbanes Oxley (SOX) Act establishes corporate accountability for all public companies, requiring strict IT controls and processes. Specifically Sarbanes-Oxley requires companies to "Audit unauthorized access, misuse and fraud, in order to ensure the accuracy of corporate financial and business information" and "maintain financial records for seven years."
- Internationally, the Basel II Accord requires all internationally active banks to adopt similar or consistent risk management practices. Banks are required to implement a comprehensive program of risk prevention, detection, analysis, and management, and mitigate operational risks associated with IT systems by 2006. The accord recommends "retaining activity logs for 3 to 7 years."

1.2 Introduction to the Syslog Server

Audit Log uses the Syslog server, which is a commonly-used simple utility and protocol to exchange log messages. The term "Syslog" is often used for the protocol, the tools that send the logs (*syslogd*), as well as the individual logs and the log files themselves.

The Syslog architecture can be summarized as follows:

- Senders (devices and relays) send messages to relays or collectors with no knowledge of whether it is a collector or relay.
- Senders may be configured to send the same message to multiple receivers.
- Relays may send all or some of the messages that they receive to a subsequent relay or collector. In the case where they do not forward all of their messages, they are acting as both a collector and a relay. In Figure 1, these devices are designated as relays.
- Relays may also generate their own messages and send them on to subsequent relays or collectors. In that case, it is acting as a device.

Figure 1.1 illustrates some common Syslog configurations.

By default, Syslog messages are sent over UDP port 514 between:

- *devices* – machines that can generate messages
- *relays* – machines that can receive messages and forward them to other machines
- *collectors* – machines that receive messages and do not relay them to any other machines (a.k.a. Syslog server)

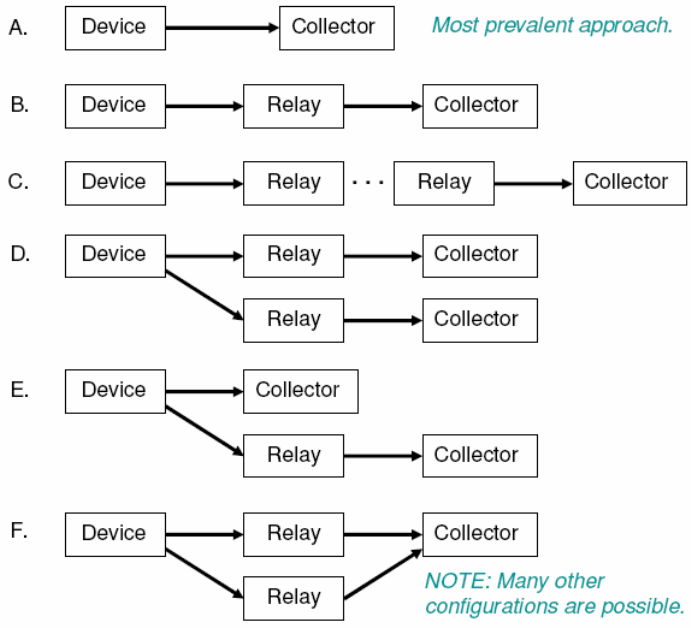

Figure 1.1 Examples of Syslog Architecture

The specific needs of your particular business will determine the system architecture. From a storage perspective, knowing where the log events need to be shipped, how the events need to be handled, and then implementing it appropriately represents the end point. The storage layer need only concern itself with plugging into this infrastructure and then transmitting the log events. In addition to the Syslog server, Audit Log also allows you to maintain a duplicate copy of the log inside the disk subsystem as a backup.

In the AMS/WMS subsystem, a log message is output to the Audit Log in two types of cases:

- A configuration change that is made either from Storage Navigator Modular or the host
- Powering up and shutting down the disk subsystem

Figure 1.2 illustrates those functions:

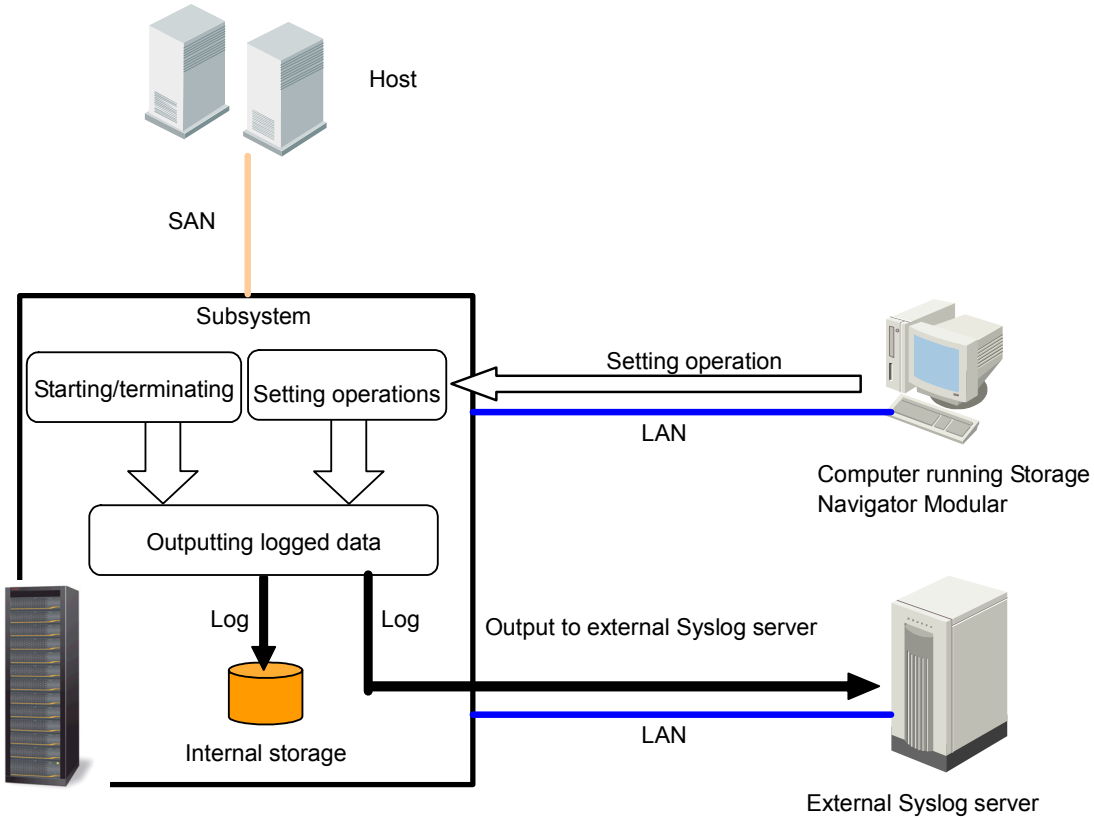

Figure 1.2 Functions That Generate Audit Log Output

Chapter 2 Preparing to Use Audit Log

This chapter discusses the following topics:

- Audit Log specifications and requirements (see section 2.1)
- Audit Log format (see section 2.2)

2.1 Audit Log Specifications and Requirements

Both the audit log and the Syslog server conform to the standards set by the BSD Syslog Protocol (RFC3164). Table 2.1 lists Audit Log specifications.

Table 2.1 Audit Log Specifications

Item	Specifications
User interface	▪ Subsystem microcode: 0760/A or higher. ▪ Storage Navigator microcode: 6.00 or higher.
Data length	Less than 1,024 bytes per log. Longer messages are truncated.
Data format	See section 2.2.
Events recorded in the Audit Log	Audit log entries are created in the following cases: ▪ Starting or stopping the subsystem ▪ If Account Authentication is enabled, logging onto or off of the subsystem. ▪ Changing the subsystem configuration (e.g., creating or deleting an LU). ▪ Initializing the log stored inside the disk subsystem (this log entry is only output to the Syslog server). Audit log entries are *not* created in the following cases: ▪ Partial blockade and recovery of the subsystem. ▪ Settings made to the subsystem by web function ▪ Device authentication success or failure ***Note***: Command Control Interface (RAID Manager), NAS Setup, and NAS Manager Modular output separate logs.
Delay between operations and Audit Log output	As a general rule, the log is sent in real time. If network traffic is very high, there might be a delay of up to a few seconds.
Port number	UDP port 514
Maximum Audit Log capacity	2,048 events. If the number of events exceeds the maximum, it is wrapped around (earlier events are dropped from the list as later events are added).
Setting the NTP server time zone	If you are operating multiple subsystems, synchronizing the clocks using NTP server is recommended. For more information, see *Hitachi TagmaStore® AMS/WMS Storage Navigator Modular for GUI User's Guide* (MK-95RD711)

2.2 Audit Log Format

Figure 2.1 illustrates the Audit Log format. Figure 2.2 illustrates a sample Audit Log output, and Table 2.2 explains each component. See Chapter 6 for more specific examples of the audit log output.

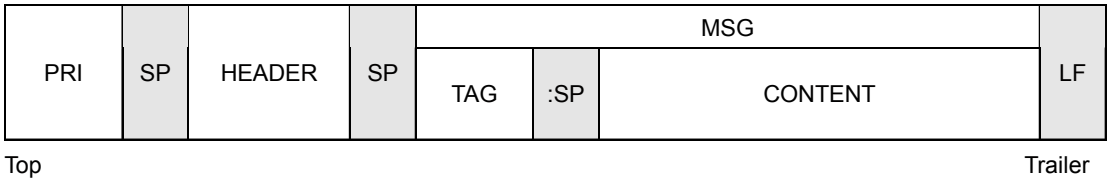

Figure 2.1 Audit Log Format

```
14 Nov 22 11:10:42 192.168.100.10 Storage: CELFSS,1,123456,,2005-11-22T11:10:40.0+09：00,Storage,
 1         2              3          4       5    6   7                9                  10

192.168.100.10,Authentication,Success,uid=Hitachi_storage_admin,DF700:750012345,,,,,,
      11              12          13              14                  15

from=192.168.100.200,,to=192.168.100.10,2000,,,,3EB70100 Account User Login
          21                    23         24               28
```

Figure 2.2 Sample Audit Log Output

Table 2.2 Items Output to the Audit Log

No.	Item		Explanation
1	PRI	Priority	The output priority is calculated by the following formula: Priority = (8 × facility) + severity, with the facility value fixed at 1. 3: Error (an operation has ended abnormally) 4: Warning (an operation has partly ended abnormally) 6: Informational (an operation has ended normally) For example, an informational message has a priority of 14: (8 × 1) + 6) **
2	Header	Date, time	MMM: month, DD: day, hh: hour, mm: minute and ss: second. If the date is a single digit, there is a blank space before the digit.
3		Detected location	IP address.
4	MSG/ TAG	Program or process name	Storage
5	MSG/ Contents	Common specification identification information of Hitachi storage security	The common specification identification character is output as CELFSS.
6			Revision number (1).
7		Message identification information	The Syslog header serial number. ***Note***: When the disk array subsystem is rebooted, the sequential numbers to be output and those that have been output before the reboot will get out of order. Be careful that orders of the sequential numbers and logs that are output do not match.
8			Message ID (not used)
9		Date, time, time difference	The date, time, and the difference between that date and time and UTC (Coordinated Universal Time), (YYYY-MM-DD-Thh:mm:ss.0 ± *hh*:*mm*" (YYYY). If there is no difference, "+00:00" is output. ***Note***: The time format for seconds is "ss.0", indicating one decimal place.
10		Detection entity identification	Storage.
11		Detected location	IP address.
12		Type of audit event	The event category ▪ **StartStop**: Subsystem power on or off ▪ **Authentication**: Success/failure of authentication ▪ **AccessControl**: An attempt by a user to perform a function outside of their user access. The rejection is logged. ▪ **ConfigurationAccess**: Configuration setting operations
13		Result of the audit event	▪ Success: The event has ended successfully. ▪ Failed: The event has ended abnormally. ▪ Occurred: Occurrence of an audit event
14		Subject identification information	The log prefix shows the type of event: ▪ uid: User ID (management I/F event). ▪ wwn: World Wide Name (fibre event) ▪ iSN: iSCSI Name (by iSCSI event)

No.	Item		Explanation
			▪ system: the disk array subsystem (disk array subsystem event) When Account Authentication is disabled or not installed, only a prefix is output.
15		Hardware identification information	The storage subsystem ID (DF700) and serial number
16		Generated location information	Not used.
17		Related information	The location identification name (not used)
18			FQDN (not used)
19			Redundant identification information (not used)
20		Agent information	Not used.
21		Detailed information	Host sending the request
22			Port sending the request (not used).
23			Host receiving the request
24			Port receiving the request
25			Collective operation identification number (not used)
26			Reserve #1 (not used)
27			Reserve #2 (not used)
28			The audit log output (includes details such as the object and parameters of the management operation, and a reason why the event is audited).

Chapter 3 Audit Log Windows

This chapter discusses the following topics:

- License Key window (see section 3.1)
- Install Options dialog box (see section 3.2)
- De-Install Options dialog box (see section 3.3)
- Audit Log window, Audit Log tab (see section 3.4)
- Audit Log window, Audit Log tab (see section 3.5)

3.1 Array System Viewer, License Key Window

Access the License Key window by opening the Array System Viewer, selecting the **Logical Status** tab, then selecting the **License Key** button on the left side of the panel.

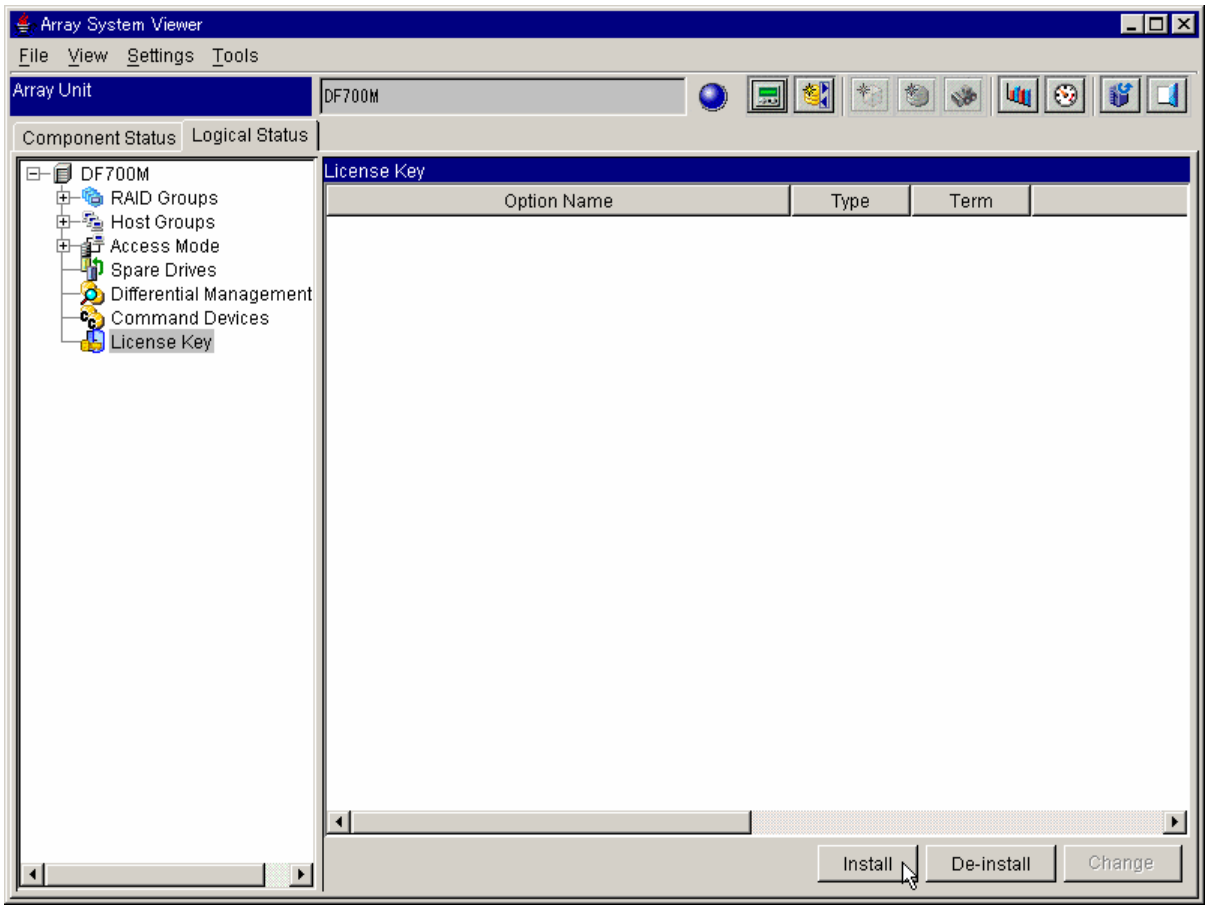

Figure 3.1 License Key Window (Audit Log Not Installed)

The License Key window has the following features:

- The **Option Name** column lists the installed options.
- The **Type** column displays the license key for each type.
  - **Temporary** indicates a temporary license key.
  - **Permanent** indicates a permanent license key.
- The **Term** column indicates whether that option is enabled.
  - **Enable** indicates that the option is enabled.
  - **Disable** indicates that the option is disabled.
- The **Install** button opens the **Install Options** dialog box (see Figure 3.4).
- The **De-install** button opens the **De-Install** Options dialog box (see Figure 3.5).

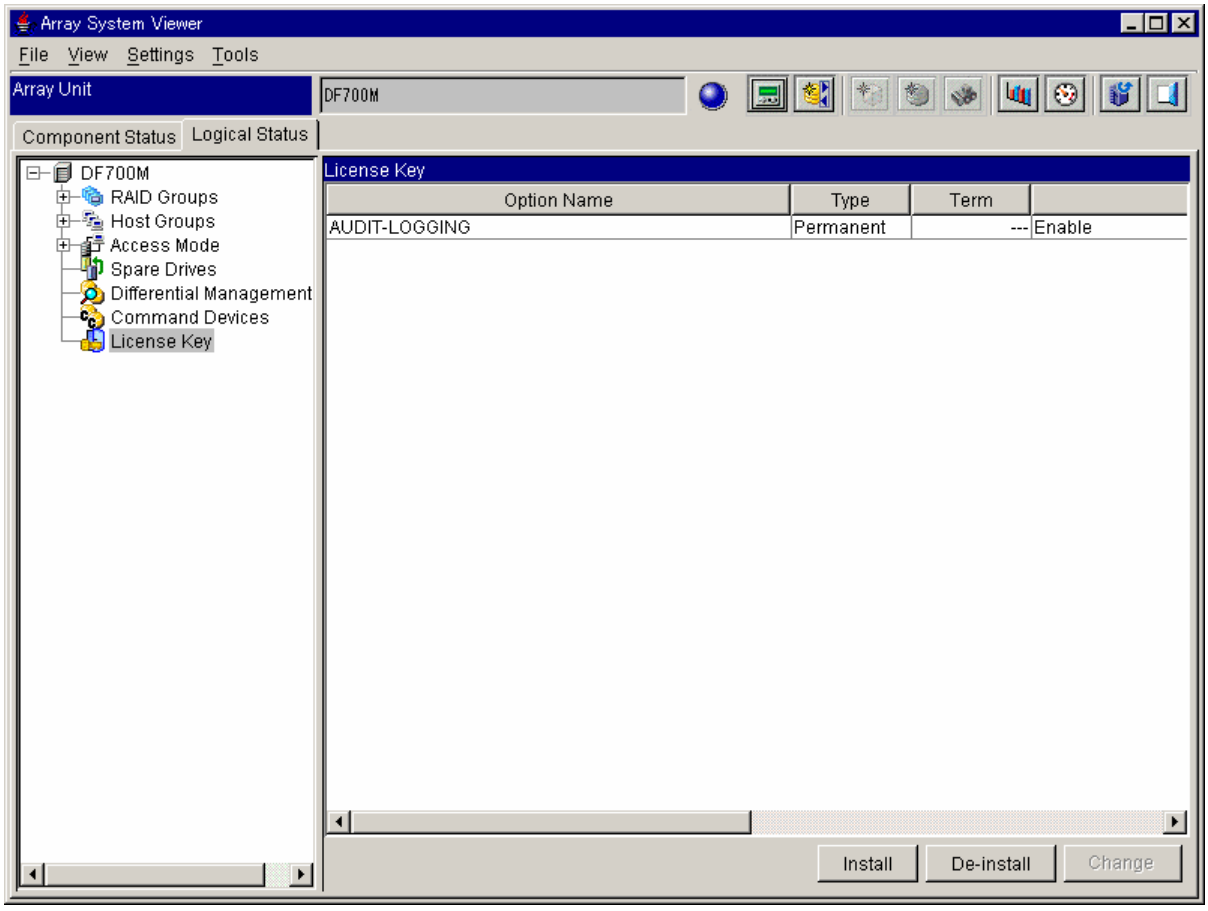

Figure 3.2 License Key Window (Audit Logging Installed and Enabled)

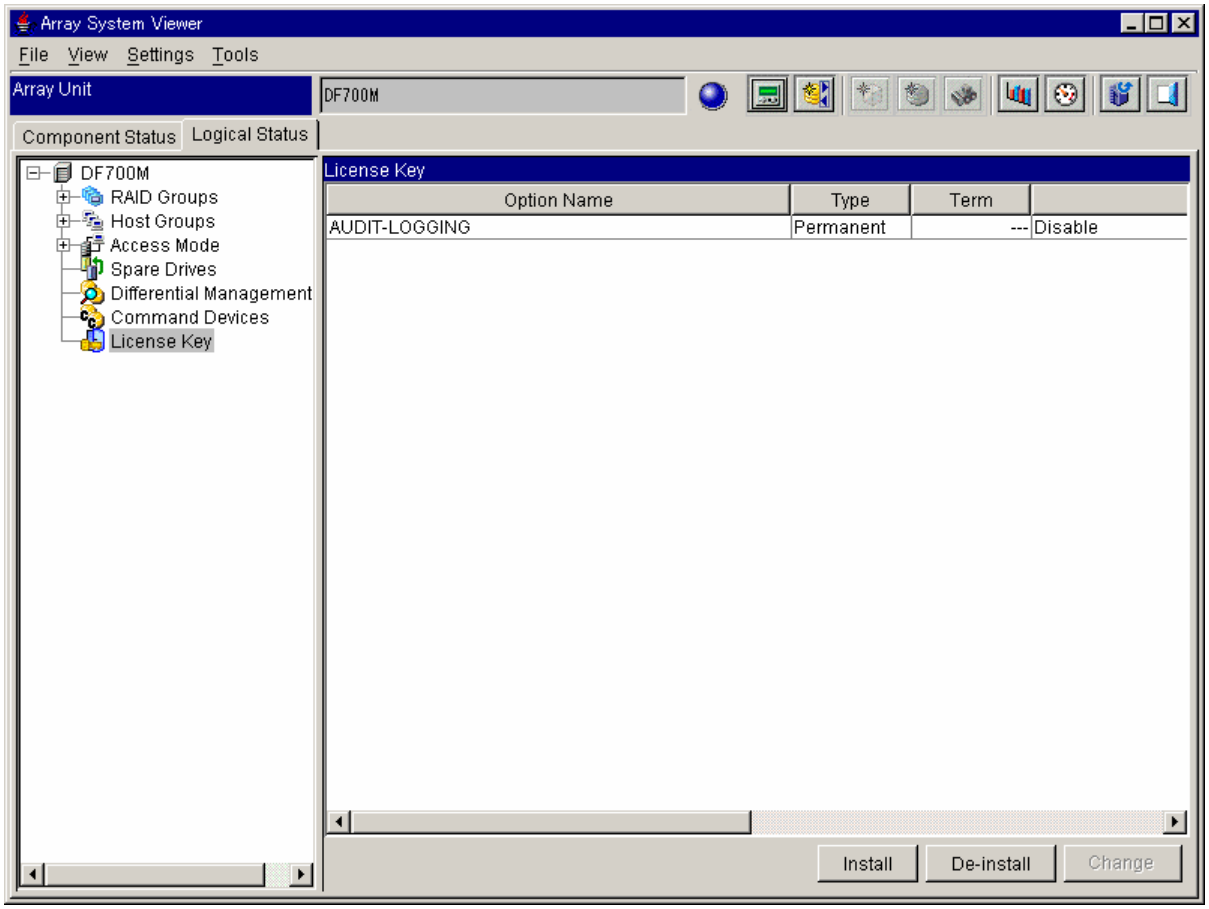

Figure 3.3 License Key Window (Audit Logging Disabled)

3.2 Install Options Dialog Box

Access the Install Options dialog box by selecting the **Install** Button on the License Key window (refer to section 3.1).

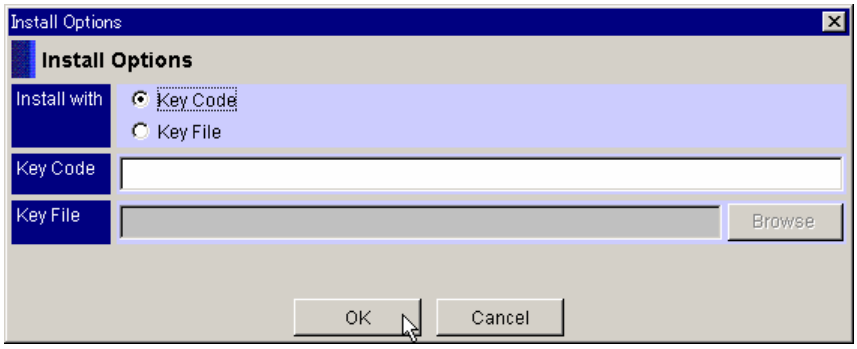

Figure 3.4 Install Options Dialog Box

The Install Options dialogue box has the following features:

- The **Key Code** radio button allows you to install an option using a key code. Selecting this button enables the **Key Code** text box.
- The **Key File** radio button allows you to install an option using a key file. Selecting this button enables the Key File text box and the **Browse** button.
- The **Key Code** text box allows you to input a license key code.
- The **Key File** text box and **Browse** button allow you to browse for and select a key file.

For more information on installing an option using the GUI (graphical user interface), see section 4.1.1.

3.3 De-Install Options Dialog Box

Access the De-Install Options dialog box by selecting the **De-Install** button on the License Key window (refer to Figure 3.2).

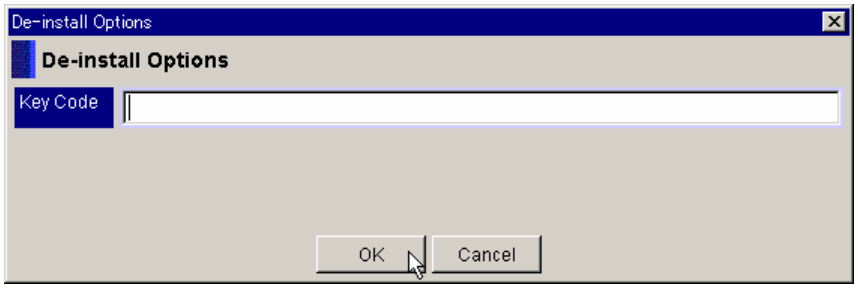

Figure 3.5 De-install Options Dialog Box

The De-Install Options Dialog box has the following features:

- The **Key Code** text box allows you to enter the license key code for the option that you want to disable.
- The **OK** button implements your choice and returns you to the License Key window.
- The **Cancel** button cancels your choice and returns you to the License Key window.

3.4 Audit Log Window, Audit Log Tab

Access the Audit Log window by opening the Array Systems viewer, selecting the **Tools** menu, and then **Audit Logging**. The Audit Log tab is the default view.

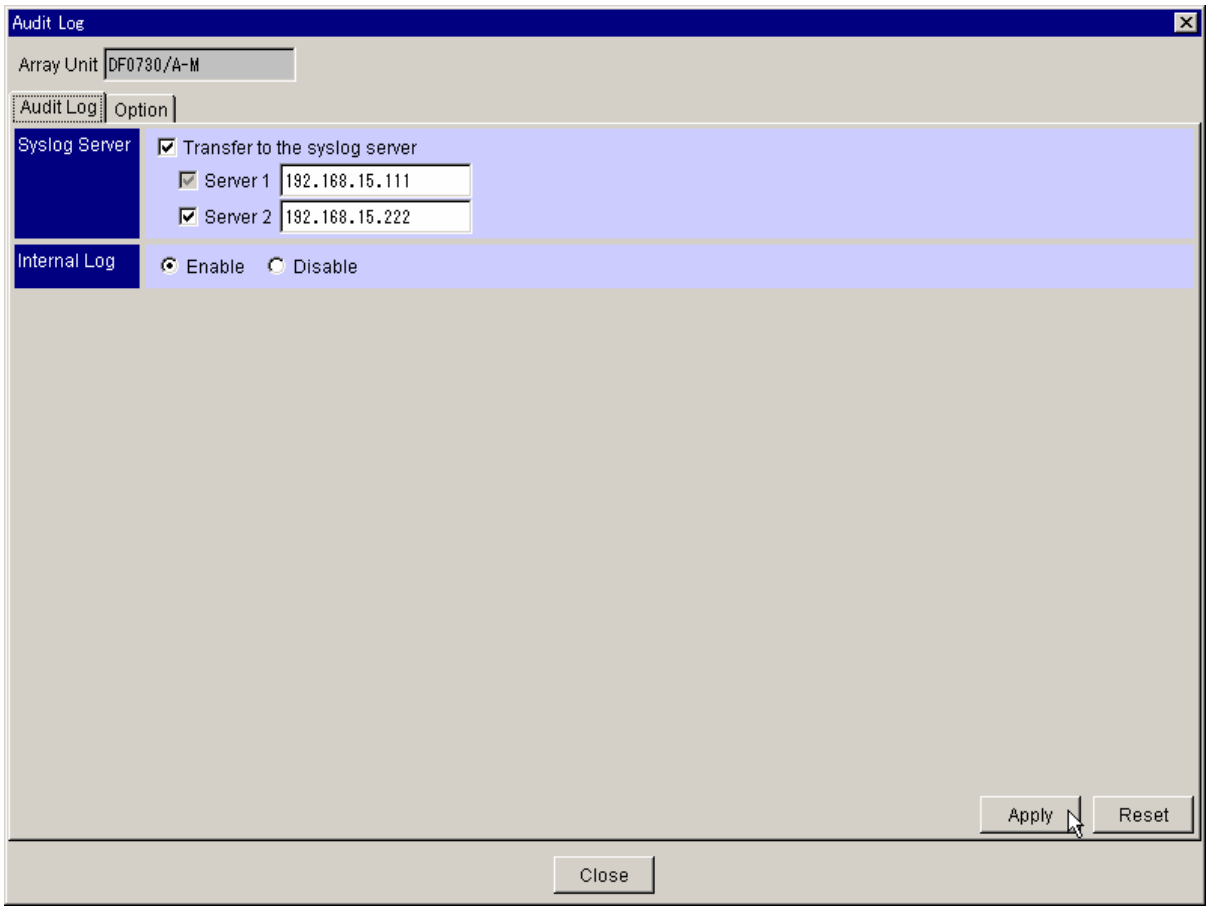

Figure 3.6 Audit Log Window, Audit Log Tab

The Audit Log tab has the following features:

- The **Syslog Server** box allows you to select up to two Syslog servers as recipients of the audit log.
  - The **Transfer to syslog server** check box allows you to download audit log to one or two Syslog servers.
  - The **Server 1** and **Server 2** checkboxes allow you to enable the audit log to be downloaded to the server specified in the adjacent text boxes.
- The **Internal Log** box allows you to maintain an internal copy of the audit log.
  - **Enable** will create an internal copy.
  - **Disable** will not create an internal copy.

3.5 Audit Log Window, Option Tab

Access the Audit Log Window, Option Tab by opening the Array Systems viewer, then selecting **Tools** and **Audit Logging**. Select the Option tab.

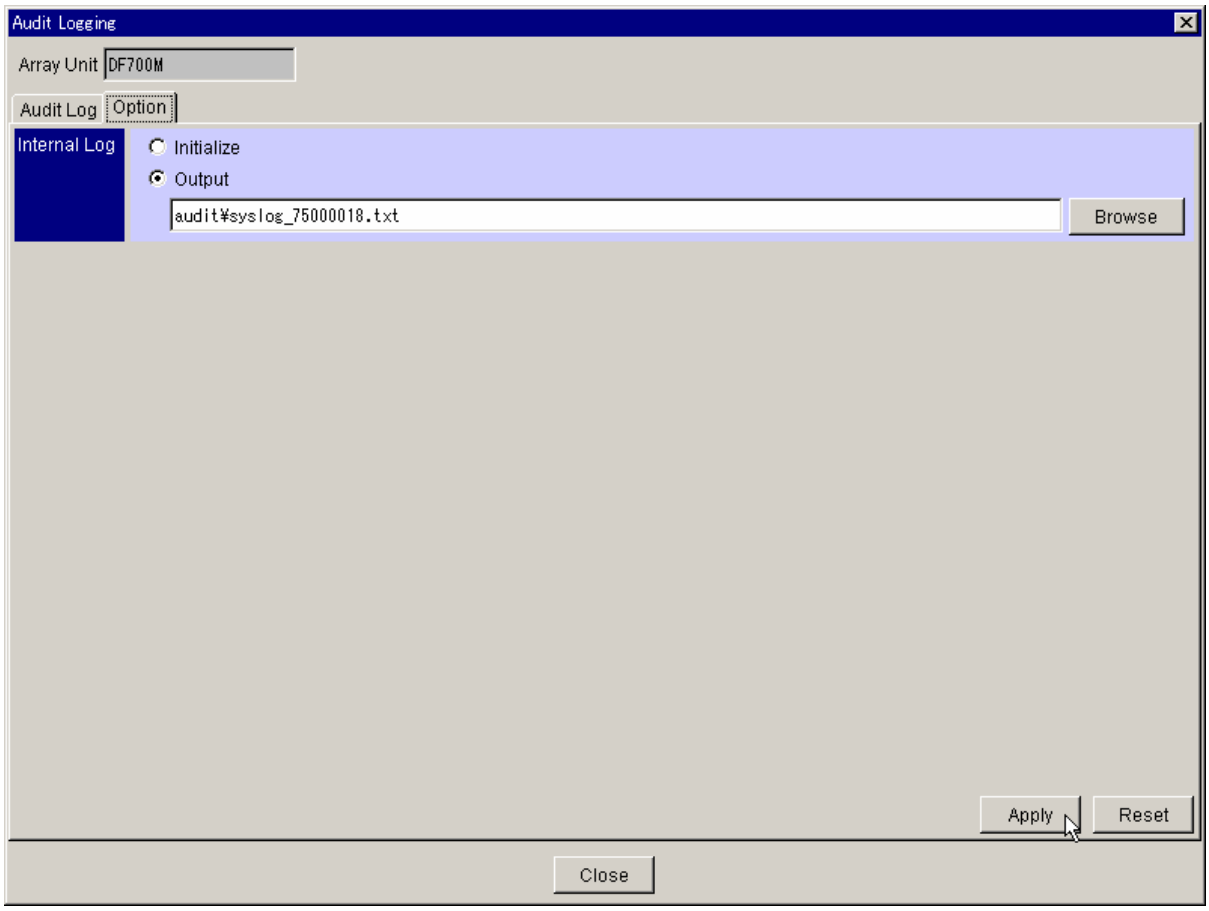

Figure 3.7 Audit Log Window , Option Tab

The Option tab has the following features:

- The **Internal Log** box allows you to configure the internal log.
  - The **Initialize** radio button allows you to initialize the internal log.
  - The **Output** radio button allows you to select an output destination for the internal log. You can either type the destination into the text box, or use the **Browse** button to select the location.
- The **Apply** button implements your choices.
- The **Cancel** button cancels your choices.
- The **Close** button closes the panel and returns you to the Array Systems Viewer.

Chapter 4 Using the GUI to Perform Audit Log Operations

This chapter discusses the following topics:

- Installing, enabling, and uninstalling Audit Log (see section 4.1)
- Configuring the Syslog output (see section 4.2)
- Exporting the internal logged data (see section 4.3)
- Initializing the logged data (see section 4.4)

For instructions on performing Audit Log functions using the command line interface, see Chapter 5.

Note: If Account Authentication is enabled, you must log onto the subsystem with Audit Log Administrator privileges in order to perform any Audit Log functions.

4.1 Installing, Enabling, and Uninstalling Audit Log

4.1.1 Installing Audit Log

To install Audit Log:

1. Log onto the subsystem.
   - If Account Authentication is enabled, log on as an audit log administrator.
   - If Account Authentication is not enabled, change the operation mode to **Management Mode**.
2. The Array System Viewer displays. Click the **Logical Status** tab, then click the **License Key** icon to display the License Key window (see Figure 4.1).
3. Click the **Install** button to display the **Install Options** dialog box (see Figure 4.2).
4. To install the option using the key code, do the following:
   - Click the **Key Code** radio button
   - In the **Key Code** text box, type or paste the key code.
5. To install the option using the key file, do the following:
   - Click the **Key File** radio button
   - Click the **Browse** button, and then navigate to the location of the key file.
6. The Install Options Confirmation Message (1) displays (see Figure 4.3). Verify that the option name(s) are correct, and then click **OK**.
7. If you used a key file, the Install Options Confirmation Message (2) displays (see Figure 4.4). Click **OK** to continue the installation, or click **Cancel** to cancel.
8. If you have enabled Cache Partition Manager, the Cache Partition Manager warning message displays (see Figure 4.5). Audit Logging does not use the data pool, so this warning does not apply. Click **OK** to continue the installation.
9. If you used a key file, the Result dialog box displays. Click **Close**.
10. The License Key panel will display Audit Logging as installed (see Figure 4.6).

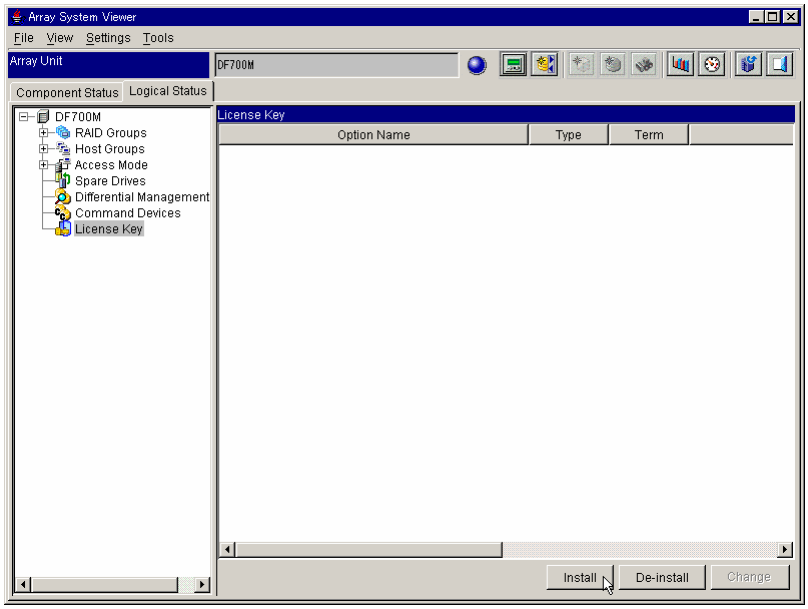

Figure 4.1 Accessing the License Key Window

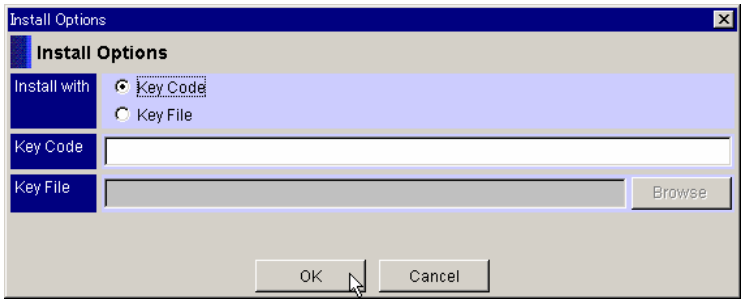

Figure 4.2 Install Options Dialog Box

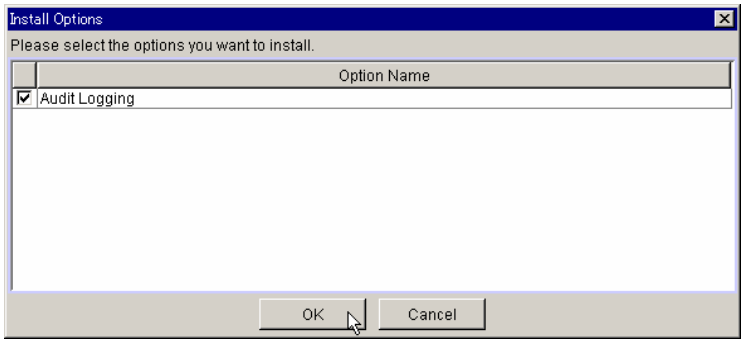

Figure 4.3 Install Options Confirmation Message (1)

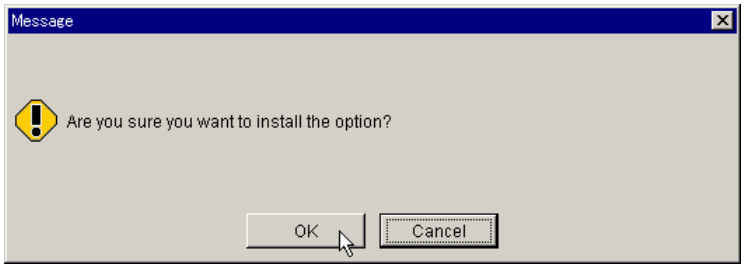

Figure 4.4 Install Options Confirmation Message (2)

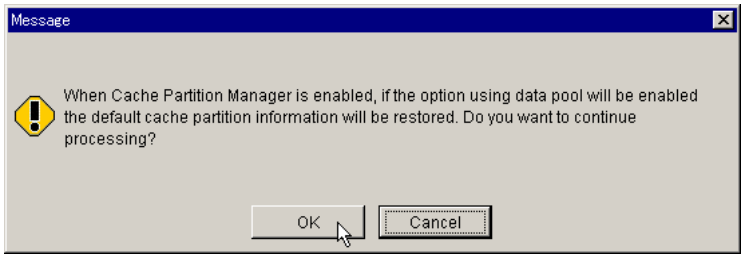

Figure 4.5 Cache Partition Manager Warning Message

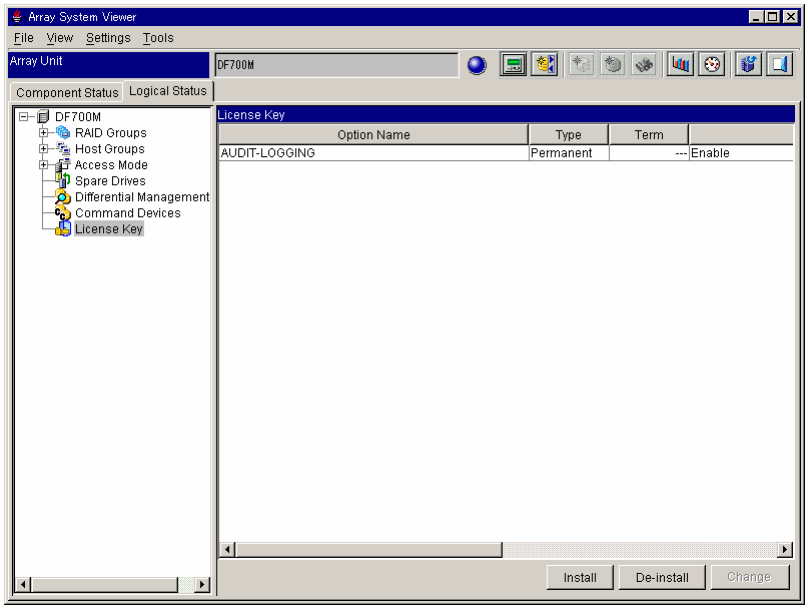

Figure 4.6 Audit Logging Installed

4.1.2 Enabling and Disabling Audit Log

To enable or disable Audit Log:

1. Log onto the subsystem.
   - If Account Authentication is enabled, log on as an audit log administrator.
   - If Account Authentication is not enabled, change the operation mode to **Management Mode**.
2. The Array System Viewer displays. Click the **Logical Status** tab, and then click the **License Key** icon to display the License Key window. Once you have installed Audit Logging, it will display in the **Option Name** column (refer to Figure 4.6).
3. To enable or disable Audit Logging, in the **Option Name** column, click on **AUDIT-LOGGING** then click **Change**.
4. Click **OK** on the confirmation message (see Figure 4.7).
5. The License Key window will display either **Enable** (see Figure 4.9) or **Disable** (see Figure 4.10).

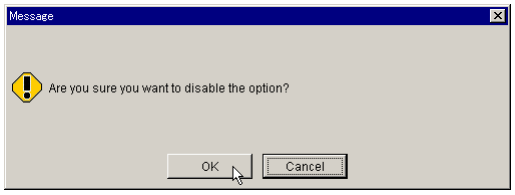

Figure 4.7 Enable/Disable Confirmation Message

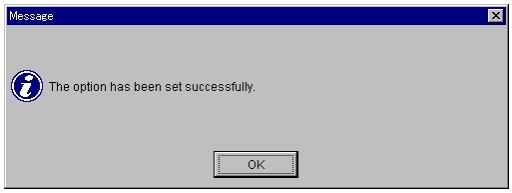

Figure 4.8 Enable/Disable Operation Complete

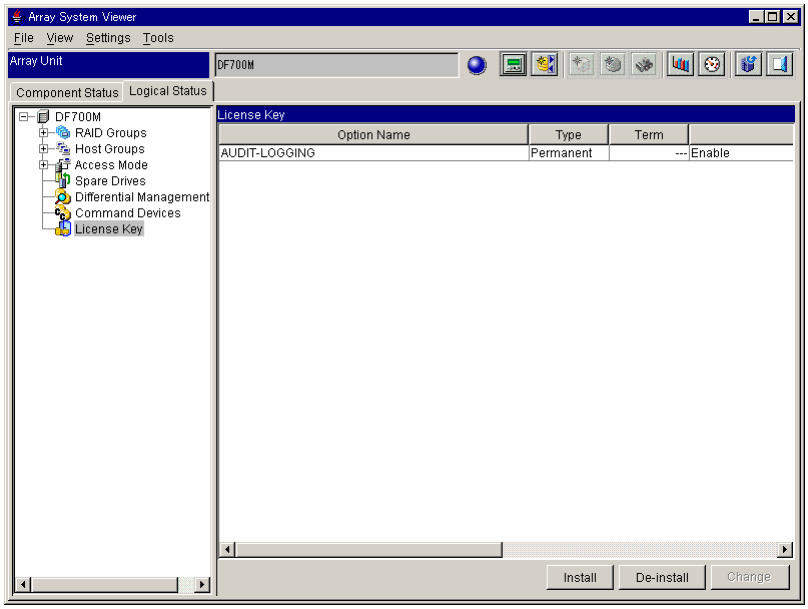

Figure 4.9 Audit Logging Enabled

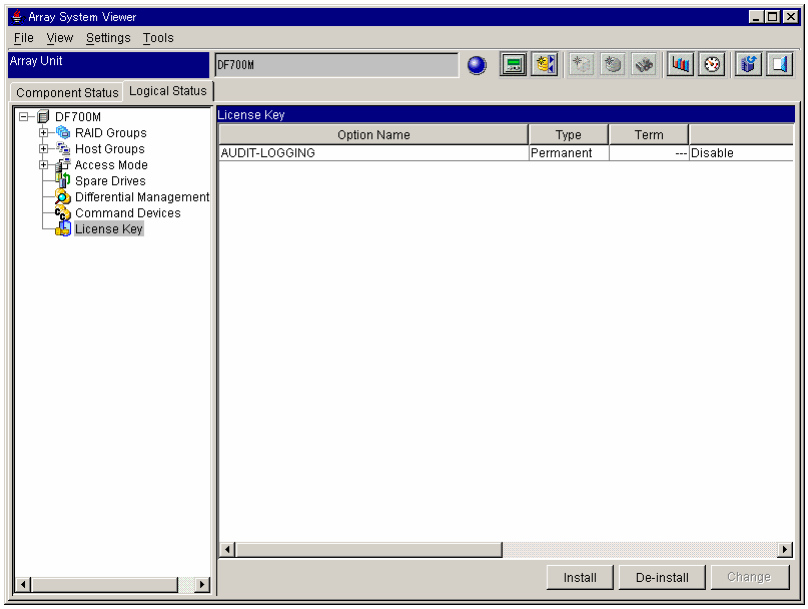

Figure 4.10 Audit Logging Disabled

4.1.3 Uninstalling Audit Log

To uninstall Audit Log:

1. Log onto the subsystem.
   - If Account Authentication is enabled, log on as an audit log administrator.
   - If Account Authentication is not enabled, change the operation mode to **Management Mode**.
2. The Array System Viewer displays. Click the **Logical Status** tab, then click the **License Key** icon to display the License Key window (refer to Figure 4.9).
3. Click the **De-install** button to display the **De-install Options** dialog box.
4. Enter a key code in the text box. Click **OK**.
5. A screen appears, requesting a confirmation to uninstall the Audit Logging option. Click **OK**.
6. A message appears, confirming that this feature has been uninstalled. Click **OK**.
7. The License Key window is updated and then displayed. (Refer to Figure 4.6)

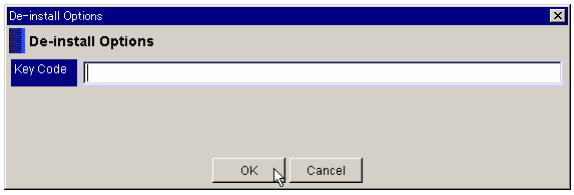

Figure 4.11 De-install Options Dialog Box

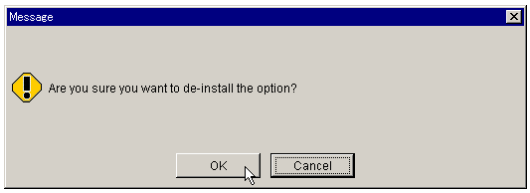

Figure 4.12 De-Install Option Confirmation Message

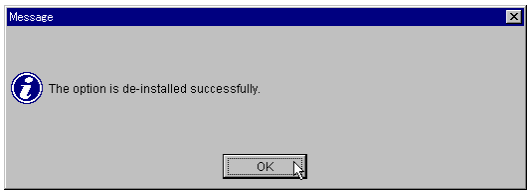

Figure 4.13 De-Installation Successful

4.2 Configuring the Syslog Output

To configure the Syslog output:

1. Log onto the subsystem.
   - If Account Authentication is enabled, log on as an audit log administrator.
   - If Account Authentication is not enabled, change the operation mode to **Management Mode**.
2. The Array System Viewer displays. From the **Tools** menu, select **Audit Logging** to display the **Audit Log** panel. The Audit Log tab is the default view (see Figure 4.14).
3. In the **Syslog Server** box, select the **Transfer to syslog server** checkbox if you want to use one or two Syslog servers.
   - Select the **Server 1** checkbox and enter the IP address for server 1.
   - If you want to add a second Syslog server, select the **Server 2** checkbox and enter the IP address for server 2.
4. If you want to save a copy of the audit log data in the subsystem, in the **Internal Log** box, select the **Enable** check box. This is recommended because the log is sent to the Syslog server using UDP, and it is not resent if there is a failure along the communication path. If that occurs, the log stored in the Syslog server may have omissions. See section 4.3 for instructions on exporting the internal log data.
5. Select **Apply**, and then select **OK** on the confirmation message (see Figure 4.15).
6. If the Syslog server is successfully configured, a confirmation message is sent to the Syslog server (see Figure 4.16). If that message is not received, verify the following:
   - The IP address of the destination Syslog server
   - The management port IP address
   - The subnet mask
   - The default gateway.
7. If the audit log is still not being received by the Syslog server, verify the following:
   - The network configuration
   - The condition of the Syslog server.

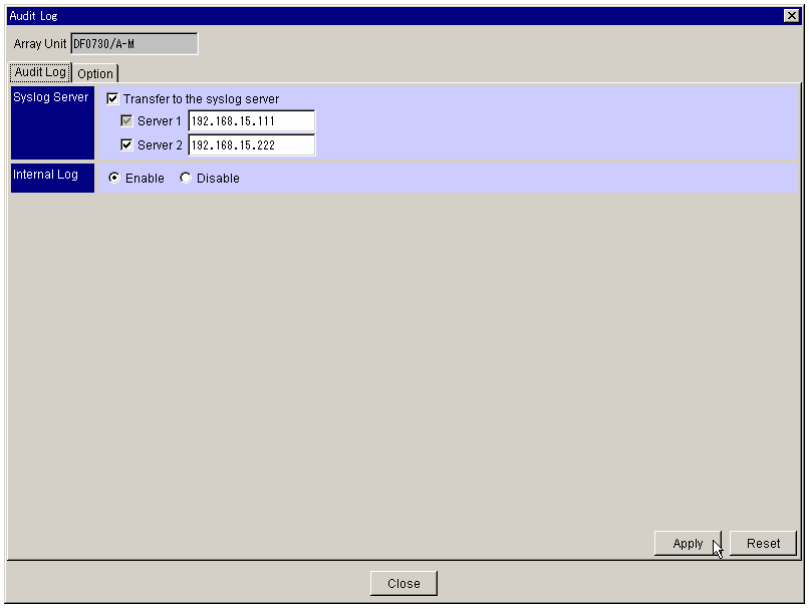

Figure 4.14 Audit Log Panel, Audit Log Tab

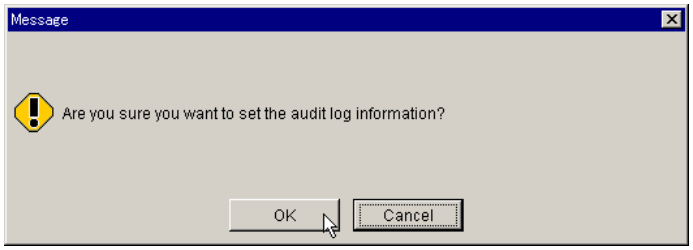

Figure 4.15 Audit Log Setting Confirmation Message

```
3EB20100 Set Audit Log Options: Transfer=*1 Server1_IP=*2 Server2_IP=*3 Internal=*4
                              *1: Whether to transfer to the syslog server or not [ON|OFF]
                              *2: IP address of syslog server 1
                              *3: IP address of syslog server 2
                              *4: Internal log [Enable|Disable]
```

Figure 4.16 Syslog Server Confirmation Message

4.3 Exporting the Internal Logged Data

Warning: This operation may affect host performance.

Note: Before performing this operation, you should already have selected the **Enable** check box in the **Internal Log** box (refer to Figure 4.14). Refer to section 4.2 if you need instructions.

Note: Only one user at a time can export the data to the internal log.

To export the internal logged data:

1. Log onto the subsystem.
   - If Account Authentication is enabled, log on as an audit log administrator.
   - If Account Authentication is not enabled, change the operation mode to **Management Mode**.
2. The Array System Viewer displays. From the **Tools** menu, select **Audit Logging** to display the **Audit Log** panel. The Audit Log tab is the default view.
3. Select the Option tab (see Figure 4.17). Either specify the file output path and output name or select **Browse** to specify the output destination file.
4. Select **Apply**, and then select **OK** on the confirmation message (see Figure 4.18).
5. If an error occurs, an error message will display (see **). Wait 3 minutes, then re-execute the export of the audit log data.

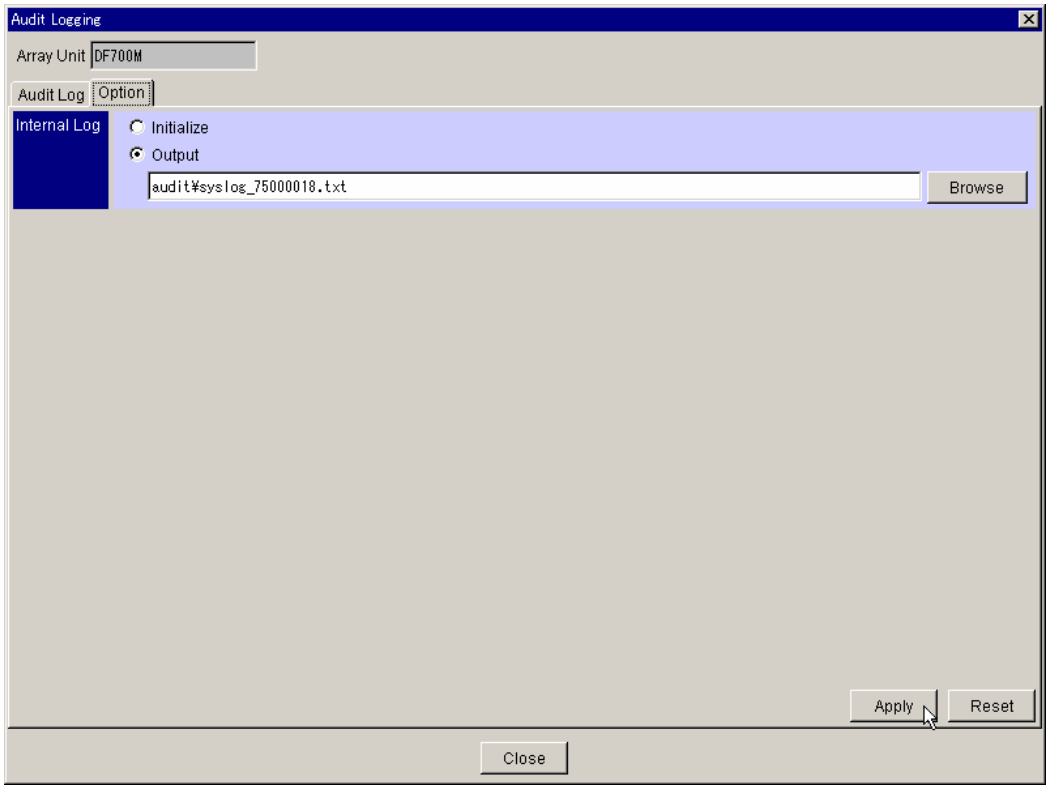

Figure 4.17 Configuring the Internal Log Output

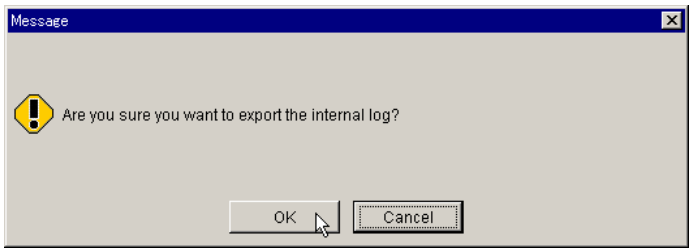

Figure 4.18 Export Internal Log Confirmation Message

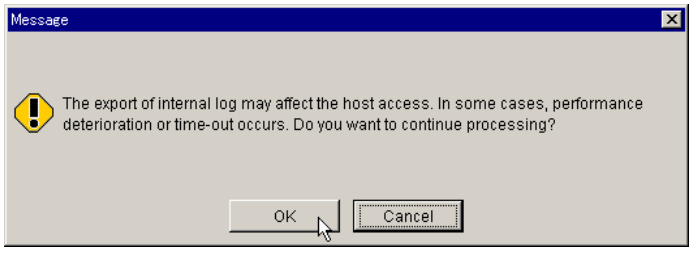

Figure 4.19 Host Access Warning Message

4.4 Initializing the Internal Logged Data

Warning: This action will delete all of the data in the internal log, and the data cannot be restored. Make sure that you have exported the log data before you perform this action. Refer to 4.3 for instructions.

Note: When the log stored inside the disk subsystem is valid, it cannot be initialized. Make the log stored inside the disk subsystem invalid, and then initialize it.

To initialize the internal logged data:

1. Log onto the subsystem.
   - If Account Authentication is enabled, log on as an audit log administrator.
   - If Account Authentication is not enabled, change the operation mode to **Management Mode**.
2. The Array System Viewer displays. From the **Tools** menu, select **Audit Logging** to display the **Audit Log** panel. The **Audit Log** tab is the default view.
3. Select the **Option** tab (see Figure 4.20).
4. Select the **Initialize** radio button, and then select the **Apply** button.
5. Select **OK** on the confirmation message (see Figure 4.21).
6. The Audit Log Initialize warning message displays. This action will permanently delete all log data. Select the **OK to initialize** checkbox, and then click **OK**.
7. When the operation is complete, a confirmation message displays. Click **OK**.

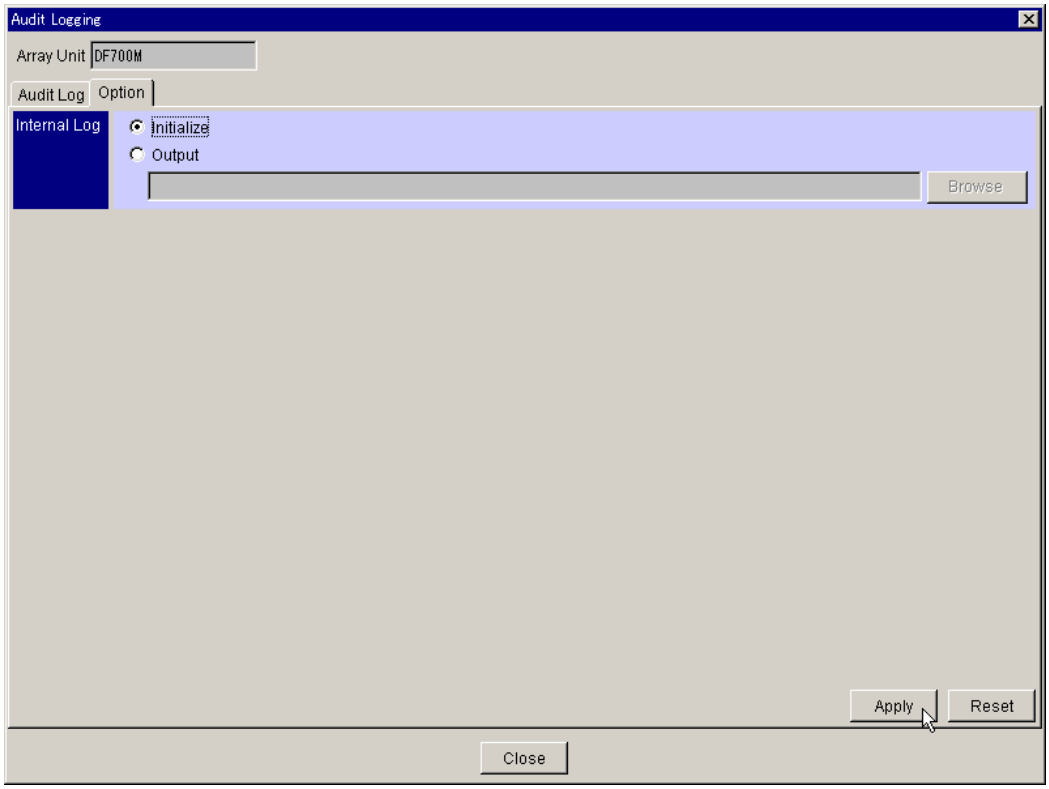

Figure 4.20 Initializing the Audit Log Internal Log

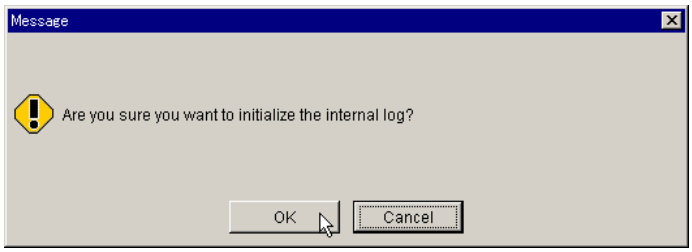

Figure 4.21 Audit Log Initialize Confirmation Message

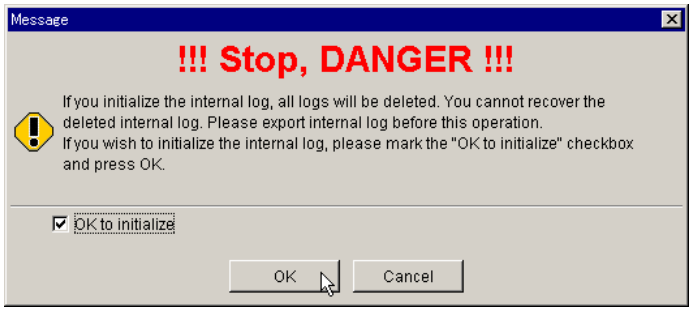

Figure 4.22 Audit Log Initialize Warning Message

Chapter 5 Using the Command Line Interface to Perform Audit Log Operations

This chapter discusses the following topics:

- Installing, enabling, and uninstalling Audit Log (see section 5.1)
- Configuring the Syslog server (see section 5.2)
- Enabling internal data logging (see section 5.3)
- Exporting the internal logged data(see section 5.4)
- Initializing the internal logged data (see section 5.5)

For instructions on performing Audit Log functions using the GUI, refer to Chapter 4.

Note: If Account Authentication is enabled, you must log onto the subsystem with Audit Log Administrator privileges in order to perform any Audit Log functions.

5.1 Installing, Uninstalling, and Enabling Audit Log (CLI)

5.1.1 Installing Audit Log

To install Audit Log:

1. From the command prompt, connect to the subsystem where you will install Audit Log.
2. Execute the auopt command, as shown in Figure 5.1. ***Note***: Part of this example has gray background shading, which is only displayed if you have previously enabled Cache Partition Manager.
3. Verify the installation as shown in Figure 5.2.

```
% auopt -unit subsystem-name -lock off -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to install the option? (y/n [n]): y
When Cache Partition Manager is enabled, if the option using data pool will be
enabled the default cache partition information will be restored.
Do you want to continue processing? (y/n [n]): y
The option is installed successfully.
%
```

Figure 5.1 Installing Audit Log

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name  Type      Term     Status
AUDIT-LOGGINGPermanent ---      Enable
%
```

Figure 5.2 Verifying Audit Log Status (Installed)

5.1.2 Enabling and Disabling Audit Log

To enable or disable Audit Log:

1. From the command prompt, connect to the subsystem.
2. To enable Audit Log, execute the **auopt** command as shown in Figure 5.3.
3. To disable Audit log, execute the **auopt** command as shown in Figure 5.4.
4. Verify the status of by executing the **auopt** command, as shown in Figure 5.5.

```
% auopt -unit subsystem-name -option AUDIT-LOGGING -st enable
Password: manager-password
Are you sure you want to disable the option? (y/n [n]): y
The option has been set successfully.
%
```

Figure 5.3 Enabling Audit Log

```
% auopt -unit subsystem-name -option AUDIT-LOGGING -st disable
Password: manager-password
Are you sure you want to disable the option? (y/n [n]): y
The option has been set successfully.
%
```

Figure 5.4 Disabling Audit Log

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name  Type      Term     Status
AUDIT-LOGGINGPermanent ---      Disable
%
```

Figure 5.5 Verifying Audit Log Status (Enable or Disable)

5.1.3 Uninstalling Audit Log

To uninstall Audit Log:

1. From the command prompt, connect to the subsystem.
2. To uninstall Audit Log, execute the **auopt** command as shown in Figure 5.6.
3. Verify the status as shown in Figure 5.7.

```
% auopt -unit subsystem-name -lock on -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to de-install the option? (y/n [n]): y
The option is de-installed successfully.
%
```

Figure 5.6 Uninstalling Audit Log

```
% auopt -unit subsystem-name -refer
Password: manager-password
DMEC002015: No information displayed.
%
```

Figure 5.7 Verifying Audit Log Status (Uninstall)

5.2 Configuring the Syslog Output

To configure the Syslog output:

1. From the command prompt, connect to the subsystem.
2. Specify the Syslog server information as shown in Figure 5.8. This example assumes that the Syslog server 1 IP address is 192.168.100.100 and that there is no output to Syslog Server 2.
3. Verify the setting, as shown in Figure 5.9.

```
% auauditlog -unit subsystem-name -set -syslogsrv enable -srv1addr 192.168.100.100 -srv2
disable
Password: manager-password
Are you sure you want to set the audit logging information? (y/n [n]): y
The audit logging information has been set successfully.
%
```

Figure 5.8 Configuring the Syslog Output

```
% auauditlog -unit subsystem-name -refer
Password: manager-password
Syslog Server Transfer : Enable
  Server   IP Address
       1   Enable   192.168.100.100
       2   Disable  0.0.0.0
Internal Log : Enable
%
```

Figure 5.9 Verifying the Syslog Settings

5.3 Need section on enabling internal logging

5.4 Exporting the Internal Logged Data

Warning: This operation may affect host performance.

To export the internal logged data:

1. Execute the **auauditlog** command, as shown in Figure 5.10.

```
% auauditlog -unit subsystem-name -export
Password: manager-password
The internal log is exported to audit\syslog_75000100.txt.
Do you want to continue processing? (y/n [n]): y
Are you sure you want to export the internal log? (y/n [n]): y
The export of internal log may affect the host access. In some cases,
performance deterioration or time-out occurs.
Do you want to continue processing? (y/n [n]): y
The internal log has been exported successfully.
%
```

Figure 5.10 Exporting the Internal Logged Data

5.5 Initializing the Internal Logged Data

To export the internal logged data:

1. Execute the **auauditlog** command as shown in Figure 5.11.

```
% auauditlog -unit subsystem-name -init
Password: manager-password
Are you sure you want to initialize the internal log? (y/n [n]): y
If you initialize the internal log, all logs will be deleted. You cannot recover
 the deleted internal log. Please export internal log before this operation.
Are you sure you want to initialize the internal log? (y/n [n]): y
The internal log will be initialized.
Are you sure you want to execute? (y/n [n]): y
The internal log has been initialized successfully.
%
```

Figure 5.11 Initializing the Internal Logged Data

Chapter 6 Audit Log Format and Output

This chapter discusses the following topics:

- Audit Log messages (see section 6.1)
- Sample Syslog server log (see section 6.2)

6.1 Audit Log Messages

Table 6.1 shows the detailed log entries. In certain cases, no parameter is output, which is explained in the notes following the table. Rows with grey background shading refer to the logged data output of operations that can only be performed by your Hitachi Data Systems service representative.

Table 6.1 Audit Log Detailed Information

Code	Message	Explanation
31000100	Create LU[*1]	Creating a logical unit *1 LU number
31000200	Delete LU[*1]	Deleting a logical unit *1 LU number
31000300	Set CTL*1 as Default CTL for LU[*2]	Changing the default controller of current logical unit *1 Controller number *2 LU number
32000100	Set Drive Maintenance: Function=*1 <Location Unit[*2] HDU[*3]>	Setting of maintenance function of drive *1 Maintenance function of drive [Detach|DataReconstruction| CopyBack|DynamicSparing| SystemCopy *2 Unit number *3 HDU number
35000100	Set Auto Detach Condition: <WarningInfo OCCUR=*1 RECV=*2 STAT=*3 Mode=*4> <OnlineVerify=*5 SkipVerify=*6> <DriveResponseDiagnosis=*7 SATA=*8 Response=*9times> <AutoDiagnosisThreshold=*10>	Setting of warning report mode to the host *1 Report occurrence of warning to the host [Enable|Disable] *2 Report recovery of warning to the host [Enable|Disable] *3 Report over of statistics threshold to the host [Enable|Disable] *4 Warning Information Report Mode [Port|LogicalUnit] Setting of verify *5 Online Verify Test [Enable|Disable] *6 Skip Verify [ON|OFF] Setting of Drive Response Diagnosis *7 Drive Response Diagnosis (***Note 1***) [Disable|Enable(Output Message only)|Enable(Output Message and Dynamic Sparing)] *8 SATA Drive Diagnosis (***Note 1***) [ON|OFF] *9 Diagnosis Criterion (Difference in response time of each drive)

Code	Message	Explanation
		(***Note* 1**) [1.5|2|4|8] *10 Auto Diagnosis Threshold of back-end
36000100	Set Restore Options: Mode1=*1 Mode2=*2 Time=*3*10ms Size=*4*128blocks Sparing=*5 Operation=*6 NoCopyBackMode=*7	Setting of drive restoration options *1 Drive Restoration Mode [Background|Interleave(Normal)| Interleave(Prior)] *2 Drive Restoration [Manual|Auto] *3 Interval Time *4 Processing Unit Size *5 Dynamic Sparing [Execute(Read/Write & Online Verify)|Execute(Read/Write)| DoNotExecute] *6 Spare Drive Operation Mode [Variable|Fixed] *7 Applying No Copy Back Mode on All Units (***Note* 2**) [ON|OFF]
3A000100	Create RAID Group[*1]	Definition a RAID group *1 RAID group number
3A000200	Delete RAID Group[*1]	Deleting the RAID group *1 RAID group number
3A000300	Delete All RAID Groups	Deleting the all RAID group
3B000100	Set Threshold/LAN: <ThresholdErrors Mech[*1/*2] R/W[*3/*4] Drive I/F[*5/*6] CTL[*7/*8] SCSI_I/F[*9/*10]> <LAN CTL 11 IP=*12 Subnet=*13 Gateway=*14 DHCP=*15 AUTO_CHNG=*16 Negotiation=*17>	Setting the threshold value for preventive maintenance *1 Recovered mechanical errors *2 Un-recovered mechanical errors *3 Recovered Read/Write errors *4 Un-recovered Read/Write errors *5 Recovered Drive I/F errors *6 Un-recovered Drive I/F errors *7 Recovered Controller hard errors *8 Un-recovered Controller hard errors *9 Recovered SCSI I/F errors *10 Un-recovered SCSI I/F errors Setting the LAN information of user's management port (set with reboot) *11 Controller number *12 IP address *13 Subnet mask *14 Default gateway address *15 DHCP [ON|OFF] *16 Maintenance port IP address

Code	Message	Explanation
		automatic change mode [Enable|Disable] *17 Negotiation mode [Auto|10Mbps/Half|10Mbps/Full| 100Mbps/Half|100Mbps/Full]
3C000100	Modify Cache Residency settings: <CTL0=*1 LU[*2]> <CTL1=*1 LU[*2]>	Setting a Cache Residency LU *1 Residency Mode [Enable|Disable] *2 LU number (***Note* 3**)
3E030100	Set Boot Options: Startup=*1 Delay=*2 Detach=*3 VendorID=*4 ProductID=*5 ROM=*6 RAM=*7	Setting the Boot Options *1 System Startup Attribute [SingleMode|DualActiveMode] *2 Delay Planned Shutdown time *3 Drive Detach Mode [Enable|Disable] *4 Vendor ID *5 Product ID *6 ROM Micro program Version *7 RAM Micro program Version
3E060100	Set SNMP Information	Setting the SNMP information
3E0C0100	Login (Password Protection)	Logged in with Password Protection user ID
3E0C0200	Logout (Password Protection)	Log out already logged in with Password Protection user ID
3E0C0300	Reset UserID (Password Protection)	Clearing logged in status with Password Protection user ID
3E0C0400	Register UserID (Password Protection)	Registering a Password Protection user ID
3E0C0500	Delete UserID (Password Protection)	Deleting the Password Protection user ID
3E110100	Set Spare Drives: Unit[*1] HDU[*2]	Setting the spare drives *1 Unit number *2 HDU number
3E110200	Release Spare Drives: Unit[*1] HDU[*2]	Releasing the spare drives *1 Unit number *2 HDU number
3E130100	Set RTC [20YY/MM/DD hh:mm:ss]	Setting a RTC information (YY: year, MM: month, DD: day, hh: hour, mm: minute, ss: second)
3E140100	Set Fibre Channel: Port0A[*1 *2 *3] Port0B[1 *2 *3] Port1A[*1 *2 *3] Port1B[1 *2 *3]	Setting a Fibre channel information for AMS200/AMS500/WMS100 *1 Port address (3 bytes with hexadecimal) *2 Transfer rate (***Note* 4**) [1Gbps|2Gbps|4Gbps|Auto]

Code	Message	Explanation
		*3 Topology (***Note 4**) [PtoP|Loop]
3E140100	Set Fibre Channel: Port0A[*1 *2 *3] Port0B[1 *2 *3] Port0C[*1 *2 *3] Port0D[1 *2 *3] Port1A[*1 *2 *3] Port1B[1 *2 *3] Port1C[*1 *2 *3] Port1D[1 *2 *3]	Setting a Fibre channel information for AMS1000 *1 Port address (3 bytes with hexadecimal) *2 Transfer rate (***Note 4**) [1Gbps|2Gbps|4Gbps|Auto] *3 Topology (***Note 4**) [PtoP|Loop]
3E180100	Modify Port Options	Setting the Port options (Reset/LIP Mode (Signal), Reset/LIP Mode (Process), LIP Port All Reset Mode)
3E200100	Set Command Devices: <Device1 LU[*1] Protect=*2> <Device2 LU[*1] Protect=*2>	Setting the Command Devices *1 LU number (***Note 5**) *2 RAID Manager protect (***Note 5**)) [Enable|Disable]
3E200200	Release Command Devices: *1	Releasing the Command Devices *1 [Device1|Device2|all]
3E200300	Set RAID Manager Protect for Command Devices: Devices1=*1 Devices2=*1	Setting the RAID Manager Protect function *1 RAID Manager Protect (***Note 5**) [Enable|Disable]
3E220100	Unify MainLU[*1] and SubLU[*2]	Unifying LUs *1 MainLU number *2 SubLU number
3E220200	Separate SubLU from MainLU[*1]	Separating all unified LUs *1 MainLU number *2 SubLU number
3E220300	Separate SubLU[*1] from MainLU[*2] (Last LU Separation)	Separating the last LU from the unified LU (***Note 6**) *1 SubLU number *2 MainLU number
3E240100	Set Remote Path: SerialNumber=*1 TimeOut=*2sec <Path0 Local_Port*3 Remote_Port*4> <Path1 Local_Port*5 Remote_Port*6>	Setting a remote path information of TrueCopy *1 Partner's serial number *2 Time out *3 Local port number of Path0 *4 Remote port number of Path0 *5 Local port number of Path1 *6 Remote port number of Path1
3E240200	Delete Remote Path	Deleting the remote path information
3E350100	Set Host Group	Setting a host group information
3E390100	Set System Parameter/LAN Port Number: WN=*1 URES=*2 AUREC=*3 WTHR=*4 OWDIS=*5 SHAD_IO=*6 CACHEXE=*7	Setting the system parameters online

Code	Message	Explanation
	DETACH=*8 OP_FAIL=*9 Title=*10 CTL0_WV=*11 CTL1_WV=*12 CTL0_Port=*13 CTL1_Port=*14	*1 Turbo LU Warning [ON|OFF] *2 Write Unique Response Mode [ON|OFF] *3 Auto Reconstruction Mode [ON|OFF] *4 Forced Write Through Mode [ON|OFF] *5 LU Ownership Change Disable Mode [ON|OFF] *6 ShadowImage I/O Switch Mode [ON|OFF] *7 Synchronize Cache Execution Mode [ON|OFF] *8 Drive Detach Mode [ON|OFF] *9 Operation if the Processor failures Occurs [ResetTheFault| ShutdownTheSystem] *10 Web Title *11 CTL0 Write & Verify Execution Mode (***Note 7***) [ON|OFF] *12 CTL1 Write & Verify Execution Mode [ON|OFF] *13 CTL0 (***Note 7***) (LAN port number) *14 CTL1 (LAN port number)
3E3A0100	Set Tuning Parameter(System): Opportunity=*1% StopOpportunity=*2% Cache=*3 Trace=*4	Setting the system tuning parameters *1 Dirty Data Opportunity *2 Dirty Data Stop Opportunity *3 Cache Control Mode [FIFO|LRU] *4 Detailed Trace Mode [ON|OFF]
3E3A0200	Default Tuning Parameter(System)	Default setting of the system tuning parameters
3E3D0100	Set Data Pool: CTL*1 Threshold=*2% LU[*3]	Adding an LU to Data Pool *1 Controller number *2 Threshold value *3 LU number (***Note 8***)
3E3D0200	Delete All LUs from Data Pool(CTL*1)	Deleting the all LUs from Data Pool *1 Controller number
3E3E0100	Set Snapshot Image(P-VOL[*1]): LU[*2]	Creating Snapshot image of P-VOL *1 P-VOL number *2 LU number
3E3E0200	Delete Snapshot Image(P-VOL[*1]): LU[*2]	Deleting Snapshot image of P-VOL *1 P-VOL number

Code	Message	Explanation
		*2 LU number
3E3F0100	Set Data Retention: LU[*1] Attribute=*2 S-VOL=*3 Term=*4day(s)	Setting the access level of LU *1 LU number *2 Access level (attribute) [Read/Write|ReadOnly|Protect] *3 S-VOL [Enable|Disable] *4 Retention term (infinite: -)
3E3F0200	Set Data Retention: ExpirationLock=*1	Setting the Expiration Lock *1 Expiration Lock [ON|OFF]
3E410100	Set Performance Statistics: Port=*1 RG_LU=*2 Cache=*3 PRO=*4 DR=*5 DR_OP=*6 Back=*7	Setting the collection of performance statistics *1 Port Information [ON|OFF] *2 RAID Group/Logical Unit Information [ON|OFF] *3 Cache Information [ON|OFF] *4 Processor Information [ON|OFF] *5 Drive Information [ON|OFF] *6 Drive Operating Information [ON|OFF] *7 Back-end Information [ON|OFF]
3E460100	Format LU[*1]	Formatting of a LU *1 LU number
3E460200	Set Format Mode: Priority=*1 FormatData=*2	Setting the format mode *1 Format priority mode (***Note* 9**) [Normal|Host|Format] *2 Format data (***Note* 9**) [Default|0]
3E480100	Change SATA Options: <Sweep=*1 Interval=*2*10min Suspend=*3sec Unload=*4 OnlineVerifyRestriction=*5> <SMART=*6 Threshold=*7%>	Setting the SATA drive options *1 Sweep function [Enable|Disable] *2 Interval time (***Note* 3**) *3 Suspended Time (***Note* 3**) *4 Unload (***Note* 3**) [Enable|Disable] *5 Online verify restriction (***Note* 3**) [Enable|Disable] *6 SMART function [Enable|Disable] *7 Threshold of reassign mount (***Note* 10**)
3E490100	Set SATA Restore Options: CorrectionCopyMount=*1time(s)	Setting the SATA drive restore options *1 Correction Copy Mount
3E4A0100	Set Remote Path(System Upgrade): SerialNumber=*1	Setting a partner's serial number of TrueCopy *1 Partner's serial number

Code	Message	Explanation
3E4B0100	Start Parity Correction: LU[*1]	Specifying starting of parity correction *1 LU number
3E3B0200	Skip Parity Correction: LU[*1]	Specifying skip of parity correction *1 LU number
3E4B0300	Cancel Parity Correction: LU[*1]	Specifying stop of parity correction *1 LU number
3E520100	Change LU Mapping Guard	Changing of the mapping guard setting
3E550100	Install: *1	Installing the priced option *1 The priced option name
3E550200	De-install: *1	Uninstalling the priced option *1 The priced option name
3E550300	Enable: *1	Validation of a priced option *1 The priced option name
3E550400	Disable: *1	Invalidation of a priced option *1 The priced option name
3E570100	*1 ENC Micro Automatic Download	Setting the Automatic Download of ENC Micro program *1 [Enable|Disable]
3E620100	Set DM-LU: LU[*1]	Setting the DM-LU *1 LU number
3E620200	Release DM-LU: LU[*1]	Releasing the DM-LU *1 LU number
3E630100	Set Cache Partition	Registering the Cache Partition information
3E640100	Assign Cache Partition LU	Registering the LU to the Cache Partition assignment
3E670100	Set LU Mapping/ Mapping Mode	Setting the mapping information of LU (per host group)
3E6C0100	Default Tuning Parameter(Multi Stream/Prefetch)	Default setting of the multi stream tuning parameters
3E6C0200	Set Tuning Parameter(Multi Stream/Prefetch)	Setting the multi stream tuning parameters
3E710100	Set Maintenance LAN: CTL0 IP=*1	Setting the IP address of maintenance port *1 IP address
3E740100	Set NAS System LU	Setting the NAS System LUs
3E740200	Set NAS User LU	Setting the NAS User LUs
3E750100	Set LAN: <CTL0 IP=*1 Subnet=*2 Gateway=*3 Negotiation=*4> <CTL1 IP=*1 Subnet=*2 Gateway=*3 Negotiation=*4>	Setting the LAN information of user's management port (set now without reboot) (***Note* 11**)

Code	Message	Explanation
	AUTO_CHNG=*5	*1 IP address *2 Subnet mask *3 Default gateway address *4 Negotiation mode [Auto|10Mbps/Half|10Mbps/Full|100Mbps/Half|100Mbps/Full] *5 Maintenance port IP address automatic change mode [Enable|Disable]
3E760100	Set LAN Information: <CTL0 IP=*1 Subnet=*2 Gateway=*3 Negotiation=*4> <CTL1 IP=*1 Subnet=*2 Gateway=*3 Negotiation=*4> AUTO_CHNG=*5	Setting the LAN information of user's management port by the constitution file (***Note* 11**) *1 IP address *2 Subnet mask *3 Default gateway address *4 Negotiation mode [Auto|10Mbps/Half|10Mbps/Full|100Mbps/Half|100Mbps/Full] *5 Maintenance port IP address automatic change mode [Enable|Disable]
3E830100	Change Host Group Security/ WWN information	Setting the host group security mode enable or disable/setting the WWN information
3E8D0100	Set iSCSI Port: <Port0A IP=*1 Subnet=*2 Gateway=*3 Port=*4*5sec> <Port0B IP=*1 Subnet=*2 Gateway=*3 Port=*4*5sec> <Port1A IP=*1 Subnet=*2 Gateway=*3 Port=*4*5sec> <Port1B IP=*1 Subnet=*2 Gateway=*3 Port=*4*5sec>	Setting the LAN information of iSCSI ports (***Note* 12**) *1 IP address *2 Subnet mask *3 Default gateway address *4 Port number of TCP/IP *5 Keep Alive time
3E8E0100	Change CHAP User Settings: Port*1	Setting the iSCSI CHAP User information *1 Port number [0A|0B|1A|1B]
3E900100	Set Target Information(iSCSI): Port*1	Setting the iSCSI target information *1 Port number [0A|0B|1A|1B]
3E910100	Set iSNS Server: <Port0A Server=*1 IP=*2 Port=*3> <Port0B Server=*1 IP=*2 Port=*3> <Port1A Server=*1 IP=*2 Port=*3> <Port1B Server=*1 IP=*2 Port=*3>	Setting the iSNS server information (***Note* 12**) *1 Whether to use the iSNS server or not [ON|OFF] *2 IP address (***Note* 13**) *3 Port number of TCP/IP (***Note* 13**)
3E920100	Send Ping	Sending ping
3E930100	Set Initiator Information(iSCSI): Port*1	Setting the iSCSI initiator information *1 Port number [0A|0B|1A|1B]

Code	Message	Explanation
3E940100	Modify Port Options	Setting the port options by the constitution file
3E950100	Set LU Mapping	Setting the mapping information of LUs or batch setting the mapping information of LUs per port (by the constitution file)
3E970100	Start Volume Migration: P-VOL[*1] S-VOL[*2] CopyPace=*3	Starting Volume Migration *1 P-VOL number *2 S-VOL number *3 Copy pace [Prior|Normal|Slow]
3E970200	Cancel Volume Migration: P-VOL[*1] S-VOL[*2]	Terminating Volume Migration *1 P-VOL number *2 S-VOL number
3E970300	Split the Pair (Volume Migration): P-VOL[*1] S-VOL[*2]	Releasing a pair of Volume Migration *1 P-VOL number *2 S-VOL number
3E970400	Change Copy Pace for Volume Migration: CopyPace=*1 P-VOL[*2] S-VOL[*3]	Changing a copy pace *1 Copy pace [Prior|Normal|Slow] *2 P-VOL number *3 S-VOL number
3E980100	*1 Reserve LU for Volume Migration: LU[*2]	Defining or releasing reserved LU for Volume Migration *1 [Add|Delete] *2 Reserved LU number
3EB00100	Set TimeZone=[*1] DaylightSaving=*2 NTP1=*3 NTP2=*4	Setting the time zone and NTP server *1 Time zone *2 Daylight saving [Enable|Disable] *3 NTP Server 1 [Enable|Disable] *4 NTP Server 2 [Enable|Disable]
3EB10100	Set NNC LAN: <NNC*1 IP=*2 Subnet=*3 MTU=*4 Negotiation=*5> <NNC*1 IP=*2 Subnet=*3 MTU=*4 Negotiation=*5>	Setting NNC LAN information (***Note* 14**) *1 NNC number *2 IP address *3 Subnet mask *4 MTU *5 Negotiation mode [Auto|100Mbps/Half| 100Mbps/Full|1000Mbps/Full]
3EB20100	Set Audit Log Options: Transfer=*1 Server1_IP=*2 Server2_IP=*3 Internal=*4	Setting the Audit Logging options *1 Whether to transfer to the syslog server or not [ON|OFF] *2 IP address of syslog server 1

Code	Message	Explanation
		(***Note* 13**) *3 IP address of syslog server 2 (***Notes* 13, 15**) *4 Internal log [Enable|Disable]
3EB30100	Export Internal Log (*1 file(s) completed)	Exporting the Audit logged files *1 Exported logged files number
3EB40100	Initialize Internal Log	Initializing the Audit logged data
3EB60100	*1 User Account	Setting the Account Authentication information *1 [Add|Delete|Modify]
3EB70100	Login (Account Authentication)	Logged in with Account Authentication user ID
3EB70200	Logout (Account Authentication)	Log out already logged in with Account Authentication user ID
3EB70300	Force Logout of *1 (Account Authentication)	Forced log out already logged in with Account Authentication user ID *1 Forced log out user ID
3EB70400	Start SNM Alert Monitoring	Starting error monitoring
3EBB0100	Spin Up RAID Group[*1]	Setting spin up *1 RAID group number
3EBB0200	Spin Down RAID Group[*1]	Setting spin down *1 RAID group number
3EC10100	Set TrueCopy Options: CycleTime=*1sec	Setting a cycle time for TrueCopy Extended Distance *1 Cycle time
3EC10200	Initialize TrueCopy Options	Initializing the setting information of TrueCopy Extended Distance
3EC40100	Set NNC Upgrade: BackupSystemLU=1* NNC=*2	Setting NNC upgrading *1 Setting system LU [Restore|Backup|Clear] *2 NNC number [0|1|2|3|0/2|1/3]
3F010100	Configuration failed: Inappropriate parameters	Configuration failed for inappropriate parameters
3F020100	Configuration failed: The Option[*1] is Disable or De-installed	Configuration failed for the priced option is disable or uninstalled (***Note* 16**) *1 The priced option name
3F030100	Configuration failed: Temporary/Emergency Key[*1] expired	Configuration failed for the temporary or emergency key is expired (***Note* 16**) *1 The priced option name
41040100	Session Timeout: *1	Session timeout occurs of the already logged in with Account

Code	Message	Explanation
		Authentication user ID *1 User ID
41090100	Reference/Modification failed: Authentication authority is insufficient	Referencing or modification failed for Authentication authority is insufficient
51010100	Start Online Microprogram Download	Starting the micro program downloading online
51010200	Start Online Microprogram Update: CTL*1	Starting the micro program updating online *1 Controller number
51020100	Start ENC Microprogram Download	Starting ENC micro program downloading online
51020200	Start ENC Microprogram Update: ENC*1	Starting ENC micro program updating online *1 ENC number
51030100	System Reboot	Rebooting after the system configuration
51030200	Release Reboot Wait Condition: CTL*1	Releasing reboot wait condition *1 Controller number
52010100	System Shutdown (Reboot Request)	Reboot request from Storage Navigator
71010100	Subsystem is Ready	Subsystem is ready
71020100	PS OFF	Subsystem power off

Note 1: If this is **Disable**, **#** is output.
Note 2: When the *6 is **Fixed**, **#** is output.
Note 3: When the *1 is **Disable**, # is output.
Note 4: When the *1 is invalid, # is output.
Note 5: When only one command device is set, # is output for the other one.
Note 6: When the MainLU value is invalid, # is output for the SubLU.
Note 7: If there is only one CTL, # is output.
Note 8: If only the *1 and *2 are set, # is output.
Note 9: If only one parameter is set, # is output for the other one.
Note 10: If *6 is **Disable**, # is output.
Note 11: If there is only one CTL, # is output for all the parameters on the CTL1 side.
Note 12: If there is only one CTL # is output for all the parameters on the Port 1A/1B side.
Note 13: When *1 is **OFF**, # is output.
Note 14: If there is only one CTL, # is output for all parameters for the other NNC.
Note 15: When the *1 is **ON** and the server 2 is not set, # is output.
Note 16: When the remote path or the pool LU is set, two abbreviations of the priced options may be output.

6.2 Sample Syslog Server Log

The following example illustrates a case where the Syslog server is set to receive the audit log from the subsystem using the Linux syslogd command.

1. Edit the "/etc/syslog.conf" file, and specify the file name to be output in the Audit log (see Figure 6.1
2. Set syslogd to accept log transfer from the outside by editing the "/etc/sysconfig/syslog" file to add –r to "SYSLOGD_OPTIONS" (see Figure 6.2).
3. Restart syslogd after setting (see Figure 6.3).

```
# Audit Logging
user.*          /var/log/Audit_logging.log
```

Figure 6.1 Specifying the Output Location

```
# SYSLOGD_OPTIONS="-r –m 0"
```

Figure 6.2 Setting the Syslog to Accept Outside Transfer

```
# service syslog restart
```

Figure 6.3 Restarting Syslogd

Chapter 7 Troubleshooting

This chapter discusses the following topics:

- General troubleshooting (see section 7.1)
- Contacting the Hitachi Data Systems Support Center (see section 7.2)

7.1 General Troubleshooting Tips

The user is responsible for operation and normal maintenance of the computer(s) that host Storage Navigator software. Following are guidelines for troubleshooting Storage Navigator software operations:

- **Check the cabling and the LAN.** Verify that both the computer and LAN cabling are firmly attached, and that the LAN is operating properly.
- **Reboot the computer.** Close any programs that are not responding. If necessary, reboot the computer.
- If Storage Navigator does not succeed in connecting to the array unit, the following message may display:

  An invalid response was received from the subsystem

  This indicates that Storage Navigator may have been connected to the array unit while the array unit automatically rebooted. Connect to the array unit again after approximately three minutes.
- Storage Navigator may hang up in the following cases:
  - The communication with the connected array unit fails due to controller blockage, array unit failure, or disconnected LAN connection, etc., or the array unit receives a Reset/LIP from the host.
  - Other applications are working concurrently and memory utilization or a CPU use rate is high.
- If Storage Navigator hangs up, terminate it forcibly and check the array unit status and the connection status of the LAN. Reboot Storage Navigator once again.
- The Storage Navigator can open multiple **Array System Viewer** windows for one array unit. When multiple **Array System Viewer** windows are open, a shortage of memory may occur, depending on the configuration of the system in which the Storage Navigator has been installed; this results in program hang-ups. When opening **Array System Viewer** windows, open only one window to operate an array unit.

7.2 Calling the Hitachi Data Systems Support Center

If you need to call the Hitachi Data Systems Support Center, make sure you can provide as much information about the problem as possible. Include the circumstances surrounding the error or failure, the Storage Navigator configuration information, and the exact content of messages displayed on the Storage Navigator.

The Hitachi Data Systems customer support staff is available 24 hours a day, 7 days a week. If you need technical support, please call:

- United States: (800) 446-0744
- Outside the United States: (858) 547-4526

Acronyms and Abbreviations

Acronym	Expansion
A	Ampere
AL-PA	arbitrated loop-physical address
AMS	Adaptable Modular Storage
API	application programming interface
ASTM	American Society for Testing Materials
ATA	Advanced Technology Attachment standard
ATM	asynchronous transfer mode
BC	business continuity
BS	Basic (power) supply
BSA	bus adapter
BTU	British thermal unit
CCI	command control interface
CEC	Canadian Electroacoustic Community
CFW	cache fast write
CHAP	challenge handshake authentication protocol
CIFS	common internet file system
CKD	count-key data
CLI	command line interface
CSA	Canadian Standards Association
CSV	comma separated value
CTG	consistency group
CTL	controller
CU	controller unit
CUDG	control unit diagnosis
dB(A)	decibel (A-weighted)
D-CNT	default (owner) controller
DAMP	Disk Array Management Program
DDL	data definition language
DHCP	dynamic host configuration protocol
DKC	disk controller unit
DLM	data lifecycle management
DM-LU	differential management logical unit
DRAM	dynamic random access memory
DWDM	dense wavelength division multiplexer
EMI	electromagnetic interference
EPO	emergency power-off
FC	fibre channel
FC-AL	fibre channel-arbitrated loop
FCC	Federal Communications Commission
FCP	fibre-channel protocol

Gbps	gigabit per second
HA	high availability
HACMP	high availability cluster multi-processing
HBA	host bus adapter
HDLM	Hitachi Dynamic Link Manager
HORCM	Hitachi Open Remote Copy Manager
H-LUN	host logical unit
H-RAIN	heterogeneous redundant array of independent nodes
HSN	hierarchical star network
HWM	high water mark
IDE	integrated drive electronics; see also ATA.
IIS	Internet Information Service
IOPS	input output operations per second
IOS	internet work operating system
iSCSI	internet small computer system interface
JRE	Java 2 runtime environment
LCP	local control port
LD	logical device
LDEV	logical device
LDM	logical device manager
LIP	loop initialization primitive
LRU	least recently used
LUN	logical unit number
LUSE	LU size expansion
LVI	logical volume image
LVM	logical volume manager
MCU	main control unit
NDMP	Network Data Management Protocol
MDB	master directory block
MIB	message information block
μP	microprocessor
MR	magneto-resistive
MU	mirror unit
MVS	multiple virtual storage
MVS/ESA	multiple virtual storage /enterprise systems architecture
MVS/XA	multiple virtual storage /extended architecture
NAS	network attached storage
NBU	NetBackup (a Symantec product)
NEC	National Electrical Code
NFS	network file system
NIC	network interface card
NIS	network information service
NNC	network node controller
NSC	network storage controller

NTP	network time protocol
NVS	nonvolatile storage
OCI	Oracle Call Interface
ODM	object data manager
OFC	open fibre control
ORM	online read margin
OSI	open systems interconnection
PCI	power control interface
PDL	product documentation library
PFUS	pool full status
POSIX	portable operating system interface
PPRC	peer-to-peer remote copy
PSUE	pair suspended-error status
PSUS	pair suspended-split
PSUS(N)	pair suspended – not restored status
PV	physical volume
P-VOL	primary volume
RAID	redundant array of independent disks
RC	reference code
RCU	remote control unit
RPO	recovery point objective
RTC	real-time clock
RTO	recovery time objective
SAN	storage-area network
SATA	serial ATA
SCSI	small computer system interface
SIM	service information message
SM	shared memory module
SMB	server message block
SMTP	simple mail transfer protocol
SNIA	Storage Networking Industry Association
SNMP	simple network management protocol
SONET	synchronous optical network
SSL	secure socket layer
SSWS	suspend for swapping S-VOL
S-VOL	secondary volume
TID	target identifier
TPOF	tolerable points of failure
UDP	user diagram protocol
UL	Underwriters' Laboratories
USP	Universal Storage Platform
VCS	Veritas Cluster Server™
VDE	Verband Deutscher Elektrotechniker
VIB	volume information block

VOLID	volume identifier
V-VOL	virtual volume (Snapshot Image)
VxVM	Veritas Volume Manager
WDM	wavelength division multiplexing

Index