

**Hitachi Compute Blade Series
Hitachi Compute Rack Series**
Server installation and monitoring tool User's Guide
log monitoring functions
for VMware vMA

FASTFIND LINKS

[Document Organization](#)

[Product Version](#)

[Getting Help](#)

[Contents](#)

© 2010-2014 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi, Ltd.

Hitachi, Ltd., reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Data Systems Corporation at <https://portal.hds.com>.

Notice: Hitachi, Ltd., products and services can be ordered only under the terms and conditions of the applicable Hitachi Data Systems Corporation agreements. The use of Hitachi, Ltd., products is governed by the terms of your agreements with Hitachi Data Systems Corporation.

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

Archivas, Essential NAS Platform, HiCommand, Hi-Track, ShadowImage, Tagmaserve, Tagmasoft, Tagmasolve, Tagmastore, TrueCopy, Universal Star Network, and Universal Storage Platform are registered trademarks of Hitachi Data Systems Corporation.

AIX, AS/400, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, ESCON, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, RS6000, S/390, System z9, System z10, Tivoli, VM/ESA, z/OS, z9, z10, zSeries, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

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

Microsoft product screen shots are reprinted with permission from Microsoft Corporation



Contents

Preface	v
Intended Audience	vi
Product Version.....	vi
Release Notes	vi
Abbreviations of Operating Systems.....	vii
Document Organization	vii
Document Conventions.....	viii
Convention for storage capacity values	viii
Getting Help	ix
Technical Information and Update Program.....	ix
Comments.....	ix
Safety guidelines	xi
Safety information.....	xii
Common precautions concerning safety	xiii
Precautions against damage to equipment	xiii
Log monitor for vMA overview	1-1
Overview	1-2
Functions	1-2
Supported Products	1-3
Supported VMware	1-3
Required Resources.....	1-4
Required Software.....	1-5
Detectable failure	1-6
Restriction	1-6
Installation of the log monitor for vMA	2-1
Overview of the installation of the log monitor for vMA.....	2-2

Setting of VMware Hypervisor and Installation of required software	2-3
Installation of the log monitor for vMA	2-18
Uninstallation	2-22
Confirmation of the version	2-24
Operation of the log monitor for vMA.....	3-1
Referring to the failure analysis result code (RC) (only for Compute Rack)	3-2
Appendix	A-1
List of the messages	A-2
Install folder organization.....	A-4
Acronyms and Abbreviations	Acronyms-1



Preface

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

This preface includes the following information:

- [Intended Audience](#)
- [Product Version](#)
- [Release Notes](#)
- [Abbreviations of Operating Systems](#)
- [Document Organization](#)
- [Document Conventions](#)
- [Convention for storage capacity values](#)
- [Getting Help](#)
- [Technical Information and Update Program](#)
- [Comments](#)

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.

Product Version

This document revision applies to Compute Blade Series CB500, CB2000 and Compute Rack Series CR220HM, CR210HM, CR220SM.

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.

- VMware vSphere® ESXi™ 5.5
(Hereinafter, referred to as VMware vSphere ESXi 5.5, VMware vSphere ESXi 5, or VMware)
- VMware vSphere® ESXi™ 5.1
(Hereinafter, referred to as VMware vSphere ESXi 5.1, VMware vSphere ESXi 5, or VMware)
- VMware vSphere® ESXi™ 5.0
(Hereinafter, referred to as VMware vSphere ESXi 5.0, VMware vSphere ESXi 5, or VMware)

Document Organization

The table below provides an overview of the contents and organization of this document. Click the chapter title in the left column to go to that chapter. The first page of each chapter provides links to the sections in that chapter.

Chapter	Description
Chapter 1, Log monitor for vMA overview	Provides an overview of Server installation and monitoring tool log monitoring functions for vMA.
Chapter 2, Installation of the log monitor for vMA	Provides information about how to install and uninstall log monitor.
Chapter 3, Operation of the log monitor for vMA	Provides information about how to use log monitor.
Appendix A, Appendix	Provides information about message list and installed folder organization.

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
Regular text bold	In text: keyboard key, parameter name, property name, hardware labels, hardware button, hardware switch. In a procedure: user interface item
<i>Italic</i>	Variable, emphasis, reference to document title, called-out term
Screen text	Command name and option, drive name, file name, folder name, directory name, code, file content, system and application output, user input
< > (angled brackets)	Variable (used when italic is not enough to identify variable).
[] (square bracket)	Optional values
{ } braces	Required or expected value
vertical bar	Choice between two or more options or arguments
_(underline)	Default value, for example, [<u>a</u>] b]

Convention for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10 ³) bytes
1 megabyte (MB)	1,000 KB or 1,000 ² bytes
1 gigabyte (GB)	1,000 MB or 1,000 ³ bytes
1 terabyte (TB)	1,000 GB or 1,000 ⁴ bytes
1 petabyte (PB)	1,000 TB or 1,000 ⁵ bytes
1 exabyte (EB)	1,000 PB or 1,000 ⁶ bytes

Logical storage capacity values (for example, logical device capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1,024^2$ bytes
1 GB	1,024 MB or $1,024^3$ bytes
1 TB	1,024 GB or $1,024^4$ bytes
1 PB	1,024 TB or $1,024^5$ bytes
1 EB	1,024 PB or $1,024^6$ bytes

Getting Help

The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, log on to the Hitachi Data Systems Portal for contact information: <https://portal.hds.com>.

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 and number including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Data Systems Corporation.

Thank you!








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.

Log monitor for vMA overview

This chapter describes overview of the Server installation and monitoring tool log monitor for VMware vMA (hereinafter describes log monitor)

(*1) vMA : vSphere Management Assistant
(The virtual appliance which unified the tool required for management of VMware)

- [Overview](#)
- [Functions](#)
- [Supported Products](#)
- [Supported VMware](#)
- [Required Resources](#)
- [Required Software](#)
- [Detectable Failure](#)
- [Restriction](#)

Overview

Log monitor for vMA can collect maintenance information and can analyze hardware problems through the log data on the VMware vSphere Hypervisor (hereinafter describes Hypervisor), 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 for vMA, quick failure restoration is available and system availability improves.



Log monitor for vMA can detect much failure than log monitor which works on guest OS (Windows or Linux). Please refer to the "[Detectable failure](#)".

Functions

This section explains the log monitor function for vMA.

Collecting and analyzing the failure information and maintenance information

Log monitor watches the Hypervisor log, and generating the failure event code when the failure event is detected.

On Compute Rack series, it watches not only the Hypervisor log but also the event of the system unit (SEL).

(The SVP watches SEL of the system unit on Compute Blade)

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.

Supported Products

Log monitor for vMA supports following products.

Series	Model	Log monitor version
Hitachi Compute Blade	CB500 CB2000	09-xx
Hitachi Compute Rack	CR220HM,CR210HM,CR220SM	86-xx

Supported VMware

Log monitor for vMA supports following VMware version.
However, it is precondition that the system unit supports the version.

VMware vSphere ESXi 5



Installing the [Required Software](#) and log monitor for vMA is required.
The vMA, which log monitor for vMA has been installed, is required for each system.
(When the VMware environment is build by plural systems, the vMAs for watching the failure are needed by the number of system units.)



Please uses the log monitor for guest OS(windows/Redhat Linux) when the VMware version is VMware vSphere 4

Required Resources

Log monitor for vMA 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.

Service	Residence process
smal2d	/opt/hitachi/miacat/Program/SMAL2MASvc
VmSyslogMAgtSrvd	/opt/hitachi/VmSyslogMAgtSrvd/bin/VmSyslogMAgtSrvd
SelManager (*1)	/opt/hitachi/SelManager/SelManager

(*1) Service of the System event (SEL) Management tool (Compute Rack only)

Log monitor for vMA uses following ports.

Port	Service	Description
23141/tcp	core-linux (*1)	Communication port of the reporting device (for Compute Rack only)
31100/tcp	smal2_mainteregagt_port (*1)	Port for internal communication of log monitor
31101/tcp	smal2_mainteagt_port (*1)	Port for internal communication of log monitor
514/udp	syslog	Port for message receipt of Hypervisor's syslog
443/tcp	https	Port for communication of esxcli command

When above ports have been already used by other processes, port number can be changed by editing /etc/services file of vMA.

*1: When Log monitor is installed, these service names are not added to /etc/services file by default.



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.

- [vSphere Client](#) or [vSphere Web Client](#)
- [vSphere Management Assistant \(vMA\)](#)
- [MPM](#)
- [System event \(SEL\) Management Tool](#)

vSphere Client or vSphere Web Client

When introducing the log monitor for vMA, vSphere Client or vSphere Web Client is used.

Please prepare the environment to operate the VMware system by vSphere Client or vSphere Web Client before installing the log monitor for vMA.

vSphere Management Assistant (vMA)

vMA is the virtual appliance which unified the tool required for management of VMware.

Please install the vMA before installing the log monitor for vMA. vMA can be downloaded from the website of VMware, Inc.

MPM

This is the software which provides the IPMI function to collect the syslog message on the Hypervisor and to access the system event log(SEL) of the system unit.

This software is included in the install package of the log monitor for vMA. Installation procedure is described in this manual.

System event (SEL) Management Tool

This is the software to manage the event of system unit and record the failure event code in the management module.

This software is included in the install package of the log monitor for vMA. Installation procedure is described in this manual.

Detectable failure

Log monitor for vMA can detect the following failure.

No	Part		Detect (V:Detectable, -:Undetectable)		
			Compute Blade	Compute Rack	
				For vMA	[Reference] For Guest OS
1	System unit	CPU failure	- (*1)	V	V
2		Memory failure/degradation	- (*1)	V	V
3		FAN failure	- (*1)	V	V
4		Mother Board failure	- (*1)	V(*3)	V(*3)
5		Power supply failure	- (*1)	V	V
6		Abnormal voltage	- (*1)	V	V
7		Abnormal temperature	- (*1)	V	V
8		RAID degradation	V	V	V
9		RAID controller failure	V	V	- (*2)
10		LAN controller failure	V	V	- (*2)
11		SAS controller failure	V	V	- (*2)
12		iSCSI controller failure	V	V	- (*2)
13		FC controller failure	V	V	- (*2)
14		PCIe Flash drive failure	V	-	-
*1: SVP detects the failure on Compute Blade. *2: Reference information of detectable failure on log monitor for guest OS (Windows/Redhat Linux). *3: BMC failure cannot be detected.					

Restriction

This section explains the restrictions which would be like to know before using the log monitor for vMA.

- When OS log is recorded by high frequency (more than five affairs/second), detection of the failure may be overdue depending on the frequency and time.
- To install the both log monitor for vMA and log monitor for guest OS (Windows/Redhat Linux) is impossible to watch one system.
- Disable the lockdown mode of VMware ESXi. If the lockdown mode is enabled, log monitor for vMA cannot detect the failure correctly.

- Please build environment to make HTTPS connection of vMA and VMware ESXi.
- Please build environment to be able to receive a syslog message from VMware ESXi to vMA.

Installation of the log monitor for vMA

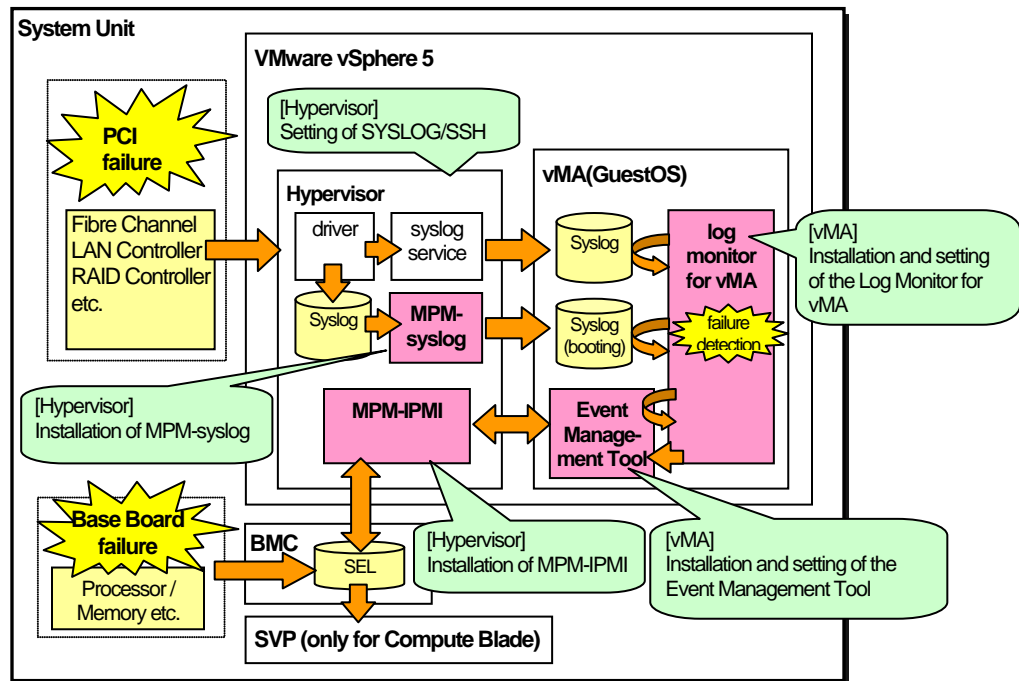
This chapter provides the procedure for installation of the log monitor for vMA.

- [Overview of the installation of the log monitor for vMA](#)
- [Setting of the VMware Hypervisor and installation of the required software](#)
- [Installation of the log monitor for vMA](#)
- [Uninstallation](#)
- [Confirmation of the version](#)

Overview of the installation of the log monitor for vMA

Install the log monitor for vMA by following operation.

- [Setting of the Hypervisor](#)
Enable the transferring of syslog message and enable the SSH function.
- [Installation of the required software](#)
(The software is included in the install package of the log monitor for vMA.)
 - MPM-IPMI
This is the software to relay IPMI via Hypervisor. This is installed in the Hypervisor.
 - MPM-syslog
This is the software to send the syslog of the Hypervisor. This is installed in the Hypervisor.
 - Event Management Tool
This is the software to refer and write the system event log(SEL) of the system unit in cooperation with MPM-IPMI. This is installed in vMA.
- [Restarting the VMware\(Hypervisor\)](#)
- [Installation of the log monitor for vMA](#) (Installed in vMA)
- [Setting of the log monitor for vMA](#)



BMC: Baseboard management controller SVP: Service Processor

Setting of VMware Hypervisor and Installation of required software

This section explains setting of VMware and installing of [Required software](#).

[Operation flow]

- [Enabling the SSH function of the Hypervisor](#)
- [Enabling the transferring of the Hypervisor syslog message](#)
- [Uploading the software to the datastore](#)
- [Installing the MPM in the Hypervisor](#)
- [Copying the software from the datastore to vMA](#)
- [Installing the Event Management Tool in vMA](#)
- [Restarting VMware\(Hypervisor\)](#)
Restart VMware(Hypervisor) surely.
Otherwise, installation of the log monitor for vMA fails.
- [Confirming the required software operation](#)

[The supplement about operation explanation]

In this operation explanation, IP address of the Hypervisor is "192.168.100.2", VMware datastore name is "datastore1", Hypervisor root password is "password", IP address of the vMA is "192.168.100.10" . Please replace the value according to the customer's environment.

After entering a command on vMA, there is a case that "vi-admin's password:" or "Password:" is displayed and entering the password is required. Please enter the password for vi-admin user used for login to the vMA when "vi-admin's password:" is displayed. Please enter the password for the root user of Hypervisor when "Password:" is displayed.

Enabling the SSH function of the Hypervisor

Enable the SSH function of the Hypervisor.

SSH function is used for installation of the required software. Log monitor can operate correctly when SSH function is disabled after installation.

1. Press [F2] key at the start screen of the system unit (Hypervisor).
2. Login by root user when login screen is displayed.
3. Select [Troubleshooting Options] and press [Enter] key at [System Customization] screen
4. Select [Enable SSH] and press [Enter] key.
5. Press [ESC] key several times and return to the start screen



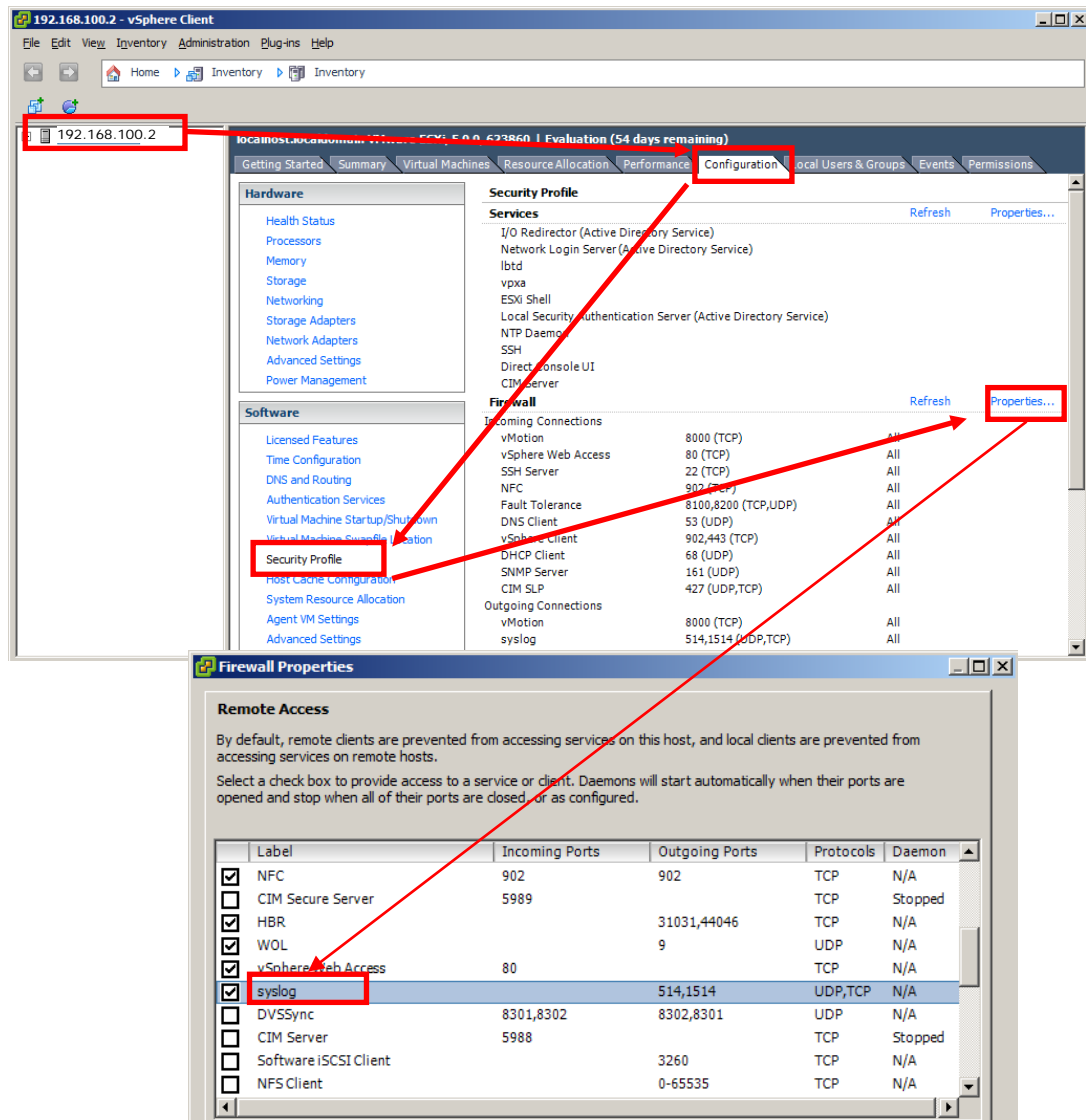
When enabling timeout of SSH function is set, SSH function is disabled automatically after the setting time.

Enabling the transferring of the Hypervisor syslog message

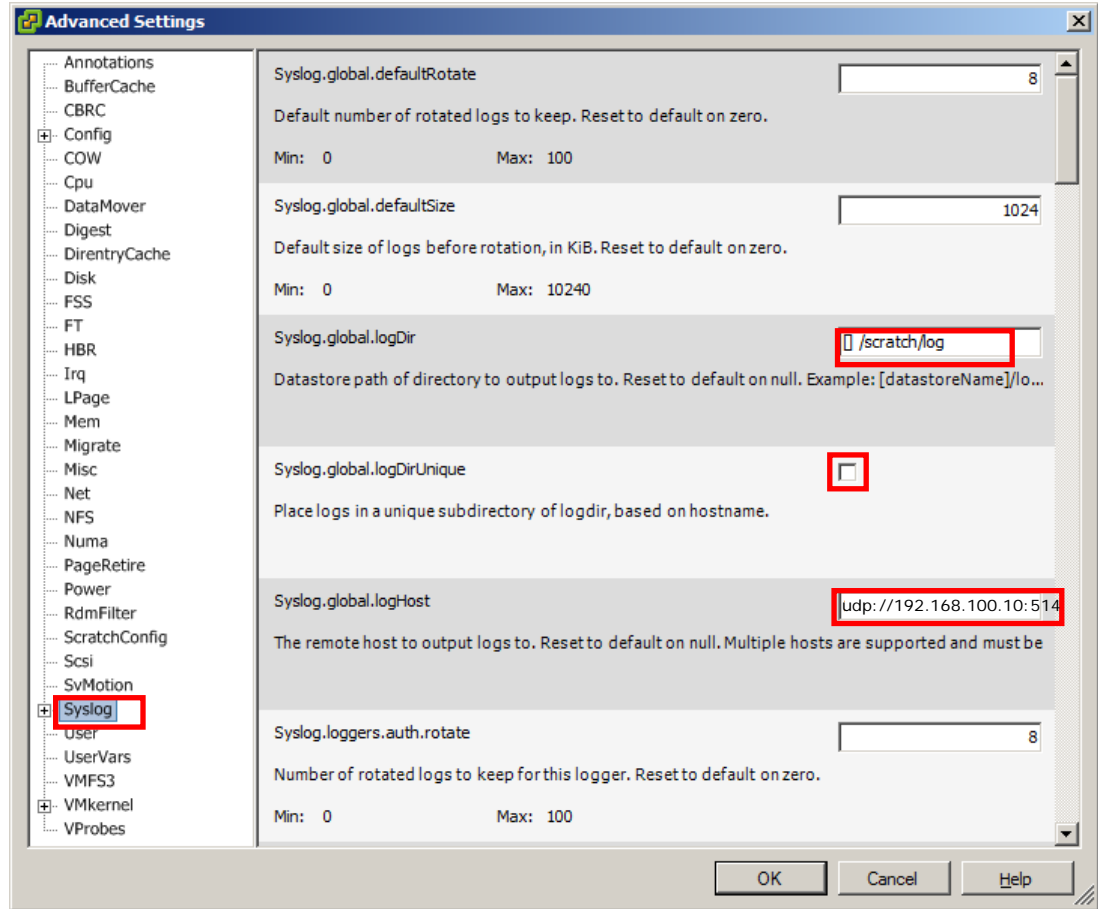
This section explains the procedure of setting the Hypervisor syslog. The procedure for vSphere client is different from vSphere Web Client.

■ Procedure for vSphere Client

1. With the vSphere Client, select "Configuration" tab of the Hypervisor, select "Security Profile", and then click the Properties of "Firewall".
2. "Firewall Properties" is displayed, check the check box of "syslog" and press "OK".

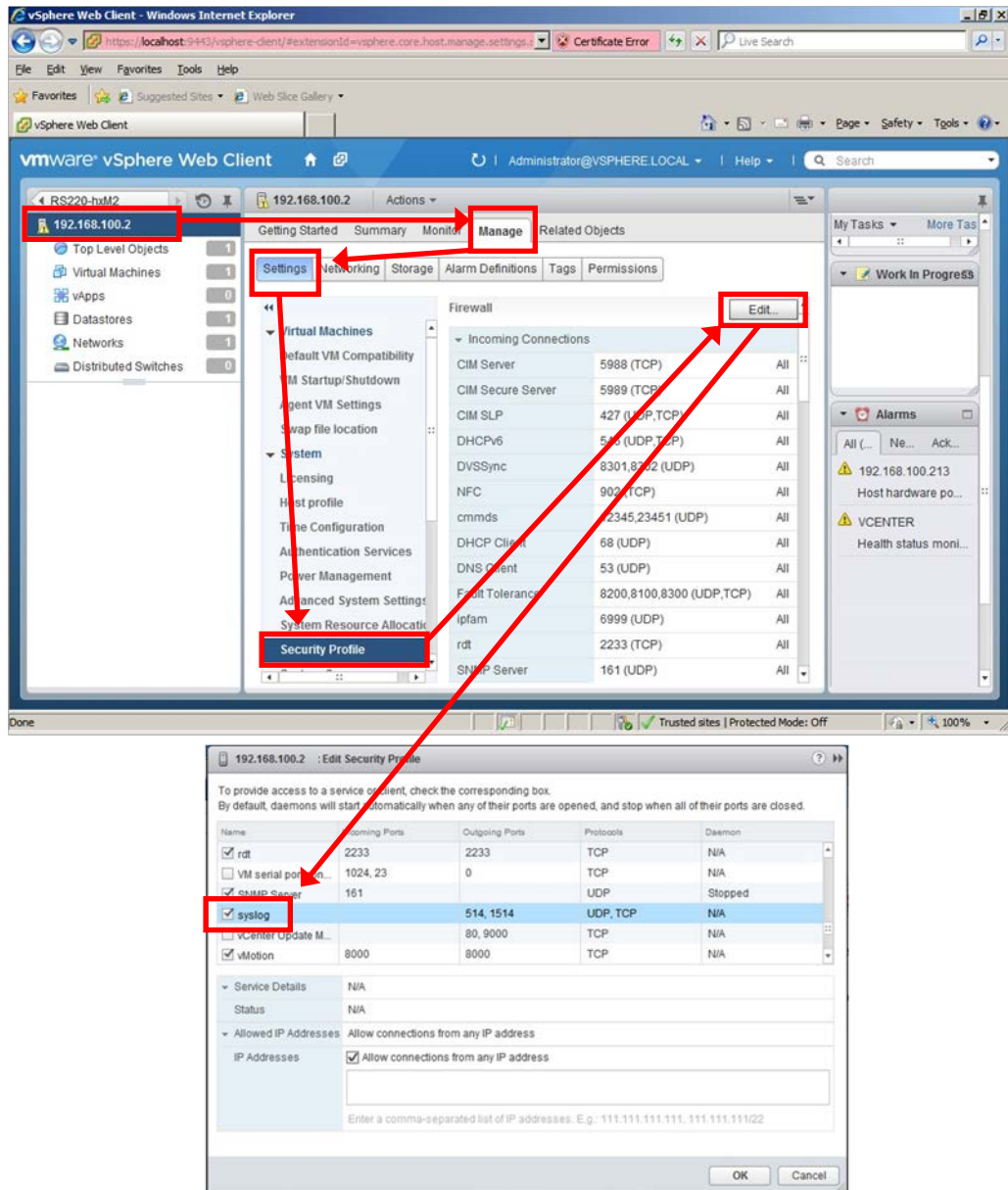


3. With the vSphere Client, select "Configuration" tab of the Hypervisor, click "Advanced Settings" of "Software".
4. Select "Syslog" at "Advanced Settings" screen. Change the following settings and then press "OK"
 - Syslog.global.logDir : "[] /scratch/log"
 - Syslog.global.logDirUnique : Remove the check
 - Syslog.global.logHost : "udp://<IP address of vMA>:514"
(ex. "udp://192.168.100.10:514")

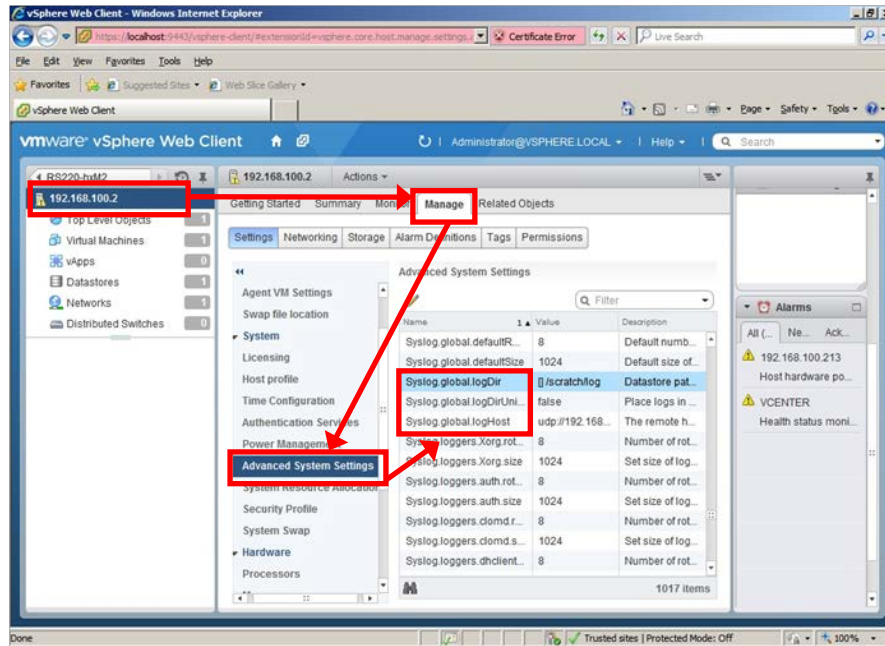


■ Procedure for vSphere Web Client

1. Open the "Manage" tab of the Hypervisor on vSphere Web Client. Click the "Settings" button and select "Security Profile". Then click the "Edit" button.
2. "Edit Security Profile" is opened. Check the check box of "syslog" and click "OK" button.



- Open the "Manage" tab of the Hypervisor on vSphere Web Client. Click the "Advanced System Settings".



- Select " Syslog.global.logDir " at the "Advanced System Settings". Set the following character at the "Edit Advanced Option" dialog and click the "OK" button.

- Syslog.global.logDir : "[] /scratch/log"



- Set the following settings as well.

- Syslog.global.logDirUnique : Select "false"
- Syslog.global.logHost : "udp://vMA IP address: 514"
(Ex. "udp://192.168.100.10: 514")

Uploading the software to the datastore

Upload the following files, which are included in the install package of the log monitor for vMA, to the system unit (VMware).

- vmware-esx-esxcli-getsyslog-500.1.0-xxxxxx.vib (MPM-syslog)
- vmware-esx-esxcli-miacat-500.1.0-xxxxxx.vib (MPM-IPMI)
- miacat-vma-install-xxxx.tar.gz (Event Management Tool)
- selman-vma-install-xxxx.tar.gz (Event Management Tool (Service)) (Only for Compute Rack)
- MIACAT_BSVMA-xxxx-x.i586.rpm (log monitor for vMA (for Compute Blade))
or
MIACAT_HAVMA-xxxx-x.i386.rpm (log monitor for vMA (for Compute Rack))

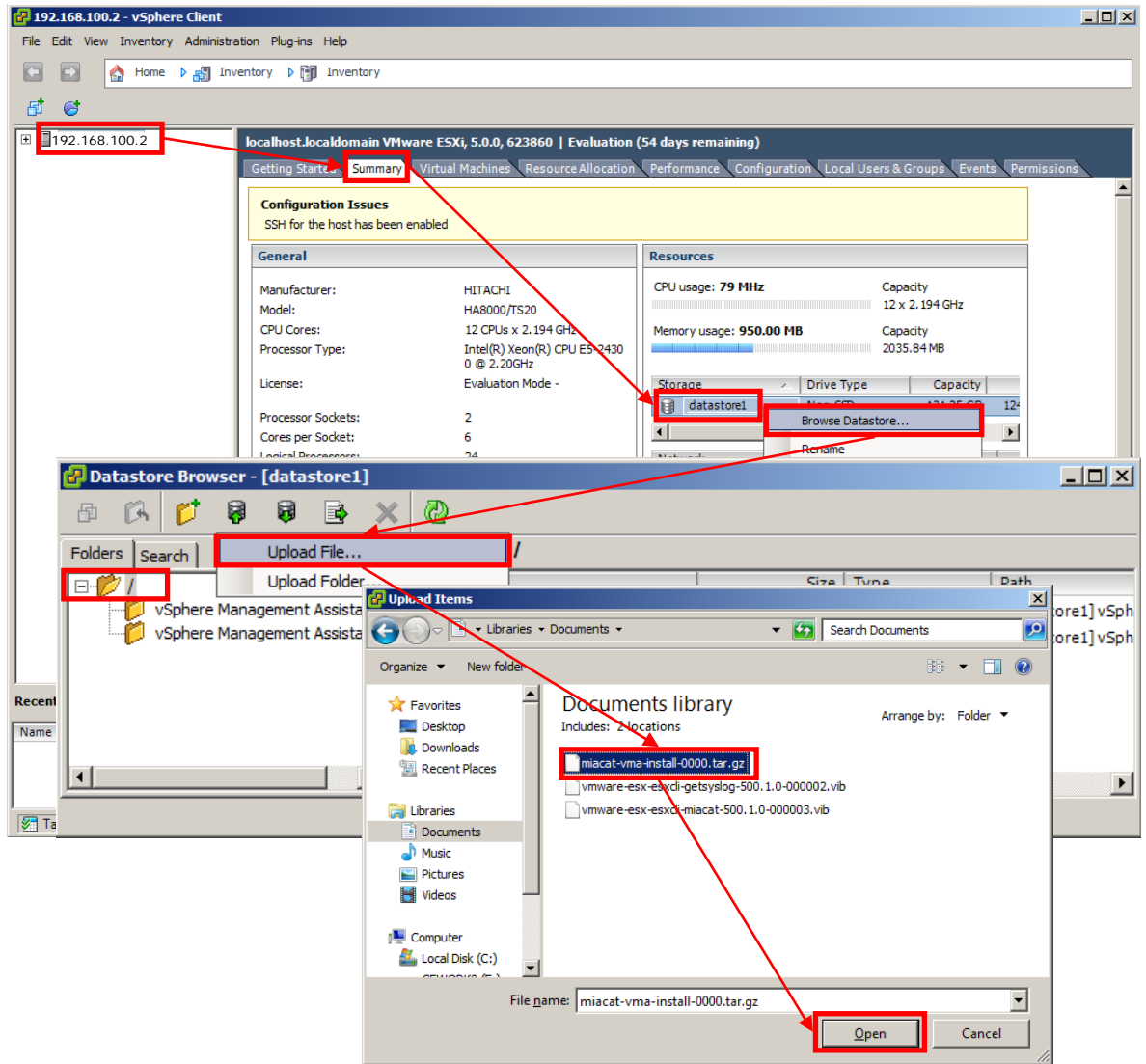
"x"(Italic font): Alphanumeric characters, such as a version number

The procedure for vSphere client is different from vSphere Web Client.

■ Procedure for vSphere Client

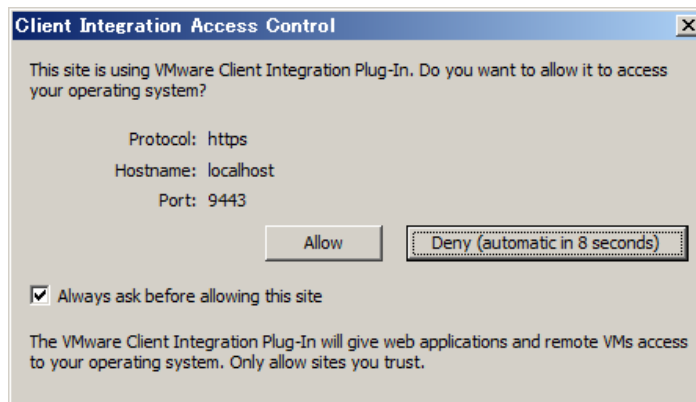
1. With the vSphere Client, select "Summary" tab of the Hypervisor.
2. Select "Browse Datastore..." by right-click at the target disk(datastore1) in "Storage".
3. "Datastore Browser" is started. Select the upload target folder("/"). Click "Upload" icon and select "Upload File...".
4. Select the file to be copied at "Upload Items" dialog.
(The file is uploaded.)
5. Upload the all files by repeating the procedure 3 and 4.
(selman-vma-install-xxxx.tar.gz is required only for Compute Rack.)

[vSphere Client screen of the uploading procedure]



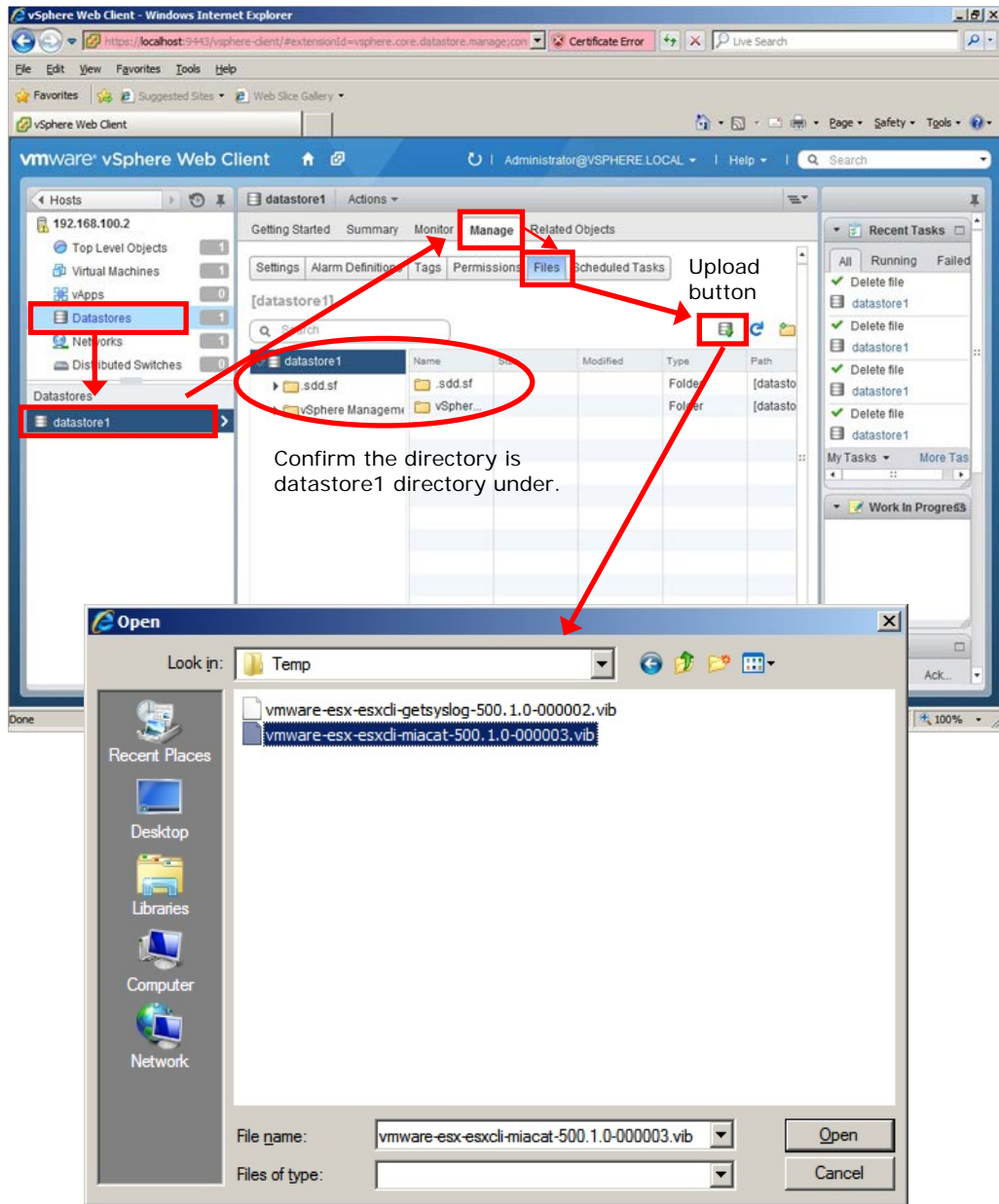
■ Procedure for vSphere Web Client

1. Select the target disk (ex. datastore1) from the "datastore" of the vSphere Web Client.
Open the "Manage" tab and click the "Files" button.
2. Upload destination is displayed after clicking the "Files" button.
Confirm the directory is datastore1 directory under and click the "Upload" button.
3. When the following dialog is displayed after clicking the "Upload" button, Click "Allow" button within 10 seconds.



4. Select the file to copy at the file selection dialog.
(The file is uploaded)
5. Upload all files by repeating procedure 2 to 4.
[selman-vma-install-xxxx.tar.gz](#) is necessary for only Compute Rack.

[vSphere Web Client screen of the uploading procedure]



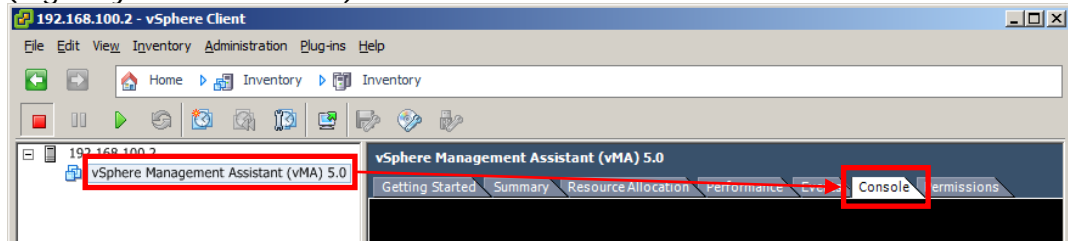
Installing the MPM in the Hypervisor

Install the following software in the Hypervisor.

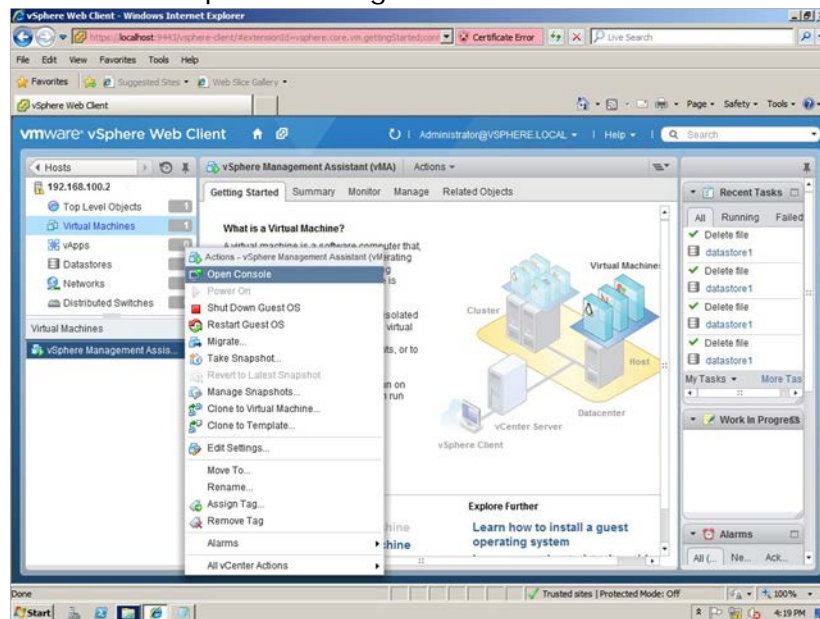
- MPM-syslog (vmware-esx-esxcli-getsyslog-500.1.0-xxxxxx.vib)
- MPM-IPMI (vmware-esx-esxcli-miacat-500.1.0-xxxxxx.vib)

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

1. When vMA is stopped, start the vMA.
2. With vSphere Client, select the "Console" tab of vMA.
(login by vi-admin user.)



To open the vMA console with vSphere Web Client, select "Virtual Machines". Right click the "vSphere Management Assistant" and select "Open Console".



3. Set the Acceptance Level by executing the following command.

```
>sudo esxcli -s 192.168.100.2 -u root -p password software acceptance set  
--level=PartnerSupported
```

4. Install the MPM(syslog,IPMI) by executing the following commands.

```
>sudo esxcli -s 192.168.100.2 -u root -p password software vib install -f
-v /vmfs/volumes/datastore1/vmware-esx-esxcli-getsyslog-500.1.0-
xxxxxx.vib
>sudo esxcli -s 192.168.100.2 -u root -p password software vib install -f
-v /vmfs/volumes/datastore1/vmware-esx-esxcli-miacat-500.1.0-
xxxxxx.vib
```

Installed software can be confirmed by following commands.
After restarting Hypervisor they are displayed, they are not displayed immediately after installation.

("getsyslog" (MPM-syslog) and "miacat-plugin" (MPM-IPMI) is displayed.)

```
>sudo esxcli -s 192.168.100.2 -u root -p password software vib list | grep HITACHI
getsyslog          500.1.0-000002          HITACHI  PartnerSupported  2012-10-
02
miacat-plugin      500.1.0-000003          HITACHI  PartnerSupported  2012-10-
02
>
```

Copying the software from the datastore to vMA

Copy the following files from the datastore to the "/tmp" of vMA.

- miacat-vma-install-xxxx.tar.gz (Event Management Tool)
- selman-vma-install-xxxx.tar.gz (Event Management Tool(Service))
(Only for Compute Rack)
- MIACAT_BSVMA-xxxx-x.i586.rpm (log monitor for vMA (for Compute Blade))
or
MIACAT_HAVMA-xxxx-x.i386.rpm (log monitor for vMA (for Compute Rack))

"x"(Italic font): Alphanumeric characters, such as a version number

1. With vSphere Client or vSphere Web Client, open the console of vMA.
(Login by vi-admin user.)
2. Copy the files to "/tmp" of vMA by executing following commands.
(The file of log monitor for Compute Blade are different from the file for Compute Rack.)

```
>sudo scp root@192.168.100.2:/vmfs/volumes/datastore1/miacat-vma-install-xxxx.tar.gz /tmp  
(Enter the password for Hypervisor root user)  
  
>sudo scp root@192.168.100.2:/vmfs/volumes/datastore1/selman-vma-install-xxxx.tar.gz /tmp  
(Enter the password for Hypervisor root user)  
  
>sudo scp root@192.168.100.2:/vmfs/volumes/datastore1/MIACAT_BSVMA-xxxx-x.i586.rpm /tmp  
~The case of Compute Blade~  
(Enter the password for Hypervisor root user)
```

Installing the Event Management Tool in the vMA

Install the Event Management Tool copied to "/tmp".

1. With vSphere Client or vSphere Web Client, open the console of vMA.
(Login by vi-admin user.)
2. Expand the files by executing the following command.

```
>cd /tmp
>sudo tar pxzvf miacat-vma-install-xxxx.tar.gz
```

3. Install the Event Management Tool by executing the following commands.

```
>cd miacat-vma-install/
>sudo ./miacat-vma-install-0000.sh
```

4. Set the Hypervisor IP address and password of the root user to the Event Management Tool by executing the following commands.
Note: Execute this command again, when Hypervisor password is changed after this setting.

```
>sudo chmod 755 -R /opt/hitachi/tools/miacat
>sudo /opt/hitachi/tools/miacat/setServerInfo Set -s 192.168.100.2 -u root -p
password
```

- Current setting is displayed when "sudo /opt/hitachi/tools/miacat/setServerInfo Get" is executed.
- When following characters are used for the password, enclose the whole password by " ' " (single quotation mark), and add "\" before each character.
Characters: ;&()|^<>?*[]\$`"\!{} [space]

5. Only for Compute Rack, install the system event log(SEL) collection functions.
(This procedure is unnecessary for Compute Blade)

```
>cd /tmp
>sudo tar pxzvf selman-vma-install-xxxx.tar.gz
>cd selman-vma-install-xxxx/
>sudo ./VmwSelMan.sh
```

Restarting VMware(Hypervisor)

Restart VMware(Hypervisor) surely.
Otherwise, installation of log monitor for vMA fails.

Overview

Log monitor for vMA can collect maintenance information and can analyze hardware problems through the log data on the VMware vSphere Hypervisor (hereinafter describes Hypervisor), 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 for vMA, quick failure restoration is available and system availability improves.



Log monitor for vMA can detect much failure than log monitor which works on guest OS (Windows or Linux). Please refer to the "[Detectable failure](#)".

Functions

This section explains the log monitor function for vMA.

Collecting and analyzing the failure information and maintenance information

Log monitor watches the Hypervisor log, and generating the failure event code when the failure event is detected.

On Compute Rack series, it watches not only the Hypervisor log but also the event of the system unit (SEL).

(The SVP watches SEL of the system unit on Compute Blade)

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.

Installation of the log monitor for vMA

This section explains the installation procedure of the log monitor for vMA.

[Operation flow]

- [Installation the log monitor for vMA](#)
- [Setting of the log monitor for vMA \(only for Compute Blade\)](#)
- [Operation confirmation of the log monitor for vMA](#)

[The supplement about operation explanation]

In this operation explanation, IP address of the Hypervisor is "192.168.100.2", VMware datastore name is "datastore1", Hypervisor root password is "password", IP address of the vMA is "192.168.100.10" . Please replace the value according to the customer's environment.

After entering a command on vMA, there is a case that "vi-admin's password:" or "Password:" is displayed and entering the password is required.

Please enter the password for vi-admin user used for login to the vMA when "vi-admin's password:" is displayed.

Please enter the password for the root user of Hypervisor when "Password:" is displayed.

Installation of the log monitor for vMA

This section explains the installation procedure of log monitor for vMA.



Upgrade installation of the log monitor for vMA is impossible on Compute Blade. Install it after uninstallation surely.

1. With vSphere Client, select the "Console" tab of vMA.
(Login by vi-admin user.)
2. Install the log monitor for vMA by executing the following commands.

The case of Compute Blade:

```
sudo rpm -ivh /tmp/MIACAT_BSVMA-xxxx-x.i586.rpm
```

The case of new installation of Compute Rack:

```
sudo rpm -ivh /tmp/MIACAT_HAVMA-xxxx-x.i386.rpm
```

The case of upgrade installation of Compute Rack:

```
sudo rpm -Uvh /tmp/MIACAT_HAVMA-xxxx-x.i386.rpm
```

"x"(Italic font): Alphanumeric characters, such as a version number

If the installation fails, following messages are displayed.

Message	Meaning and action(if necessary)
package MIACAT_xxVMA-xxxx-x is already installed	Log monitor for vMA has already been installed. Action: [Compute Blade] When installing again, uninstall it. [Compute Rack] Upgrade install.
Failed. You are not root user.	The user is not "root". Action: Change the user to "root" and install it.
Failed. ipmiRawCmd command not found.	Required software of Event Management Tool is not installed. Action: Install the Event Management Tool and install it again.
Failed. ipmiRawCmd command failed. (Command Error)	Operation of the Event Management Tool fails. - Restarting of the VMware(Hypervisor) is not performed after installation of the required software. - Setting of the Event Management Tool is incorrect. Action: Restart the VMware(Hypervisor), or set the Event Management Tool setting again.
"MIACAT Plug-in Module" is not installed.	Required software is not installed. Action: Install the required software and install it again.

Setting of the log monitor for vMA (only for Compute Blade)

This section explains the setting procedure of the log monitor for vMA on Compute Blade.

1. With vSphere Client, select the "Console" tab of vMA.
(Login by vi-admin user.)
2. Change the setting of the log monitor for vMA by executing the following commands.

```
> sudo chmod 755 -R /opt/hitachi/miacat/Program    <-Set the execution
authorization
> sudo /opt/hitachi/miacat/Program/mpmsetup.sh    <-Execute the setting script

-----
MIACAT Setup tool.
  All Rights Reserved. Copyright (C) 2006,2012, Hitachi, Ltd.
-----

Please choose Server Model of the use.
  1. BS320 / CB320
  2. BS500 / CB500
  3. BS2000 / CB2000
(1-3,q) : 2    <-Select the system

Confirm Data.
  Server Model : BS500 / CB500
Do you update this configuration ?
(y|n|n) : y    <-select "y" when the selection is correct (When "n" is selected,
the setting is
terminated)
Do you start agent program?
(y|n|n) : y    <-Select "y" to start the Log Monitor (It doesn't start when "n"
is
selected)
Starting VmSyslogMAgtSrvd services: done
Please wait for a while...
Starting SMAL2MASvc services: done
Setup was completed. <-Setting is completed
```

If the setting fails, following messages are displayed.

Message	Meaning and action(if necessary)
It is initialization. The test report demand was canceled.	The setting or connection confirmation is canceled, because the service is under initializing. Action: Execute the connection confirmation again after 10 or more minutes from installation or starting the service.
Failed in the SEL output.	Setting information or failure event code can not be recorded in the management module. Action: Confirm whether the System event (SEL) Management Tool of Required software is installed.
Because the number of accumulation of alert report demands was exceeded, it was annulled.	The setting or connection confirmation is not received, because the event detection is under processing. Action: Wait 10 or more minutes, and execute it again.

Operation confirmation of the log monitor for vMA

[Operation confirmation on Compute Blade/Compute Rack common]

Please check that the updated date of the following file, which is on vMA, is the time of after the installation of the log monitor.

- /opt/hitachi/tools/miacat/vmkernel.log
(vmkernel.log on Hypervisor gotten when starting the log monitor)

Check the following operations when the updated date is not updated.

- " Syslog.global.logDir" and "Syslog.global.logDirUnique" settings of the "[Enabling the transferring of the Hypervisor syslog message](#)"
- Installation of the MPM-syslog of the "[Installing the MPM in the Hypervisor](#)".

[Operation confirmation on Compute Blade]

This section explains the procedure of connection confirmation between log monitor for vMA and the management module on Compute Blade.

1. With vSphere Client, select the "Console" tab of vMA.
(Login by vi-admin user.)
2. Confirm the operation by executing the following commands.

```
> sudo /opt/hitachi/miacat/Program/MRegCUI    <-Execute the connection
confirmation tool
Please choose function.

  1. Check connection with an obstacle report service center.
  2. Display current optional configuration.
  3. Change optional configuration.

(1-3,Quit): 1    <-Enter "1"

As for this connection verification because log file transmission is not done,
doing fire wall setting, it completes.

Do you check connection ?
(Yes,[No]): y    <-Enter "y"

Check connection ...

Connection check succeeded. <-Connection confirmation is completed
```

[Operation confirmation on Compute Rack]

Restart the system unit.

Confirm that the failure analysis result code (RC) is generated after restarting.

About the procedure of confirming the failure analysis result code (RC), refer to "[Referring to the failure analysis code \(RC\) \(only for Compute Rack\)](#)"

Uninstallation

This section explains uninstallation procedure.

- [Uninstallation of the MPM](#)
- [Uninstallation of the Event Management Tool](#)
- [Uninstallation of the log monitor for vMA](#)

Uninstallation of the MPM

This section explains the uninstallation procedure of the MPM.

1. With vSphere Client, select the "Console" tab of vMA.
(Login by vi-admin user.)
2. Uninstall the MPM(syslog,IPMI) by executing the following commands.

```
>sudo esxcli -s 192.168.100.2 -u root -p password software vib remove -f  
-n getsyslog  
>sudo esxcli -s 192.168.100.2 -u root -p password software vib remove -f  
-n miacat-plugin
```

3. Restart the system unit (VMware).

Uninstallation of the Event Management Tool

This section explains the uninstallation procedure of the Event Management Tool.

1. With vSphere Client, select the "Console" tab of vMA.
(Login by vi-admin user.)
2. Uninstall the Event Management Tool by executing the following commands.

```
>sudo /opt/hitachi/SelManager/UninstSelMan.sh  
>sudo rm /opt/hitachi/tools/miacat/*  
>sudo rmdir /opt/hitachi/tools/miacat
```

Uninstallation of the log monitor for vMA

This section explains the uninstallation procedure of the log monitor for vMA.

1. With vSphere Client, select the "Console" tab of vMA.
(Login by vi-admin user.)
2. Execute the following commands

The case of Compute Blade:

```
sudo rpm -e MIACAT_BSVMA
```

The case of Compute Rack:

```
sudo rpm -e MIACAT_HAVMA
```

Confirmation of the version

This section explains the confirmation procedure of the version.

Confirmation of the MPM version

This section explains the confirmation procedure of the MPM version.

1. With vSphere Client, select the "Console" tab of vMA.
(Login by vi-admin user.)
2. Execute the following command.
("getsyslog"(MPM-syslog) and "miacat-plugin"(MPM-IPMI) are displayed.)

```
>sudo esxcli -s 192.168.100.2 -u root -p password software vib list | grep HITACHI
getsyslog      500.1.0-000002      HITACHI  PartnerSupported  2012-10-02
miacat-plugin  500.1.0-000003      HITACHI  PartnerSupported  2012-10-02
>
```

Confirmation of the log monitor for vMA version

This section explains the confirmation procedure of the log monitor version.

1. With vSphere Client, select the "Console" tab of vMA.
(Login by vi-admin user.)
2. Execute the following command.

The case of Compute Blade:

```
sudo rpm -qi MIACAT_BSVMA
```

The case of Compute Rack:

```
sudo rpm -qi MIACAT_HAVMA
```

3. The version number is displayed at the "Version".

Operation of the log monitor for vMA

This chapter explains the operation of the log monitor for vMA.

- [Referring to the failure analysis result code \(RC\) \(only for Compute Rack\)](#)

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

This section explains the procedure to refer to the failure analysis result code (RC).



On Compute Blade, the failure analysis code (RC) can be referred by the management module.

1. With vSphere Client, select the "Console" tab of vMA.
(Login by vi-admin user.)
2. Start the RC Viewer by executing the following command.

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

3. Failure analysis code (RC) is displayed.

```
MODEL CODE : N/A / PRODUCT No. : N/A
MODEL NAME : HA8000/TS20AM
MODEL FRU  : 0020T20500
RC DICT   : xm_ts20_10-hxm_25/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 15:23:33   10 2000 AC 042F0BF1 0BA1FFFF
      Time stamp          Failure analysis code(RC)
-- (q:quit) --
```

4. Enter "q" and quit the RC Viewer.



A

Appendix

This chapter explains the list of the message and the list of the installed files.

- [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 for vMA.

- [List of the syslog messages of the log monitor for Compute Blade](#)
- [List of the syslog messages of the log monitor for Compute Rack](#)

List of the syslog messages of the log monitor for Compute Blade

This section explains the list of the messages, which the log monitor for vMA outputs on the Compute Blade.

Message of the log monitor is displayed with the tag name "SMAL2_MainteAgtSvc".

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

The list of the message is described below.

Message	Meaning and action(if necessary)
[INFO]----- Maintenance Agent Service Start - -----	Log monitor is start up.
[INFO]----- Maintenance Agent Service Preparation completion. -----	IPMI command is ready
[INFO]----- Maintenance Agent Service End --- --	Log monitor is exited
[INFO]----- Service Start -----	Log monitor was started.
[INFO]----- Preparation completion. -----	The preparation of IPMI command was completed.
[INFO]----- Service End -----	Log monitor was stopped.
[INFO] SEL was written in BMC.,Date:xxxx/xx/xx xx:xx:xx,SEL:xxxxxxxxxxxxxxxx	SEL outputs succeed.
[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, Detail:xxxxxxxx), Date:xxxx/xx/xx xx:xx:xx, SEL:xxxxxxxxxxxxxxxx	SEL output fails. Action: Confirm Event Management Tool 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 syslog messages of the log monitor for Compute Rack

This section explains the list of the messages, which the log monitor for vMA outputs on the Compute Rack.

Message of the log monitor is displayed with the tag name "SMAL2_MainteAgtSvc".

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

The list of the message is described below.

Message	Meaning and action(if necessary)
[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 for vMA.

Log monitor for vMA for CB

```
/opt/hitachi/miacat
| - MainteData <-Folder to store the definition and setting
| - Program <-Folder of service program (The files in this folder are unchanged.)
/opt/hitachi/VmSyslogMAgt.Srvd
| - bin <-Folder of sub program (The files are unchanged.)
| - data <-Folder to store the definition and setting of sub program
/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.)
/var/opt/hitachi/VmSyslogMAgt.Srvd
| - 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.)
```

Log monitor for vMA for CR

```
/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	Fiber 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

