HITACHI
Inspire the Next

Hitachi Compute Blade Series
Hitachi Compute Rack Series

Server installation and monitoring tool User's Guide log monitoring functions

FastFind Links

Getting Help

Contents

Hitachi Data Systems

MK-99COM064-02

Contents

Preface

This document provides information on Server installation and monitoring tool User's Guide log monitoring function for Compute Blade and Compute Rack. Please read this document carefully, and maintain a copy for reference.

This preface includes the following information:

Notice: The use of the Compute Blade, Compute Rack, and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems

Intended Audience

This document is intended for the personnel who are involved in planning, managing, and performing the tasks to prepare your site for Compute Blade and Compute Rack installation and to install the same.

This document assumes the following:

- The reader has a background in hardware installation of computer systems.
- The reader is familiar with the location where the Compute Blade or Compute Rack will be installed, including knowledge of physical characteristics, power systems and specifications, and environmental specifications.

Release Notes

Release notes contain requirements and more recent product information that may not be fully described in this manual. Be sure to review the release notes before installation.

Abbreviations of Operating Systems

This section describes abbreviations of operating systems used in this manual.

- Microsoft® Windows Server® 2012 R2, Datacenter Edition
  (Hereinafter, referred to as Windows Server 2012 R2, Datacenter Edition; Windows Server 2012 R2)
- Microsoft® Windows Server® 2012 R2, Standard Edition
  (Hereinafter, referred to as Windows Server 2012 R2, Standard Edition; Windows Server 2012 R2)
- Microsoft(R) Windows Server(R) 2012, Datacenter Edition
  (Hereinafter, referred to as Windows Server 2012, Datacenter Edition; Windows Server 2012)
- Microsoft(R) Windows Server(R) 2012, Standard Edition
  (Hereinafter, referred to as Windows Server 2012, Standard Edition; Windows Server 2012)
- Microsoft(R) Windows Server(R) 2008 R2 Datacenter x64 Edition
  (Hereinafter, referred to as Windows Server 2008 R2, Datacenter x64 Edition; Windows Server 2008 R2 x64 Editions; Windows Server 2008 R2)
- Microsoft(R) Windows Server(R) 2008 R2 Standard x64 Edition
  (Hereinafter, referred to as Windows Server 2008 R2, Standard x64 Edition; Windows Server 2008 R2 x64 Editions; Windows Server 2008 R2)
- Microsoft(R) Windows Server(R) 2008 R2 Enterprise x64 Edition
  (Hereinafter, referred to as Windows Server 2008 R2, Enterprise x64 Edition; Windows Server 2008 R2 x64 Editions; Windows Server 2008 R2)
- Microsoft(R) Windows Server(R) 2008 Datacenter
  (Hereinafter, referred to as Windows Server 2008 Datacenter; Windows Server 2008; Windows)
- Microsoft(R) Windows Server(R) 2008 Standard
  (Hereinafter, referred to as Windows Server 2008 Standard; Windows Server 2008; Windows)
- Microsoft(R) Windows Server(R) 2008 Enterprise
  (Hereinafter, referred to as Windows Server 2008 Enterprise; Windows Server 2008; Windows)
- Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V™
  (Hereinafter, referred to as Windows Server 2008 Datacenter without Hyper-V; Windows Server 2008 Datacenter; Windows Server 2008; Windows)
- Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V™
  (Hereinafter, referred to as Windows Server 2008 Standard without Hyper-V; Windows Server 2008 Standard; Windows Server 2008; Windows)

- Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V™
  (Hereinafter, referred to as Windows Server 2008 Enterprise without Hyper-V; Windows Server 2008 Enterprise; Windows Server 2008; Windows)
- Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
  (Hereinafter, referred to as Windows Server 2003 R2, Standard x64 Edition; Windows Server 2003 R2 x64 Editions; Windows Server 2003 R2)
- Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
  (Hereinafter, referred to as Windows Server 2003 R2, Enterprise x64 Edition; Windows Server 2003 R2 x64 Editions; Windows Server 2003 R2)
- Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
  (Hereinafter, referred to as Windows Server 2003 R2, Standard Edition; Windows Server 2003 R2 (32-bit); Windows Server 2003, R2)
- Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
  (Hereinafter, referred to as Windows Server 2003 R2, Enterprise Edition; Windows Server 2003 R2 (32-bit); Windows Server 2003, R2)
- Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
  (Hereinafter, referred to as Windows Server 2003, Standard x64 Edition; Windows Server 2003 x64 Editions; Windows Server 2003; Windows)
- Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
  (Hereinafter, referred to as Windows Server 2003, Enterprise x64 Edition; Windows Server 2003 x64 Editions; Windows Server 2003; Windows)
- Microsoft(R) Windows Server(R) 2003, Standard Edition
  (Hereinafter, referred to as Windows Server 2003, Standard Editio; Windows Server 2003 (32-bit); Windows Server 2003; Windows)
- Microsoft(R) Windows Server(R) 2003, Enterprise Edition
  (Hereinafter, referred to as Windows Server 2003, Enterprise Edition; Windows Server 2003 (32-bit); Windows Server 2003; Windows)
- Red Hat Enterprise Linux Server 6.2
  (Hereinafter, referred to as Red Hat Enterprise Linux Server 6.2, Red Hat Enterprise Linux 6, or Linux)
- Red Hat Enterprise Linux Server 6.4
  (Hereinafter, referred to as Red Hat Enterprise Linux Server 6.4, Red Hat Enterprise Linux 6, or Linux)
- Red Hat Enterprise Linux 5.9
  (Hereinafter, referred to as Red Hat Enterprise Linux 5.9, Red Hat Enterprise Linux 5, or Linux)
- Red Hat Enterprise Linux 5.7
  (Hereinafter, referred to as Red Hat Enterprise Linux 5.7, Red Hat Enterprise Linux 5, or Linux)
- Red Hat Enterprise Linux 5.6
  (Hereinafter, referred to as Red Hat Enterprise Linux 5.6, Red Hat Enterprise Linux 5, or Linux)

- Red Hat Enterprise Linux 5.4
  (Hereinafter, referred to as Red Hat Enterprise Linux 5.4, Red Hat Enterprise Linux 5, or Linux)
- Red Hat Enterprise Linux 5.3
  (Hereinafter, referred to as Red Hat Enterprise Linux 5.3, Red Hat Enterprise Linux 5, or Linux)
- Red Hat Enterprise Linux 5.1
  (Hereinafter, referred to as Red Hat Enterprise Linux 5.1, Red Hat Enterprise Linux 5, or Linux)
- Red Hat Enterprise Linux 4.7
  (Hereinafter, referred to as Red Hat Enterprise Linux 4.7, Red Hat Enterprise Linux 4, or Linux)
- Red Hat Enterprise Linux 4.5
  (Hereinafter, referred to as Red Hat Enterprise Linux 4.5, Red Hat Enterprise Linux 4, or Linux)
- VMware vSphere® ESXi™ 5.5
  (Hereinafter, referred to as VMware vSphere ESXi 5.5, VMware vSphere ESXi, VMware vSphere 5.5, VMware vSphere 5, or VMware)
- VMware vSphere® ESXi™ 5.1
  (Hereinafter, referred to as VMware vSphere ESXi 5.1, VMware vSphere ESXi, VMware vSphere 5.1, VMware vSphere 5, or VMware)
- VMware vSphere® ESXi™ 5.0
  (Hereinafter, referred to as VMware vSphere ESXi 5.0, VMware vSphere ESXi, VMware vSphere 5.0, VMware vSphere 5,or VMware)
- VMware vSphere® ESX® 4.1
  (Hereinafter, referred to as VMware vSphere ESX 4.1, VMware vSphere ESX, VMware vSphere 4.1, VMware vSphere 4, or VMware)
- VMware vSphere® ESX® 4.0
  (Hereinafter, referred to as VMware vSphere ESX 4.0, VMware vSphere ESX, VMware vSphere 4.0, VMware vSphere 4, or VMware)

Document Conventions

This term "Compute Blade" refers to all the models of the Compute Blade; the term "Compute Rack" refers to CR 210 and CR 220; unless otherwise noted.

The Hitachi Virtualization Manager (HVM) name has been changed to Hitachi logical partitioning manager (LPAR manager, or LP). If you are using HVM based logical partitioning feature, substitute references to Hitachi logical partitioning manager (LPAR manager, or LP) with HVM.

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: copy *source-file target-file* ***Note:*** Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or entered by the user. Example: `# pairdisplay -g oradb`
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `# pairdisplay -g <group>` ***Note:*** Italic font is also used to indicate variables.
[ ] 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.
underline	Indicates the default value. Example: [a | b]

Getting Help

If you purchased this product from an authorized HDS reseller, contact that reseller for support. For the name of your nearest HDS authorized reseller, refer to the HDS support web site for locations and contact information. To contact the Hitachi Data Systems Support Center, please visit the HDS website for current telephone numbers and other contact information: http://support.hds.com.

Before calling the Hitachi Data Systems Support Center, please provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The exact content of any error message(s) displayed on the host system(s).

Technical Information and Update Program

It is recommended that you apply the latest drivers, utilities, BIOS, and firmware for using the system unit safely. For the latest version of update programs, contact your reseller.

When maintenance personnel change components due to some failure, basically the latest version of BIOS and firmware are applied to the newly installed components. BIOS and firmware may be updated for not-replaced components in maintenance work.

Comments

Please send us your comments on this document: doc.comments@hds.com. Include the document title, number, and revision, and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Data Systems Corporation. **Thank you!**

Safety guidelines

Safety guidelines include warnings and important safety guidelines for using utilities for Hitachi Compute Rack series and Hitachi Compute Blade series. Read and understand the following information before using utilities.

- ☐ Safety information
- ☐ Common precautions concerning safety
- ☐ Precautions against damage to equipment

Safety information

This document uses the following symbols to emphasize certain information.

Symbol	Label	Description
	WARNING	This indicates the presence of a potential risk that might cause death or severe injury.
	CAUTION	This indicates the presence of a potential risk that might cause relatively mild or moderate injury.
NOTICE	NOTICE	This indicates the presence of a potential risk that might cause severe damage to the equipment and/or damage to surrounding properties.
	Note	This indicates notes not directly related to injury or severe damage to equipment.
	Tip	This indicates advice on how to make the best use of the equipment.
	General Mandatory Sign	This indicates a general action to take. Action by following the instructions in this guide.

Common precautions concerning safety

Please carefully read through these safety instructions to follow:

- When operating the equipment, follow the instructions and procedures provided in the manual.
- Be sure to follow notes, cautionary statements and advice indicated on the equipment or in the manual.
- Referring to manuals attached to other products which you install in the equipment, follow the instructions described in those manuals.

Failure to follow those instructions can cause the system unit to fail or data to be corrupted.

Precautions against damage to equipment

Installation

Use this product with a system unit supporting this product. If you install this product on a system other than that, failure may occur due to the specification difference. See your system unit manual to find whether your system support this product or not.

1

Log monitor overview

This chapter describes about the functional overview of log monitor function. (hereinafter describes log monitor)(Previous name : Hardware Maintenance Agent)

Overview

Log monitor can collect maintenance information and can analyze hardware problems through the log data on the OS, and then generate the failure event code (based upon IPMI-SEL format).
The generated event code is stored in the management module (Compute Blade : in SVP, Compute Rack : in BMC), and is used for grasp of a phenomenon, and for pointing out of the failure part at maintenance.

By introducing log monitor, quick failure restoration is available and system availability improves.

Functions

This section explains the log monitor function.

Collecting and analyzing the failure information and maintenance information

Log monitor watches the OS log (Windows: event log, Linux:syslog), and generating the failure event code when the failure event is detected.
On Compute Rack series, it watches not only the OS log but also the system event log of the system unit (SEL).

Storing the failure event code in the management module

Log monitor stores the generated failure event code in the management module when the failure happens.
Therefore the failure event can be checked without starting customer's OS.

Generating the failure analysis result code (RC) (on only Compute Rack series)

On Compute Rack series, the failure analysis result code (RC) is generated based on the failure event code and the system event log (SEL) of the system unit.
The failure analysis result code is used for grasp of a phenomenon, and for pointing out of the failure part at maintenance.
On Compute Blade series, the management module generates the failure analysis result code.

Transferring the log to the management module (for only CB500)

On CB500, log monitor can receive the request of the log transfer from the management module and then transfer the log information of OS to the management module.

Supported Products

Log monitor supports following products.

Series	Model
Hitachi Compute Blade	CB500 CB2000
Hitachi Compute Rack	CR220HM, CR210HM, CR220SM

Supported OS/Virtual Environment

Supported OS

Log monitor supports following OS's.
However, it is precondition that the system unit supports the OS.

[Windows] (Both 32-bit and 64-bit are supported)
- Windows Server 2012R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003

[Linux] (Both 32-bit and 64-bit are supported)
- Red Hat Enterprise Linux Server 6.4
- Red Hat Enterprise Linux Server 6.2
- Red Hat Enterprise Linux Server 6.1
- Red Hat Enterprise Linux 5.9
- Red Hat Enterprise Linux 5.7
- Red Hat Enterprise Linux 5.6
- Red Hat Enterprise Linux 5.4
- Red Hat Enterprise Linux 5.3
- Red Hat Enterprise Linux 5.1
- Red Hat Enterprise Linux 4.7
- Red Hat Enterprise Linux 4.5

Supported virtual environment

Following virtual environments is supported.
However, it is precondition that the system unit supports the OS.

Virtual environment		Support (V : supported, - : unsupported)	
	Installed place (*1)	Compute Blade	Compute Rack
VMware vSphere 5.5 VMware vSphere 5.1 VMware vSphere 5.0	Guest OS	- (*2)	V (*2)(*3)
VMware vSphere 4.1 VMware vSphere 4.0	Guest OS	-	V
Windows Hyper-V	Host OS	V	V
LPAR manager	Guest OS	V	-

*1 : The supported guest OS and host OS are same as "Supported OS".

*2 : Supported by the other tool of log monitor VMware vMA(vSphere Management Assistant) edition.

*3 : To use the log monitor VMware vMA edition is recommended..

[Note for Compute Rack about the guest OS (for watching the failure) on VMware]

- Install the log monitor and the required software on the guest OS.
- Connect the management LAN port on the system and the LAN port on the guest OS for watching the failure by physical network.
  The connection is necessary to manage the system event log (SEL) of the system unit from the guest OS.
  For details, refer to SEL Manager Instruction Manual
- One guest OS for watching the failure can watch only one system unit.
  When the VMware environment is build by plural systems, the guest OS's for watching the failure are needed by the number of system units.

Please use the log monitor VMware vMA(vSphere Management Assistant) edition for VMware vSphere 5
Log monitor VMware vMA edition can detect more failure than Log monitor on guest OS by watching the hypervisor messages.

Required Resources

Log monitor is resident type application. The standards of required resources, when Log monitor detects the failure at the time of idling, are shown below.

Requirement	Idling	Detecting failure
CPU Utilization	1% and below	Approx. 10 - 30%
Memory Consumption	Approx. 7MB	Approx. 15MB
Disk Capacity (*1)	Approx. 7MB	Approx 200MB

(*1) About install folder of log monitor, refer to"Appendix. Install folder organization".

Following services are resident by log monitor

OS	Service	Residence process
Windows	SMAL2_MainteAgtSvc	C:\Program Files\HITACHI\miacat\Program\SMAL2Svc.exe C:\Program Files\HITACHI\miacat\Program\SMAL2MASvc.exe (For Compute Rack, the directory is "C:\Program Files(x86)" on x64 environment)
Linux	smal2d	/opt/hitachi/miacat/Program/SMAL2MASvc

Log monitor uses following ports.

Port	Service	Description
23141/tcp	core-linux	Communication port of the reporting device(SVP for Compute Blade)
31100/tcp	smal2_mainteregagt_port	Internal communication of the program for the log monitor
31101/tcp	smal2_mainteagt_port	Internal communication of the program for the log monitor

When above ports have already used by other processes, port number can be changed by editing services file (*1).
(*1) Windows : C:\WINDOWS\system32\drivers\etc\services
Linux:/etc/services

It is necessary to release the port used by log monitor, when the port is restricted by firewall function.

Required Software

Required software for log monitor is follows.

- System event (SEL) management tool
- Internal RAID management tool
- syslog service (Linux only)
- Library for 32bit environment application (for Compute Rack Linux x86_64 only)

System event (SEL) management tool

In order to manage the system event and to register the failure event code in the management module, the following software needs to be installed. The software is attached the system unit.

v: necessary, -: unnecessary

Software	Compute Blade		Compute Rack			
					VMware	
	Windows	Linux	Windows	Linux	Windows	Linux
SelManager	-	-	v (either)	v (either)	v	v
ServerConductor/Agent	v (either)	v (either)			-	-
IPMI service(OS standard) [Windows] IPMI Driver (OS standard) [RHEL 5.x] OpenIPMI package(RPM) OpenIPMI-tool package(RPM) [RHEL 6.x] OpenIPMI package(RPM) ipmitool package(RPM)			-	v (Only when Sel-Manager is used)	-	-

Install the SelManager on the guest OS in VMware environment
It is necessary to connect the maintenance LAN port of the system with guest OS by physical network, and to set the communication settings. (Because SelManager manages the system event log (SEL) of the system unit.)
For details, refer to SelManager Instruction Manual.

Internal RAID management tool

In order to detect failure of the Internal RAID, the following software needs to be installed. (However unnecessary in VMware environment)
The software is attached the system unit.

- Internal storage monitor
- MegaRAID Storage Manager

syslog service (Linux only)

Log monitor supports only following format of the syslog service which is installed by default.

- Standard format of syslogd
```
Oct 31 00:00:00 localhost AppName[1234]: Message text ...
```
- Format of syslogd with -S or -SS option
```
Oct 31 00:00:00 <syslog.info> localhost AppName[1234]: Message text ...
```
- Standard format of rsyslogd (When "RSYSLOG_TraditionalFileFormat" is specified by "$ActionFileDefaultTemplate" directive.)
```
Oct 31 00:00:00 localhost AppName[1234]: Message text ...
```
- Format of rsyslogd when" RSYSLOG_FileFormat " is specified by "$ActionFileDefaultTemplate"directive
```
2011-10-31T00:00:00.913136+09:00 localhost AppName[1234]: Message text ...
```

Library for 32bit application (for Compute Rack Linux x86_64 only)

In x86_64 environment of Linux, following libraries need to be installed only for Hitachi Compute Rack.
These packages are stored in the install medium of the OS.

- glibc (32-bit x86)
- libstdc++ (32-bit x86)
- libgcc (32-bit x86)

Detected Failure

Log monitor can detect following failure.
However, required software need to be installed and need to be operating normally.

No	Part		Detect failure (v :supported, -:unsupported)			
			Compute Blade (OS common) (*2)	Compute Rack		
				Windows	Linux	VMware (guest OS)
1	System unit	CPU failure	-(*1)	V	V	V
2		Memory failure/degradation	-(*1)	V	V	V
3		FAN failure	-(*1)	V	V	V
4		Mother board failure	-(*1)	V(*3)	V(*3)	V
5		Power supply failure	-(*1)	V	V	V
6		Abnormal voltage	-(*1)	V	V	V
7		Abnormal temperature	-(*1)	V	V	V
8		RAID degradation	V	V	V	V
9		RAID controller failure	V	V	V	-
10		LAN controller failure	V	V	V	-
11		SAS controller failure	V	V	V	-
12		iSCSI controller failure	V	V	V	-
13		FC controller failure	V	V	V	-
14		PCIe Flash drive failure	V	-	-	-

*1: SVP detects the failure on Compute Blade.
*2: In LPAR manager environment, the failures of only dedicated devices are detected.
*3: BMC failure cannot be detected.

Restriction

This section explains the restrictions which would be like to know before use the log monitor

- When OS log (Windows:Event Log, Linux:syslog message) is recorded by high frequency (over 5 events/sec), detection of the failure may be overdue depending on the frequency and time.
- On Linux, when syslog message is recorded except for standard format, detection of the failure may be impossible. Please refer to "syslog service (Linux only) " about the syslog message format that is possible to detect failure.
- Confirm the operation of the log monitor for Compute Rack before starting to monitor the failure. About the procedure, see "3.Operation of the log monitor"-"Confirmation of the operation of the log monitor (for only Compute Rack)"

Restriction in VMware environment

- When log monitor is used in VMware environment, detectable failure is restricted. For details, refer to "Detected Failure".

2

Installation of the log monitor

This chapter provides the procedures for installation of the required software.

- ☐ Preparation before installing the log monitor
- ☐ Installing the log monitor for Compute Blade
- ☐ Installing the log monitor for Compute Rack
- ☐ Uninstallation
- ☐ Confirmation of the version

Preparation before installing the log monitor

This section explains the preparation before installing the log monitor.

Installing the required software

Before installing the log monitor, install the required software.
Please refer to each software manual about how to install.

Setting the firewall

Set the permission of the external communication to 23141/tcp, when using the log transfer function on the system whose communication is restricted by firewall.

Installing the log monitor for Compute Blade

This section explains how to install the log monitor for Compute Blade
In order to use the function of log transfer to the management module, building the network between the management module and OS, and setting up the log monitor is needed.

- Network setting between management module and OS (CB500 only)
- Logical partitioning manager setting
- Installation for Compute Blade - Windows
- Installation for Compute Blade - Linux

Upgrade installation of the log monitor for Compute Blade is unnecessary.
Please install it after uninstall.

Rebooting system is not required after installing the log monitor.

Network setting between management module and OS (CB500 only)

This section explains the network setting when using the log transfer function of the log monitor for Compute Blade.
To set this setting is not necessary when the log transfer function is not use.

1. Set a cooperation setup to log monitor of a management module as "enable."
   For details, refer to the "*CLI console user's guide*" - "Remote access" - "set hwm-agent port command".

2. Build the network to communicate the LAN port of OS with the management LAN port of the management module.

3. Set the firewall (open 23141/tcp port) to communicate the LAN port of OS with the management LAN port of the management module.

Logical partitioning manager setting

Set Y(Yes) to AC(Auto Clear) for the target LPAR at "Logical Partition Configuration" screen, when IPMI service (OS standard) is used as event (SEL) management tool in LPAR manager environment.
(The failure cannot be notified to SVP correctly, when default value:N(No) is set.)

Installation for Compute Blade - Windows

This section explains how to install, set, and confirm the operation about Compute Blade - Windows

Installation of the log monitor for Compute Blade - Windows

This section explains how to install the log monitor for Compute Blade - Windows.

1. Log in with an account of the "Administrator" right
2. Start the following installer in the installer package.

   Install.wsf

   Please confirm the directory of the installer package by referring to the Support_EN.html in the Server installation and monitoring tool DVD.
3. Continue the installation according to directions of a screen.
   (There are no settings to customize during installation)

Install the log monitor on all logical servers (LPAR) when using LPAR manager.

Following messages are displayed when the installation has failed.

Message	Description
The object platform is different. (OS)	The installer was started on unsupported OS. Solution:None
The object platform is different. (ARCH)	The installer, which did not match with the platform (ia32,x64), was started. Solution:Start the installer which matches with the platform.
Microsoft Management Console(mmc) is running cannot be installed.	Installation was terminated because Microsoft Management Console (Event Viewer, service, and computer management) was enabled. Solution: Close the Microsoft Management Console and then restart the installation.
Not environment that can execute IPMI command.	Required software (IPMI driver (OS standard) or ServerConductor/Agent) has not been installed. Solution: Install either ServerConductor/Agent or IPMI driver and then restart the installation
It has already been installed. The installation is discontinued.	Log monitor or Hardware Maintenance Agent has already been installed. Solution: After uninstalling log monitor or Hardware Maintenance Agent, restart the installation.

Settings of the log monitor for Compute Blade - Windows

This section explains setting procedure when using the log transfer function to the management module.

1. Log in with an account of the Administrator right.
2. Select "Server installation and monitoring tool" -"log monitor" - "Connect Test Tool" from start menu, or execute the following command.
   C:\Program Files\HITACHI\miacat\Program\ MRegWinBS.exe
3. Connect Test Tool dialog is displayed, and then click the "Option..." button.
4. Option dialog is displayed, and then click the "Setting..." button.
5. Setup dialog is displayed, and then set the Log Collector settings
   Set as below.

Setting	Value
Permission to send log	Enable (check)
IP Address Connect with SVP	Input the IP address on OS to be used for communication.

6. After the setting, click "OK" button and terminate the Connect Test Tool.

Following messages are displayed when the setting has failed.

[Connect Test Tool]
The error of the Log Monitor was detected.

[Log Monitor]
< Message >

Message	Description
It is initialization. The test report demand was canceled.	The setting or connection confirmation was canceled, because the service initialization process does not complete. Solution: Wait at least five minutes after installing or starting, and then restart the connection confirmation.
Failed in the SEL output.	Settings or failure event codes were not recorded in the management module. Solution: Check the system event log (SEL) management tool has been installed.
Because the number of accumulation of alert report demands was exceeded, it was annulled.	The connection check couldn't be accepted for such reasons as the hardware failure detection was being processed. Solution: Wait five to ten minutes, and then restart the operation.

Confirmation of the log monitor for Compute Blade - Windows

This section explains the procedure to verify the connection between the log monitor for Compute Blade - Windows and the management module.
Wait at least five minutes after installing or starting the log monitor.

1. Log in with an account of the Administrator right
2. Select "Server installation and monitoring tool" -"log monitor" - "Connect Test Tool" from start menu.
   Otherwise, execute
   "C:\Program Files\Hitachi\miacat\Program\MRegWinBS.exe".
3. Option dialog is displayed, and then click the "Connection Test..." button.
4. Connection Confirmed dialog is displayed, and then click the "Start" button.
5. "Connected confirmation was completed" is displayed in the dialog when it completes normally.

Refer to the "Message when the setting is failed" when the confirmation fails.

Tip

Click [Unblock] to continue the process if the Windows Security Alert window opens in the environment where firewall feature is enabled.

Installation for Compute Blade - Linux

Installation of the log monitor for Compute Blade - Linux

This section explains how to install the log monitor for Compute Blade - Windows.

1. Log in with an account of the root right.
2. Install the log monitor with the rpm command.
   (The rpm file is in the installer package)

   ia32 : `rpm -i MIACAT-xxxx-x.i386.rpm`

   x64 : `rpm -i MIACAT-xxxx-x.x86_64.rpm`

Please confirm the directory of the installer package by referring to the Support_EN.html in the Server installation and monitoring tool DVD.

Following messages are displayed when the installation has failed.

Message	Description
package MIACAT -xxxx-x is already installed	Log monitor or Hardware Maintenance Agent has already been installed. Solution: After uninstalling log monitor or Hardware Maintenance Agent, re-install it.
Failed. You are not root user.	The user is not "root" right. Solution: Change the user to "root" and install it.
OpenIPMI-tools or JP1/SC-Agent is not installed. OpenIPMI-tools or JP1/SC-Agent please install it.	ServerConductor/Agent or OpenIPMI-tools has not been installed. Solution: After install ServerConducter/Agent or OpenIPMI-tools, re-install it.

Settings of the log monitor for Compute Blade - Linux

This section explains setting procedure when using the log transfer function to the management module.

1. Log in with an account of the root right.
2. Execute the following command.
   /opt/hitachi/miacat/Program/MRegCUI
3. The menu is displayed, and enter "3" (3.Change optional configuration).
4. Setting items are displayed one by one, change the following value

Setting item	Value
Log sending	Yes
IP Address Connect with SVP	Input the IP address on OS to be used for communication.

   Press [ENTER] for the other setting items described above, and skip the setting.
5. Enter "Yes" and exit the command when "Do you update this configuration ?" is displayed.

Following messages are displayed when the setting has failed.

```
The error of the Log Monitor was detected. <0x00000000/0x00000000>
[Log Monitor]
  <Message>
```

Message	Description
It is initialization. The test report demand was canceled.	The setting or connection confirmation was canceled, because the service initialization process does not complete. Solution: Wait at least five minutes after installing or starting, and then restart the connection confirmation.
Failed in the SEL output.	Settings or failure event codes were not recorded in the management module. Solution: Check the system event log (SEL) management tool has been installed.
Because the number of accumulation of alert report demands was exceeded, it was annulled.	The connection check couldn't be accepted for such reasons as the hardware failure detection was being processed. Solution: Wait about ten minutes, and then restart the operation.

Confirmation of the log monitor for Compute Blade - Linux

This section explains the procedure to verify the connection between the log monitor for Compute Blade - Windows and the management module.
Wait at least ten minutes after installing or starting the log monitor.

1. Log in with an account of the root right.
2. Execute the following command.
   /opt/hitachi/miacat/Program/MRegCUI
3. The menu is displayed, and enter "1" (Check connection with an obstacle report service center.).
4. The confirmation message is displayed, and enter "y".
5. The message "Connection check succeeded." is displayed when it completes normally.

Refer to the "Message when the setting is failed" when the confirmation fails.

Installing the log monitor for Compute Rack

This section explains how to install the log monitor for Compute Blade

- Installation for Compute Rack - Windows
- Installation for Compute Rack - Linux
- Installation for Compute Rack VMware - Windows (guest OS)
- Installation for Compute Rack VMware - Linux (guest OS)

[Note of VMware environment]
・Install the log monitor on the guest OS (for watching the failure)
・One guest OS is needed to watch the failure of one Compute Rack system.
・One guest OS for watching the failure cannot watch the failure of plural Compute Rack systems.
・Always activate the guest OS for watching the failure

Rebooting system is not required after installing and updating the log monitor.

However, rebooting may be necessary to install the required software.
(For details, refer to the manual of each software.)

Installation for Compute Rack - Windows

Installation of the log monitor for Compute Rack - Windows

This section explains how to install the log monitor for Compute Rack - Windows.
Even when the log monitor of old version has been installed, it can be installed by same procedure.
(Uninstalling the old version is not needed. All the settings are taken over.)

1. Log in with an account of the Administrator right.

2. Execute the following installer.

   MIACAT.exe

   Please confirm the directory of the installer package by referring to the Support_EN.html in the Server installation and monitoring tool DVD.

3. Continue the installation according to directions of a screen.
   (There are no settings to customize during installation)

Following messages are displayed when the installation has failed.

Message	Description
Not support this OS version.	The installer was started on unsupported OS. Solution:None
You do not have access to make the required system configuration modifications. Stop the installation. Please rerun this installation from an administrators account.	There is no right to change the system setting. Solution: Install the log monitor by Administrator right

Installation for Compute Rack - Linux

Installation of the log monitor for Compute Rack - Linux

This section explains how to install and upgrade the log monitor for Compute Rack - Linux

1. Log in with an account of the root right.

2. Install the log monitor by rpm command.
   (The rpm file is in the installer package)

   New installation : `rpm -i MIACAT-xxxx-x.i386.rpm`

   Upgrade : `rpm -U MIACAT-xxxx-x.i386.rpm`
   (All the settings are taken over by upgrading)

   "*x*" (Italic type): Alphanumeric characters, such as a version

   Please confirm the directory of the installer package by referring to the Support_EN.html in the Server installation and monitoring tool DVD.

Following messages are displayed when the installation has failed.

Message	Description
MIACAT-xxxx-x is already installed.	[Only when newly installing] Log monitor or Hardware Maintenance Agent has already been installed. Solution: Upgrade the log monitor
Failed. You are not root user.	The user is not "root" right. Solution: Change the user to "root" and install it.
This machine is un-support model, or failed to read model code.	Log monitor was intended to be installed on the unsupported system. Solution: None

Installation for Compute Rack VMware - Windows (guest OS)

Install the log monitor on the guest OS in VMware environment.

Installation of the log monitor for Compute Rack - Windows

This section explains how to install the log monitor for Compute Rack - Windows on the guest OS.

1. Log in with an account of "Administrator" right on guest OS.

2. Execute the following batch file in the installer package.

   MIACAT_vmware_install.bat

   Please confirm the directory of the installer package by referring to the Support_EN.html in the Server installation and monitoring tool DVD.

3. Model select menu is displayed.
   Enter the number of the system model.

4. Continue the installation according to directions of a screen.
   There are no settings to customize during installation.

5. The installation completes when "Installation successfully." is displayed.

Following messages are displayed when the installation has failed.

Message	Description
Not support this OS version.	The installer was started on unsupported OS. Solution:None
You do not have access to make the required system configuration modifications. Stop the installation. Please rerun this installation from an administrators account.	There is no right to change the system setting. Solution: Install the log monitor by Administrator right

Installation for Compute Rack VMware - Linux (guest OS)

Install the log monitor on the guest OS in VMware environment.

Installation of the log monitor for Compute Rack - Linux

This section explains how to install the log monitor for Compute Rack - Linux on the guest OS.

1. Log in with an account of the root right.

2. Execute the following installer in the installer package.

   MIACAT_vmware_install.sh

   Please confirm the directory of the installer package by referring to the Support_EN.html in the Server installation and monitoring tool DVD.

3. Model select menu is displayed when newly installation.
   Enter the number of the system model.
   "Do you update it? [y/n]:" is displayed when upgrading.
   Enter "y" and press "Enter".

4. Log monitor is installed.
   There are no settings to customize during installation.

5. The installation completes when "Installation successfully." or "Update successfully" is displayed.

Following messages are displayed when the installation has failed.

Message	Description
Failed. You are not root user.	The user is not "root" right. Solution: Change the user to "root" and install it.
This machine is un-support model, or failed to read model code.	Log monitor was intended to be installed on the unsupported system. Solution: None

Uninstallation

This section explains how to uninstall the log monitor.

Uninstallation of the log monitor for windows

This section explains how to uninstall the log monitor for Windows.

1. Log in with an account of "Administrator" right.
2. Select "Server installation and monitoring tool" -"log monitor" - "Uninstall" from start menu
   or execute the following command.

   Compute Blade:
   `C:\Program Files\HITACHI\miacat\uninstall.wsf`
   Compute Rack:
   `C:\Program Files\HITACHI\miacat\UNINST.EXE`
   (The directory is "C:\Program Files(x86)" in x64 environment)

Uninstallation of the log monitor for Linux

This section explains how to uninstall the log monitor for Linux.

1. Log in with an account of root right.
2. Execute the following command.
   `rpm -e MIACAT`

Confirmation of the version

This section explains how to confirm the version.

Confirmation of the log monitor version for Compute Blade - Windows

This section explains how to confirm the version of the log monitor for Compute Blade - Windows

1. Log in with an account of "Administrator" right.
2. Select "Server installation and monitoring tool" -"log monitor" - "Connect Test Tool" from start menu, or execute "C:\Program Files\Hitachi\miacat\Program\MRegWinBS.exe"
3. Connect Test Tool dialog is displayed, and then click the "About..." button.
4. Log monitor version is displayed.

Confirmation of the log monitor version for Compute Rack - Windows

This section explains how to confirm the version of the log monitor for Compute Rack - Windows

1. Log in with an account of "Administrator" right.
2. Execute the following command.

   ```
   sc qdescription SMAL2_MainteAgtSvc
   ```

3. Product name and version of the log monitor is displayed.

Confirmation of the log monitor version for Linux

This section explains how to confirm the version of the log monitor for Linux.

1. Log in with an account of root right.
2. Execute the following command

   ```
   rpm -qi MIACAT
   ```

3. Version number is displayed at the "Version"

3

Operation of the log monitor

This chapter explains how to operate the log monitor.

Referring to the failure analysis result code (RC) (for only Compute Rack)

This section explains how to refer to the failure analysis result code.

On Compute Blade, the failure analysis result code can be referred by management module.

1. Log in with an account of manager right
   Windows :"Administrator"
   Linux :"root"

2. Start the RC Viewer.

   Windows :
   Select "Server installation and monitoring tool" - "log monitor" - "RC Viewer" from start menu.
   Or execute the following command.

   C:\Program Files\HITACHI\miacat\Program\ASSIST\ccp.exe
   (The directory is "C:\Program Files(x86)" in x64 environment)

   Linux :
   Execute the following command.

   /opt/hitachi/miacat/Program/ASSIST/ccp

3. The failure analysis result code (RC) is displayed.

```
MODEL CODE : N/A / PRODUCT No. : N/A
MODEL NAME : HA8000/RS220HM(WW)
MODEL FRU  : 0021R22500
RC DICT    : xm_rs220-hxm_en/xM-00-01

date/time          Lv RE UID  EC Failure  Additional
------------------ -- -- ---- -- -------- ----------
12/08/01 15:24:33  ** 10 E400 10 19006500 65000000
12/08/01 15:23:35     10 0100 E2 1F22FFFF 6F06FFFF
12/08/01 15:23:33     10 2000 E0 09370BF1 0BA1FFFF
12/08/01 15:23:33     10 2000 AC 042F0BF1 0BA1FFFF
    Time stamp        Failure analysis result
code(RC)
-- (q:quit) --
```

4. Exit the RC Viewer by pressing "q".

Confirmation of the operation of the log monitor (for only Compute Rack)

This section explains how to confirm the operation of the log monitor on Compute Rack.

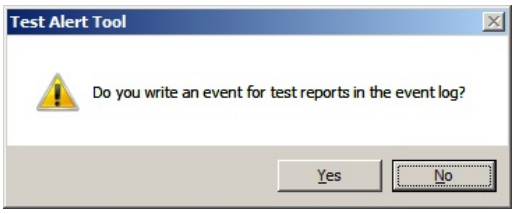
1. Log in with an account of manager right
   Windows :"Administrator"
   Linux :"root"

2. Start the test alert execution tool.

   Windows:
   Execute the following command.

   C:\Program Files\HITACHI\miacat\Program\ASSIST\testalt.wsf
   (The directory is "C:\Program Files(x86)" in x64 environment)

   After the command execution, "Test Alert Tool" dialog is displayed.
   Click [Yes] button.



   Click [OK] button, when "Wrote an event for test reports." is displayed

Linux:

Execute the following command.

```
/opt/hitachi/miacat/Program/ASSIST/testalt.sh
```

After the command execution, confirmation message is displayed.
Input "yes".

```
#  /opt/hitachi/miacat/Program/ASSIST/testalt.sh
==== TEST ALERT TOOL ====
Do you write a message for test reports in the
syslog?
(yes|no[no]): yes
```

"Wrote a message for test reports." is displayed.

```
#  /opt/hitachi/miacat/Program/ASSIST/testalt.sh
==== TEST ALERT TOOL ====
Do you write a message for test reports in the
syslog?
(yes|no[no]): yes
Wrote a message for test reports.
```

3. Wait about 3 minutes, start RC Viewer.

Windows :

Select "Server installation and monitoring tool" - "log monitor" - "RC Viewer" from start menu.

Or execute the following command.

```
C:\Program Files\HITACHI\miacat\Program\ASSIST\ccp.exe
```

(The directory is "C:\Program Files(x86)" in x64 environment)

Linux :

Execute the following command.

```
/opt/hitachi/miacat/Program/ASSIST/ccp
```

4. Failure analysis result code(RC)s are displayed. Confirm that the following RC is displayed.

   RC : 10 E000 FA F00001FF 01FFFFFF

```
MODEL CODE : N/A / PRODUCT No. : N/A
MODEL NAME : HA8000/CR220-sSM
MODEL FRU  : 0021R22610
RC DICT    : xm_rs220-sxm/xM-00-08

date/time          Lv RE UID  EC Failure  Additional
------------------ -- -- ---- -- -------- ----------
12/08/01 15:24:33     10 E000 FA F00001FF 01FFFFFF
12/08/01 15:23:35     10 0100 E2 1F22FFFF 6F06FFFF
12/08/01 15:23:33     10 2000 E0 09370BF1 0BA1FFFF
12/08/01 15:23:33     10 2000 AC 042F0BF1 0BA1FFFF
     Time stamp        Failure analysis result
-- (q:quit) --
```

   This RC may not be displayed immediately after OS installation.
   In this case, perform again from "2. Start the test alert execution tool." in that case.

5. Exit the RC Viewer by pressing "q".

Appendix

This chapter explains the supplementary information of the log monitor

- ☐ List of the messages
- ☐ Install folder organization

List of the messages

This section explains the list of the message which is output by log monitor.

List of the event log for Compute Blade - Windows

This section explains the list of the event log messages, which the log monitor for Compute Blade - Windows outputs.

The list of the event log is described below.

Event source name:"SMAL2_MainteAgtSvc"

Event ID	Message	Description
1	----- Service Start -----	Log monitor is started up.
2	----- Preparation completion. -----	IPMICMD is ready
3	----- Service End -----	Log monitor is exited
10	SEL was written in BMC. DATE:xxxx/xx/xx xx:xx:xx SEL :xxxxxxxxxxxxxxx	SEL outputs succeeds
15	Accepted a transmission request of the log. FROM:xxx.xxx.xxx.xxx *(IP address, source of request to collect the log)* ORDER:xxxxxxxx	Request of collecting the log is received.
16	Transferred a log file. TO:xxx.xxx.xxx.xxx*(IP address, target of log transfer)* ORDER:xxxxxxxx	Reply of the request to collect the log completes.
500	The test report is done. (TestReportOpportunity) CheckID: xxxxxxxx	Confirming connection is executed
1007	Failed in the SEL output. (ErrorCode:xxxxxxxx,DetailCode:xxxxxxxx) DATE:xxxx/xx/xx xx:xx:xx SEL:xxxxxxxxxxxxxxx	SEL output fails. Action:Confirm ServerConductor/Agent or SelManager is installed accurately.
1008	Login failed. ErrorCode:xxxxxxxx DetailCode:xxxxxxxx	Reject the request to collect the log. Action:Confirm whether collecting the log is permitted.
1009	Failed in log transfer. ErrorCode: xxxxxxxx DetailCode: xxxxxxxx	Log transfer fails. Action: Check communication path with SVP.

List of the event log for Compute Blade - Linux

This section explains the list of the event log messages, which the log monitor for Compute Blade - Linux outputs.

The message of the log monitor is output with tag name"SMAL2_MainteAgtSvc"

```
Aug  2 16:38:07 RHEL6264 SMAL2_MainteAgtSvc[4026]: (Message)
```

The list of the event log is described below.

Message	Description
[INFO]----- Service Start -----	Log monitor is started up.
[INFO]----- Preparation completion. -----	IPMICMD is ready
[INFO]----- Service End -----	Log monitor is exited
[INFO] SEL was written in BMC.,Date:xxxx/xx/xx xx:xx:xx, SEL:xxxxxxxxxxxxxxx	SEL outputs succeeds
[INFO] Receiving a request to collect the logs. FROM:xxx.xxx.xxx.xxx ORDER:xxxxxxxx	Request of collecting the log is received.
[INFO] Transferred a log file.TO:xxx.xxx.xxx.xxx ORDER:xxxxxxxx	Reply of the request to collect the log completes.
[INFO] The test report is done. (TestReportOpportunity)CheckID:{xxxxxxxx }	Confirming connection is executed
[WARN]Failed in the SEL output. (ErrorCode:xxxxxxxx, Detaile:xxxxxxxx), Date:xxxx/xx/xx xx:xx:xx,SEL:xxxxxxxxxxxxxxx	SEL output fails. Action:Confirm ServerConductor/Agent or SelManager is installed accurately.
[WARN] Login failed.(ErrorCode:xxxxxxxx DetailCode:xxxxxxxx)	Reject the request to collect the log. Action:Confirm whether collecting the log is permitted.
[WARN] Failed in log transfer.(ErrorCode:xxxxxxxx DetailCode:xxxxxxxx)	Log transfer fails. Action: Check communication path with SVP.

List of the event log for Compute Rack - Windows

This section explains the list of the event log messages, which the log monitor for Compute Blade - Windows outputs.

The list of the event log is described below.

Event source name:"SMAL2_MainteAgtSvc"

EventID	Message	Description
12	Transmitted to the ASSIST agent.	A fault report has been sent to the integrated monitoring unit.
13	Received a log collection demand from the ASSIST agent.	Request of log collection has been received from the integrated monitoring unit.
14	Transmitted log information to the ASSIST agent.	Log information has been sent to the integrated monitoring unit
100	Started log monitoring.	Log monitor is started up.
101	Started alive-check.	Alive check function is stated up.
102	Stopped alive-check, because received the stop demand from the ASSIST agent.	Alive check function is stopped.
103	Stopped log monitoring.	Log monitor is stopped.
500	The test report is generated.	A test report trigger messages is sent.
1008	An error occurred at communication control.	An error occurred when a fault report is being sent to the integrated monitoring unit at the maintenance company. Action: Check the communication path with integrated monitoring unit.
2100	Failed in the initialization.	The log monitor has been stopped due to an inconsistency of the setting information or a conflict of network resources. Action: Check whether the port number, used by log monitor, conflicts.
2101	Failed to start of alive-check. The setting has not adjusted to the ASSIST agent.	The Alive check function cannot be started because a setting of the device such as the model name or serial number does not coincide with the setting in the integrated monitoring unit located at the maintenance company. Action: Check the setting.

List of the event log for Compute Rack - Linux

This section explains the list of the event log messages, which the log monitor for Compute Rack - Linux outputs.

The message of the log monitor is output with tag name"SMAL2_MainteAgtSvc"

```
Aug  2 16:38:07 RHEL6264 SMAL2_MainteAgtSvc[4026]: [INFO] (Message)
```

The list of the event log is described below.

Message	Description
[INFO] Transmitted to the CE-Station.	A fault report has been sent to the integrated monitoring unit located at the maintenance company.
[INFO] Received a log collection demand from the failure report manager.	Log information has been sent to the integrated monitoring unit located at the maintenance company.
[INFO] Transmitted log information to the failure report manager.	Log information has been sent to the integrated monitoring unit located at the maintenance company.
[INFO] Started log monitoring.	Log monitor has been started.
[INFO] Started alive-check.	The Alive check function has been started.
[INFO] Stopped alive-check, because received the stop demand from the failure report manager.	The Alive check function has been stopped.
[INFO] Stopped log monitoring.	Log monitor has been stopped.
[INFO] The test report is generated.	A test report trigger messages is sent.
[WARN] An error occurred at communication control.	An error occurred when a fault report is being sent to the integrated monitoring unit at the maintenance company. Action: Check the communication path with integrated monitoring unit
[ERROR] Failed in the initialization.	The log monitor has been stopped due to an inconsistency of the setting information or a conflict of network resources. Action: Check whether the port number, used by log monitor, conflicts.
[WARN] Failed to start of alive-check. The setting has not adjusted to the failure report manager.	The Alive check function cannot be started because a setting of the device such as the model name or serial number does not coincide with the setting in the integrated monitoring unit located at the maintenance company. Action: Check the setting.

Install folder organization

This section explains the folder organization of the log monitor.

Folder organization for Windows

Folder organization for Windows is described below.

```
C:\Program Files\   (Only Compute Rack x64 environment "C:\Program Files(x86)\")
 |- HITACHI\miacat\
    |- Log            <- Folder to store execution log
    |                      (The files in this folder are created, changed, or deleted in operation.)
    |- LogCollector   <- Folder of log collection program (The files are unchanged.)
    |- MainteTool     <- Folder of sub program (The files are unchanged.)
    |- MainteData     <- Folder to store the definition and setting
    |                      (The files in this folder are changed when changing the setting.)
    |- Program        <- Folder of service program (The files are unchanged.)
    |- Temp           <- Folder to store temporary files
                           (The files in this folder are created, changed, or deleted in operation.)
```

Folder organization for Linux

Folder organization for Linux is described below.

```
/opt/
 |- hitachi/miacat/
    |- LogCollector    <-Folder of log collecting program (The files are unchanged.)
    |- MainteTool      <-Folder of sub program (The files are unchanged.)
    |- MainteData      <-Folder to store the definition and setting
    |                    (The files in this folder are changed when changing the setting.)
    |- Program         <-Folder of service program (The files in this folder are unchanged.)

/var/
 |- opt/hitachi/miacat
    |- Log             <-Folder to store execution log
    |                    (The files in this folder are created, changed, or deleted in operation.)
    |- Temp            <-Folder to store temporary files
                         (The files in this folder are created, changed, or deleted in operation.)
```

Acronyms and Abbreviations

BMC	Baseboard management controller
FC	Fibre Channel
GB	gigabyte
GUI	Graphical User Interface
Hz	Hertz
IPMI	Intelligent Platform Management Interface
KB	Kilobyte
LAN	local area network
OS	operating system
RAID	Redundant Arrays of Inexpensive Disks
RC	Failure Analysis Result Code (for Compute Rack) Reference Code (for Compute Blade)
SAS	Serial Attached SCSI
SEL	System Event Log
URL	Uniform Resource Locator
VGA	video graphics array
VM	virtual machine

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

MK-99COM064-02