

Hitachi Compute Blade 2500 Series

Logical partitioning manager User Guide

FASTFIND LINKS

[Document Organization](#)

[Product Version](#)

[Getting Help](#)

[Contents](#)

© 2014-2020 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	xi
Intended Audience	xii
Product Version	xii
Release Notes	xii
Document Organization	xii
Referenced Documents	xiii
Document Conventions	xiv
Conventions for storage capacity values	xv
Safety information	xvi
Getting help	xvi
Comments	xvi
1 Overview of LPAR manager	1-1
Logical partitioning of hardware resources	1-2
Physical and logical resources	1-2
Dedicated and shared use of logically partitioned resources	1-2
Operating mode of the server blades	1-4
OSs running on LPARs	1-4
Features of processors logically partitioned by LPAR manager	1-4
Features of memory that is logically partitioned by LPAR manager	1-5
Features of PCI devices that are logically partitioned by LPAR manager	1-7
Dedicated NIC	1-7
Shared NIC	1-8
VF NIC	1-9
Virtual NIC	1-10
Dedicated FC	1-11
Shared FC	1-11
Management path and operation path	1-12
NIC to be used for management path communication	1-13
When omit configure the NIC for management path communication	1-14
Influence when management path communication is not available	1-16
Notes on communication on the management path	1-17
CB 520X NIC configuration and assignment example	1-19
CB 520H NIC configuration and assignment example	1-21
Configuration example of a network path on which VLANs are used	1-22
LPAR manager system requirements	1-24

Server blades supported by LPAR manager	1-24
Guest OSs supported by LPAR manager	1-25
Memory for LPAR manager	1-27
General procedure from installing LPAR manager to operating LPARs	1-28
Notes on configuring and operating logical environments	1-29
Notes when hardware resources are blocked or enter reduced-operation mode	1-29
Notes on logical NICs	1-30
Multicast communication errors	1-34
Notes on FC configurations	1-35
Notes on USB devices	1-36
SMP configuration	1-38
Maximum resolution of a remote console	1-39
2 Starting and Stopping LPAR manager	2-1
Preparing the server blades so that they can operate in LP mode	2-2
Connecting to the management paths	2-2
Checking and setting the LPAR manager firmware	2-3
Setting the operation mode and network address	2-3
Checking the status of a server blade	2-6
Checking the virtual WWN of a server blade	2-6
Checking the virtual MAC address of a server blade	2-6
Configuring the address for communication between a management tool and LPAR manager	2-7
Starting LPAR manager	2-7
Restarting LPAR manager	2-9
Stopping LPAR manager	2-9
3 Creating LPARs	3-1
Creating LPARs	3-2
Setting NUMA	3-3
Setting the boot order for LPARs from the Web console	3-4
Setting the boot order	3-4
Connecting virtual drives	3-5
Setting up the HBA boot driver	3-6
Setting the boot order for LPARs from UEFI	3-7
Setting up the UEFI driver	3-7
Creating a boot option	3-10
Changing the boot order	3-12
Deleting a boot option	3-12
Changing the configuration of an LPAR	3-13
Saving the LPAR manager configuration	3-13
Deleting LPARs	3-14
4 Starting and Stopping LPARs	4-1
Activating an LPAR	4-2
Reactivating an LPAR	4-2
Deactivating an LPAR	4-2
5 Setting Processors and Memory Functionality	5-1
Setting the service ratio of a physical processor	5-2

Service ratio	5-2
Setting the service ratio	5-2
Setting the idle-detection functionality for processors	5-3
What is the detection of an idle state?	5-3
Detecting an idle state	5-3
Setting up processor capping	5-4
What is processor capping?	5-4
Setting up processor capping	5-4
Setting up a processor group	5-5
What is a processor group?	5-5
Adding a processor group	5-5
Assigning an LPAR to a processor group	5-5
Assigning a physical processor to a processor group	5-6
Setting a name for a processor group	5-6
Deleting a processor group	5-6
Performance tuning options	5-7
System requirements	5-7
How the set values change due to the application of Performance tuning options	5-8
Notes	5-9
Enabling Performance tuning options	5-10
Enabling hyper-threading	5-10
Features of processors for which hyper-threading is enabled	5-10
Checking the core information of physical processors	5-11
What is a core scheduling?	5-11
Enabling the PRTE function	5-12
Applying NUMA to an LPAR	5-14
Applying NUMA	5-14
Enabling NUMA for an LPAR	5-15
Specifying a memory node	5-18
Automatic memory allocation and specification of a node	5-18
Setting a memory allocation type for an LPAR	5-19
Applying the L3 cache allocation functionality	5-19
What is the L3 cache allocation functionality?	5-19
Enabling the L3 cache allocation functionality	5-20
6 Setting the Functionality for PCI Devices	6-1
Enabling the SR-IOV functionality and using VF NICs	6-2
Notes on using the SR-IOV functionality	6-2
Performing an FCoE boot by enabling the FCoE functionality	6-4
Creating more segments than there are physical NICs	6-4
Changing scheduling mode of a physical NIC to dedicated mode or shared mode for a port	6-4
Dedicated port functionality	6-5
Support requirements for the dedicated port functionality	6-5
Enabling the dedicated port functionality	6-5
Disabling the dedicated port functionality	6-6
Notes on the dedicated port functionality	6-6
VLAN functionality using shared and virtual NICs	6-6
Using inter-LPAR communication	6-15
Inter-LPAR communication packet filtering	6-15
Configuring inter-LPAR communication packet filtering	6-16

Using teaming functionality to build redundancy into the NIC configuration	6-16
Teaming functionality	6-16
Notes on using inter-LPAR communication in a redundant network configuration	6-17
Monitoring data by using promiscuous mode	6-18
Maintaining the I/O performance by using the HBA dedicated core mode of shared FCs	6-20
HBA dedicated core mode of shared FCs	6-20
Requirements for HBA-core dedicated mode	6-21
Maintaining the I/O performance by using HBA-core dedicated mode	6-21
Notes on HBA-core dedicated mode	6-21
Using N+M cold standby (LUID mode) to start LPARs	6-22
What is N+M cold standby (LUID mode)?	6-22
Requirements to support N+M cold standby (LUID mode)	6-22
Setting N+M cold standby (LUID mode)	6-23
Notes on N+M cold standby (LUID mode)	6-24
7 Controlling access to the LPAR manager functions	7-1
Restricting LPAR manager operations by using Role Based Access Control	7-2
User and roles that can be assigned	7-3
Role types	7-3
Editing role privileges	7-4
Setting a role for the management module users	7-5
Privileges of LPAR manager supported	7-6
LPAR manager security permission	7-6
Performing operations on LPAR manager from the management module	7-8
Logging in to LPAR manager on the Web console	7-8
Notes on performing Role Based Access Control	7-9
Authenticating LPAR manager users	7-9
Overview of user authentication	7-9
Enabling user authentication	7-11
Collecting user authentication log data	7-12
Authenticating a local user by using LPAR manager	7-12
Initially registered user account for local authentication	7-13
Creating a local user	7-13
Deleting a local user	7-14
Changing a password or role for local user	7-15
Setting a validity period for the password of a local user	7-17
When the password expires	7-18
Authenticating a user by using LDAP	7-19
Support requirements for LDAP authentication	7-19
Enabling LDAP authentication	7-20
Setting LDAP information	7-21
Authenticating a user by using RADIUS	7-21
Support requirements for RADIUS authentication	7-22
Enabling RADIUS authentication	7-23
Setting RADIUS information	7-23
Verifying connection with the RADIUS server	7-24
8 Managing LPAR manager and LPARs	8-1
Setting the ports to be used for management path communication	8-3

What is the management path specification functionality?	8-3
Specifying the ports to be used for management path communication	8-4
Confirming the communication statuses of management paths	8-5
Diagnosis of the standby port of management paths	8-6
Switching the active port of the management path	8-7
Monitoring the link status of the active port of the management path	8-7
Displaying the LPAR manager screen and the guest screen	8-8
OS console and virtual COM console for displaying screens	8-8
Using the OS console to display the LPAR manager screen	8-9
Notes on using the virtual COM console	8-9
Configuring the terminal software	8-10
Enabling the virtual COM console functionality	8-11
Using the virtual COM console to display the guest screen	8-11
LP communication settings	8-12
Setting the port numbers for LPAR manager management and communication	8-13
Encrypting communication of the LPAR manager	8-13
Encrypting communication with the virtual COM console	8-13
Re-creating an SSH host key	8-14
Initializing the LPAR manager configuration	8-14
Backing up and restoring the LPAR manager configuration information	8-14
Before backing up the LPAR manager configuration	8-14
Backing up the LPAR manager configuration as of a time before device isolation	8-16
Backing up the LPAR manager configuration	8-17
Restoring the LPAR manager configuration	8-18
Updating LPAR manager firmware	8-18
Relationship between server blades and LPAR manager firmware	8-19
Performing a version upgrade of LPAR manager firmware	8-20
Installing LPAR manager firmware	8-20
Updating LPAR manager firmware	8-21
Uninstalling LPAR manager firmware	8-21
Linking with management software	8-21
Linkage with HCSM	8-21
Linkage with HVM Navigator	8-22
N+M cold standby	8-22
HA monitor and LPAR manager	8-25
Use of USB devices with the server blade	8-25
Setting the times handled by LPAR manager	8-26
Times handled by LPAR manager	8-26
Setting NTP time synchronization for the LPAR manager system time	8-29
Logical VGA snapshot	8-29
Viewing the LPAR manager system logs	8-30
Collecting audit logs	8-31
Support requirements for collecting audit logs system	8-31
Format of audit logs	8-32
Enabling the collection of audit logs	8-35
Specifying the DNS server	8-36

9 Maintaining LPAR manager and LPARs	9-1
Migration between basic and LPAR manager environments	9-2
Settings and items to be confirmed during migration from Basic mode to LP mode	9-2

Settings and items to be confirmed during migration from LP mode to Basic mode	9-2
Notes on migration between Basic mode and LP mode	9-3
Upgrading LPAR manager licenses	9-3
Requesting an LPAR manager license key	9-3
Registering LPAR manager license keys directly	9-4
Registering LPAR manager license keys by loading a license key file	9-4
Notes on temporary LPAR manager licenses	9-4
LPAR manager security	9-5
Using certificates in LPAR manager	9-5
Server certificate issued by LPAR manager	9-6
Creating signed server certificates	9-7
Authenticating other systems	9-9
About security on LPAR manager features and tools that used management network	9-10
Collecting a memory dump of a guest OS	9-14
Guest memory dump collection	9-14
Specifications of guest memory dump collection command	9-14
Executing the guest memory dump collection command	9-16
Notes on using the guest memory dump collection command	9-16
Collecting LPAR manager failure information from the Web console	9-17
Collecting LPAR manager dumps	9-18
Overview of LPAR manager dump collection	9-18
Specifications of LPAR manager dump collection commands	9-18
Executing the LPAR manager dump collection commands	9-19
Notes on using the LPAR manager dump collection commands	9-20
LPAR Migration	9-20
Safe mode	9-20
Checking whether LPAR manager is running in safe mode	9-21
Exiting safe mode	9-22
Collecting SYS2 dump files	9-22
10 LPAR manager Screen	10-1
Operations and roles of the keys used to manipulate the LPAR manager screen	10-3
Names and usages of the LPAR manager screen	10-3
Screen names and usages	10-3
Items common to the LPAR manager screen	10-5
LPAR manager Menu screen	10-5
Logical Partition Configuration screen	10-8
Logical Processor Configuration screen	10-20
Physical Processor Configuration screen	10-23
PCI Device Information screen	10-26
PCI Device Assignment screen	10-30
Virtual NIC Assignment screen	10-34
Shared FC Assignment screen	10-42
Allocated FC Information screen	10-45
System Configuration screen	10-47
System Service State screen	10-58
Date and Time screen	10-63
LP Options screen	10-74
LPAR Usage screen	10-81
Front Panel screen	10-86

LP System Logs screen	10-89
Firmware Version Information screen	10-91
LPAR manager sub-screens	10-92
Memory Allocation Display sub-screen	10-93
11 LPAR manager Messages	11-1
LPAR manager boot messages	11-2
LPAR manager screen operation messages	11-7
LPAR manager system log messages	11-17
Error log messages for the LPAR manager system	11-17
Warning log messages for the LPAR manager system	11-23
Information log messages for the LPAR manager system	11-28
Audit log messages	11-34
Notation used in audit log messages	11-34
Lists of audit log messages	11-35
HCSM alert messages	11-72
HCSM alert message format	11-72
List of HCSM alert messages	11-72
A Software License Information	A-1
Software License Information	A-2
B Functionality Supported by LPAR manager	B-1
List of PCI devices supported by LPAR manager	B-2
List of functionality supported by LPAR manager	B-4
SR-IOV functionality supported by LPAR manager	B-12
Dedicated port functionality supported by LPAR manager	B-19
LPAR manager licenses	B-21
Differences in supported items depending on the guest OSs	B-22
C LPAR manager Setting Items List	C-1
LPAR manager setting items	C-2
EFI driver setting items	C-7
D Available Consoles in LPAR manager	D-1
Relationship between consoles and the functionality of LPAR manager	D-2
E Port numbers used by LPAR manager	E-1
Port numbers used for communication with the management server	E-2
Port numbers used for communication with a management module	E-3
Port numbers used for LPAR migration	E-5

Glossary

Index



Preface

This document describes how to use the Compute Blade 2500 series.

This preface includes the following information:

Notice: The use of Compute Blade 2500 series and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

- ☐ [Intended Audience](#)
- ☐ [Product Version](#)
- ☐ [Release Notes](#)
- ☐ [Document Organization](#)
- ☐ [Referenced Documents](#)
- ☐ [Document Conventions](#)
- ☐ [Conventions for storage capacity values](#)
- ☐ [Safety information](#)
- ☐ [Getting help](#)
- ☐ [Comments](#)

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 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 will be installed, including knowledge of physical characteristics, power systems and specifications, and environmental specifications.

Product Version

This document revision applies to Logical partitioning manager 02-69.

Release Notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document.

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, Overview of LPAR manager	Provides an overview of LPAR manager.
Chapter 2, Starting and Stopping LPAR manager	Describes how to start and stop LPAR manager running on server blades. This chapter also describes how to restart LPAR manager.
Chapter 3, Creating LPARs	Describes how to create LPARs.
Chapter 4, Starting and Stopping LPARs	Describes how to start and stop LPARs. This chapter also describes how to restart LPARs.
Chapter 5, Setting Processors and Memory Functionality	Describes processors that are assigned to LPARs, the functionality that can be set for memory, and how to set the functionality.
Chapter 6, Setting the Functionality for PCI Devices	Describes the functionality that can be set for the PCI devices that are assigned to LPARs, and describes how to set up the functionality.

Chapter	Description
Chapter 7, Managing LPAR manager and LPARs	Describes the functionality for managing LPAR manager and LPARs, and how to set the functionality.
Chapter 8, Maintaining LPAR manager and LPARs	Describes the functionality for maintaining LPAR manager and LPARs.
Chapter 9, LPAR manager Screen	Describes the configuration and items displayed on the LPAR manager screen. In addition, the configuration and items displayed on the sub-screens that open from the LPAR manager screen are also described.
Chapter 10, LPAR manager Messages	Describes messages output by LPAR manager and HCSM alarm messages.
Appendix A, Software License Information	Provides software license information.
Appendix B, Functionality Supported by LPAR manager	Describes PCI devices, their functionality, and the SR-IOV functionality supported by LPAR manager.
Appendix C, LPAR manager Setting Items List	Describes the list of LPAR manager setting items.
Appendix D, Available Consoles in LPAR manager	Describes the functionality of LPAR manager for each console that can be used in LPAR manager.
Appendix E, Port numbers used by LPAR manager	Describes the port numbers that LPAR manager uses to communicate with modules and external programs.

Referenced Documents

- Hitachi Compute Blade 2500 Series Getting Started Guide, MK-99CB2500003
- Hitachi Compute Blade 2500 Series Management Module User Guide, MK-99CB2500004
- Hitachi Compute Blade 2500 Series UEFI Setup Guide, MK-99CB2500005
- Hitachi Compute Blade Series Hitachi Compute Rack Series OS Installation Guide for Windows Server, MK-99COM076
- Hitachi Compute Blade Series OS Installation Guide for Red Hat Enterprise Linux, MK-99COM141
- Hitachi Compute Blade Emulex Adapter User's Guide for Driver, MK-99COM103
- Hitachi Compute Blade Emulex Adapter User's Guide for Hardware, MK-99COM104
- Server installation and monitoring tool OS Setup Guide, MK-99COM061
- Hitachi Gigabit Fibre Channel Adapter USER'S GUIDE (BIOS/EFI Edition)
- Hitachi Compute Blade HVM Navigator User's Guide - Getting Started, MK-99COM022

- Hitachi Compute Blade HVM Navigator Installation Manual, MK-99COM023
- Hitachi Compute Blade HVM Navigator User's Guide - LPAR Configuration, MK-99COM042
- Hitachi Compute Blade HVM Navigator User's Guide - Monitoring, MK-99COM025
- Hitachi Compute Blade HVM Navigator User's Guide - Viewer, MK-99COM027
- Hitachi Compute Blade HVM Navigator User's Guide - Migration, MK-99COM024
- Hitachi Compute Blade HVM Navigator User's Guide - Operation Quick Reference, MK-99COM026
- Hitachi Compute Blade LPAR Migration Guide, MK-99COM194
- Hitachi Compute Blade Logical VGA SnapShot, MK-99COM074
- HVM Management Command (HvmSh) Operation Guide, MK-99COM015
- Hitachi Command Suite Compute Systems Manager User Guide

Document Conventions





The term "Compute Blade" refers to all the models of the Compute Blade, 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
< > (angle brackets)	Variable (used when italic is not enough to identify variable)
[] (square brackets)	Optional value
{ } (braces)	Required or expected value
(vertical bar)	Choice between two or more options or arguments.

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

Icon	Meaning	Description
 WARNING	WARNING	This indicates the presence of a potential risk that might cause death or severe injury.
 CAUTION	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	Note	Calls attention to important or additional information.
 Tip	Tip	This indicates advice on how to make the best use of the equipment.

The following table shows abbreviations of logical partitioning manager and logical partition.

Term	Abbreviation
logical partitioning manager	LPAR manager or LP
logical partition	LPAR

Conventions for storage capacity values

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

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

Logical 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

Logical capacity unit	Value
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

Safety information

Before replacement, read the Safety Guidelines in this document.

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>

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!

Overview of LPAR manager

This chapter provides an overview of LPAR manager.

- ☐ [Logical partitioning of hardware resources](#)
- ☐ [Features of processors logically partitioned by LPAR manager](#)
- ☐ [Features of memory that is logically partitioned by LPAR manager](#)
- ☐ [Features of PCI devices that are logically partitioned by LPAR manager](#)
- ☐ [Management path and operation path](#)
- ☐ [LPAR manager system requirements](#)
- ☐ [General procedure from installing LPAR manager to operating LPARs](#)
- ☐ [Notes on configuring and operating logical environments](#)

Logical partitioning of hardware resources

LPAR manager is software that can logically partition the resources of one server blade and configure multiple server environments. Server environments that are generated from logically partitioned resources are called LPARs.

The following figure shows the concept for a system configuration in which LPAR manager runs.

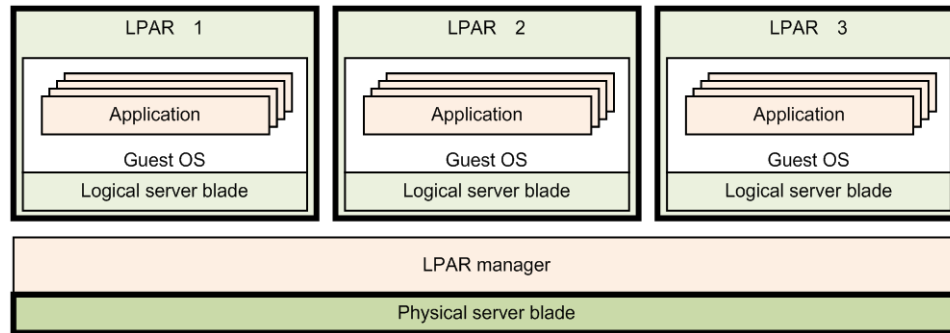


Figure 1-1 Concept of LPAR operation when the system is booted in LP mode

Physical and logical resources

Unless otherwise noted, this manual uses the terms "physical" and "logical" as defined in the following table.

- **Physical**
Indicates resources that actually exist in the system. "Physical" is sometimes omitted, except where doing so would cause confusion.
- **Logical**
Indicates logical resources that appear to exist on an LPAR or for software on LPARs. For each logical resource, an actual resource might or might not exist.

Dedicated and shared use of logically partitioned resources

When allocating logically partitioned hardware resources to LPARs, you can specify an allocation type for each hardware resource: dedicated use by a single LPAR or shared use among multiple LPARs. These types for allocating logically partitioned hardware resources are called "dedicated mode" and "shared mode". In addition, there is an allocation type called exclusively shared mode. In this mode, a single hardware resource is shared among multiple LPARs, but it is used exclusively. These modes are explained below.

- **Dedicated mode**
In this mode, a hardware resource is allocated to an LPAR for dedicated use by that LPAR. A feature of this mode is that the hardware resource can always be used with stable performance. In addition, a hardware

resource that is allocated to an LPAR in dedicated mode cannot be allocated to other LPARs.

- The processing speed is higher than the speed in shared mode.
- If you allocate hardware resources to LPARs in dedicated mode, you can create LPARs that require fast processing and high I/O performance, as well as LPARs that have critical time periods and processing needs related to performance.
- You cannot assign the ports of an I/O adapter that has multiple ports to a different LPAR in dedicated mode. However, if the dedicated port functionality is enabled, you can assign a port of your choice in dedicated mode.
- To change the LPAR that has dedicated use of a hardware resource, stop the LPAR and change the configuration definition.

- Shared mode

In this mode, a logically partitioned hardware resource is allocated to multiple LPARs for shared use. A benefit of this mode is that hardware costs can be reduced because hardware resources are shared among multiple LPARs.

A hardware resource can be shared by finely dividing and distributing the time that each LPAR uses the resource. LPAR manager divides the time each LPAR can use a hardware resource and transfers the right to use that resource to the LPAR.

- If you allocate processors in shared mode, you can create LPARs that require cost efficiency and flexibility, as well as LPARs that require balanced processing between logically partitioned systems.
- If there is a high load on a processor or a PCI device of an LPAR, other LPARs to which the resource is allocated in shared mode might experience severe degradation of processing performance.

- Exclusively shared mode

Similar to shared mode, a single hardware resource can be shared among multiple LPARs, but the hardware resource is not shared in a time-sharing schedule. While a hardware resource is being used by an LPAR, the hardware resource cannot be used by other LPARs.

- You can switch the LPAR to which a USB device is connected while the LPARs are running.
- For CB 520X B1/B2/B3, devices connected via the KVM connector and the remote console are always assigned in exclusively shared mode.
- For CB 520H B3/B4, devices connected to the USB port on the front interface of the server blade, devices connected via the KVM connector, and the remote console are always assigned in exclusively shared mode.

In this document, the USB port on the front interface of the server blade is called the front USB port.

There are different types of logical partitioning that can be set for each hardware resource. The following table shows hardware resources and logical partitioning types that can be set.

Table 1-1 Hardware resources and logical partitioning types

Hardware resource	Type of logical partitioning		
	Dedicated	Shared	Exclusively shared
Processor	Y	Y	N
Memory	Y	N	N
PCI device	Y	Y	N
USB device connected to the front USB port	CB 520X B1/B2/B3: Y CB 520H B3/B4: N	N	CB 520X B1/B2/B3: N CB 520H B3/B4: Y
Device connected via the KVM connector	N	N	Y
Remote console	N	N	Y
Legend: Y: Can be used. N: Cannot be used.			

Operating mode of the server blades

The operating mode of the server blades on which LPAR manager is running is called *LP mode*. On the other hand, the operating mode of the server blades on which LPAR manager is not running is called Basic mode. To set up LPAR manager and configure LPARs, first set the server blade to LP mode.

OSs running on LPARs

One OS can run on one LPAR. This OS running on an LPAR is called a *guest OS*.

The independence of LPARs ensures that a guest OS running on an LPAR operates independently of the guest OSs running on other LPARs.

Features of processors logically partitioned by LPAR manager

LPAR manager allows you to flexibly allocate resources, such as by allocating processors in dedicated mode to LPARs that require high performance, and allocating processors in shared mode to LPARs so that many LPARs can efficiently use limited hardware resources. Dedicated mode and shared mode are generally called scheduling modes. You can dynamically switch the processor scheduling mode without deactivating the LPARs.

Note that LPAR manager provides the following functionality for using processors allocated in shared mode with high efficiency.

- Specifying the service ratio (the proportion of time an LPAR uses processors) for each LPAR
You can specify the ratio for which the time to use a processor is distributed to each of the LPARs to which processors are allocated in shared mode. This ratio is called the service ratio. If you want to create an LPAR that has higher performance than the other LPARs that share processors with that LPAR, specify a higher service ratio for the LPAR.
- Detecting a processor in the idle state and allocating it to another LPAR
LPAR manager can detect when a processor that is allocated to LPARs in shared mode is in the idle state (in other words, is not running). This functionality is called the idle-detection functionality. When a processor in the idle state is detected, that processor can be allocated to another LPAR that shares the processor.
- Maintaining the specified service ratio by using processor capping
By using processor capping with the idle-detection functionality, you can control which LPAR a processor is re-allocated to when the processor in the idle state is detected. For example, if three LPARs (LPAR 1 to LPAR 3) are running and you want to always re-allocate processors to LPAR 2 when the idle state of LPAR 1 is detected, apply processor capping to LPAR 3.
- Dividing shared processors into processor groups
Logically partitioned processors can be divided into groups. These groups are called processor groups. The load of the processors is shared by the LPARs to which the processors are allocated in shared mode. By using processor groups, you can limit the effect of the load of the processors to the corresponding processor group.
- Increasing the number of processors that can be logically partitioned by using hyper-threading
If you enable hyper-threading for a server blade by using UEFI, the unit for the processors that can be logically partitioned changes from the number of cores to the number of threads, and the number of processors that can be logically partitioned increases.

Features of memory that is logically partitioned by LPAR manager

Logically partitioned memory is always allocated to LPARs in dedicated mode. Logical firmware uses a part of the memory allocated to each LPAR.

- For memory for logical firmware and memory for a guest OS, specify the amount of memory in multiples of 256 MB.
- Each guest OS has dedicated use of the memory allocated to its LPAR.
- LPAR manager automatically determines which offset physical memory is allocated to an LPAR when the LPAR is activated.
- The amount of memory to be allocated to a guest OS is calculated by subtracting the amount of memory used by logical firmware from the amount of memory allocated to the LPAR.

- Depending on the specifications of the guest OS and the environment, the entire allocated memory cannot be used.
- To prevent performance degradation due to a memory swap, make sure that you allocate enough memory to LPARs, taking into account the amount of memory used by logical firmware.

The following figure shows the concept of logical partitioning of memory.

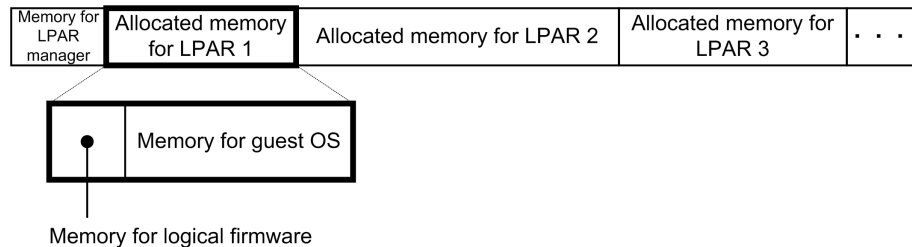


Figure 1-2 Logical partitioning of memory

Memory capacity used by logical firmware

You can estimate the amount of memory used by logical firmware by using the following calculation formulas:

- If the amount of memory allocated to the LPAR is less than 8 GB

$$0.6\% \text{-of-memory-allocated-to-LPAR} + \text{number-of-logical-processors} \times 2.25 \text{ MB} + 65 \text{ MB}$$
- If the amount of memory allocated to the LPAR is 8 GB or more

$$0.25\% \text{-of-memory-allocated-to-LPAR} + \text{number-of-logical-processors} \times 2.25 \text{ MB} + 80 \text{ MB}$$

Application to NUMA configurations

NUMA (Non-Uniform Memory Access) is an architecture where memory is shared in the multiprocessor computer system. To create an LPAR that meets all of the following conditions, we recommend that you use a NUMA configuration so you can easily improve memory access and memory bandwidth.

- If you want to create an LPAR on a server blade in an SMP configuration:
- If you want to create an LPAR with the scheduling mode set to dedicated mode:
 You can set the scheduling mode by using the Logical Partition Configuration screen.
- If you want to manually specify the number of the physical processor to be assigned to the LPAR and then fix the number:
 You can set the physical processor number by using the Logical Processor Configuration screen.

Related topics

- [Logical Partition Configuration screen on page 10-8](#)

- [Logical Processor Configuration screen on page 10-20](#)
- Manual *Hitachi Compute Blade 2500 Series UEFI Setup Guide*

Features of PCI devices that are logically partitioned by LPAR manager

For a PCI device that is logically partitioned by LPAR manager, you can specify scheduling mode so that the device is used by only one LPAR or you can specify a mode for sharing the device among multiple LPARs. The scheduling mode includes dedicated mode and shared mode.

If PCI devices are NICs, in addition to the "dedicated NICs" where physical NICs are dedicated to LPARs, the three types of logically partitioned NICs below are provided. You can configure these types for communication with external networks and communication between LPARs.

- Shared NIC
- VF NIC
- Virtual NIC

Shared NICs, VF NICs, and virtual NICs are generally called logical NICs.

If PCI devices are FCs, in addition to the "dedicated FCs" where physical FCs are dedicated to LPARs, "shared FCs" where FCs are logically partitioned are provided.

To use SAN boot on guest OSs, configure the network so that the LPARs can communicate with external storages via FC devices.

Dedicated NIC

LPAR manager supports dedicated NIC assignment. There are two types of dedicated NICs: Device dedicated NICs, where physical NICs are dedicated to LPARs, and port dedicated NICs, where ports of your choice are dedicated to LPARs.

Device dedicated NIC

Device dedicated NICs have the following features: If there are sufficient number of physical NICs for the number of LPARs, we recommend using device dedicated NICs.

- You can obtain stable performance that is not affected by other LPARs.
- You can perform data transfer at high speed.

Port dedicated NICs

Port dedicated NICs have the following features: If there are not sufficient number of physical NICs for the number of LPARs, we recommend using port dedicated NICs.

- You can obtain stable performance that is not affected by other LPARs.
- You can perform data transfer at high speed.
- Dedicated mode and shared mode can both be used in a port.
- There are limitations on supported physical NICs.

Shared NIC

In LPAR manager, a NIC can be shared among LPARs. When you use shared mode as the NIC scheduling mode, you can assign network segments to shared NICs. These NICs to which network segments are assigned are called shared NICs.

Shared NICs have the following features:

- One physical NIC can be shared by multiple LPARs.
- You can resolve shortages of physical resources in an virtual environment. You can use devices more efficiently by increasing the usage rate of each device.
- A shared NIC is recognized as a 1-GB NIC (Intel 82576 specification) on a guest OS, regardless of whether the physical NIC is a 10-GB NIC or 1-GB NIC. As a result, the total throughput of the shared NICs is approximately 3 Gbps per LPAR manager environment.
- Performance varies depending on the number of LPARs that share the physical NIC and the volume of traffic.
- In LPAR manager, you can assign a maximum of eight physical LAN controllers, and a maximum of 16 physical ports.
- You can assign shared NICs by using the Virtual NIC Assignment screen.

In the configurations below, network segments 1a and 1b serve as management paths.

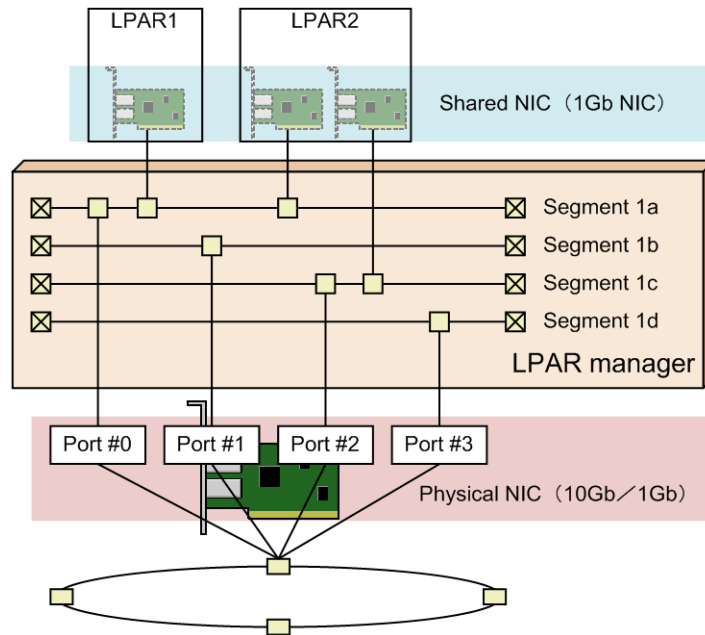


Figure 1-3 Configuration example of a network using shared NICs

VF NIC

When the SR-IOV functionality of physical NICs is enabled, if you set shared mode for the NICs, you can assign network segments for VF NICs. These NICs to which network segments are assigned are called VF NICs.

VF NICs have the following features:

- You can use SR-IOV, which is hardware functionality of a physical NIC.
- You can perform data transfer at high speed comparable to dedicated NICs.
- The load on a physical processor is low compared to a shared NIC and virtual NIC.
- You can set transmission band limitations in 100-Mpbs increments.
- There are limitations on supported physical NICs, server blades, and OSs.
- You can assign VF NICs by using the Virtual NIC Assignment screen.
- In LPAR manager, you can assign a maximum of 8 physical LAN controllers, and a maximum of 16 physical ports.

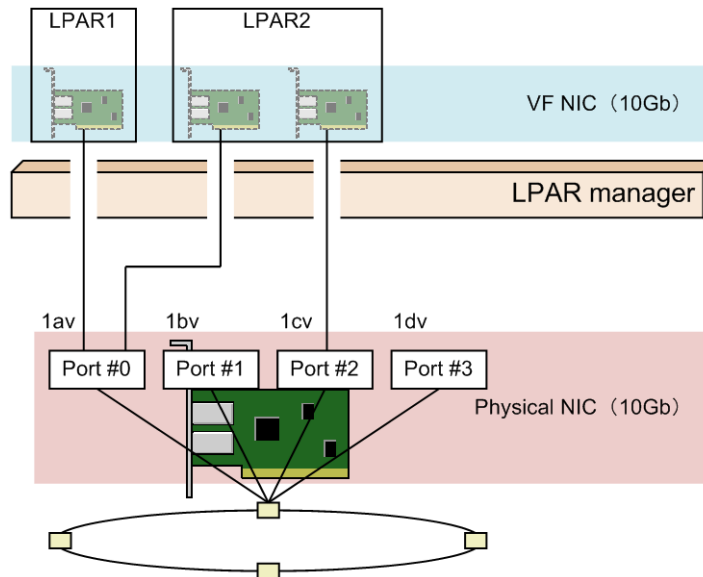


Figure 1-4 Configuration example of a network using VF NICs



Tip:

- Communication between VF NICs connected to the same network segment does not use an external network. In contrast, communication between VF NICs connected to different network segments takes place over an external network.

Virtual NIC

In LPAR manager, you can assign a maximum of four network segments to a virtual NIC. These NICs to which network segments are assigned are called virtual NICs.

Virtual NICs have the following features:

- Virtual NICs enables communication between LPARs without using a physical NIC
- The required specifications for using virtual NICs is the same as those for using 1Gb NICs (Intel 82576 specifications).
- You can assign network segments on the Virtual NIC Assignment screen. The available network segment identifiers are Va to Vd.
- The total throughput of the virtual NICs is approximately 3 Gbps per LPAR manager instance.

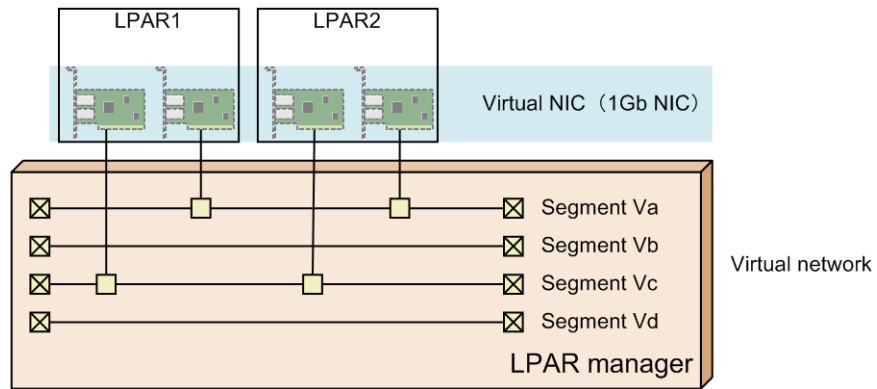


Figure 1-5 Configuration example of a network using virtual NICs



Tip:

- Virtual NICs that are connected to the same network segment can communicate with each other. However, a virtual NIC cannot communicate with a virtual NIC that is connected to a different network segment.

Dedicated FC

The features of dedicated FCs for LPAR manager are as follows:

- One fibre channel adapter is dedicated to one LPAR, and the LPAR has exclusive use of that fibre channel adapter.
- Multiple LPARs cannot use the same fibre channel adapter at the same time.
- A dedicated FC uses the same WWN as vfcID=1.
- Port vfcID=1 of the shared FC takes the same EFI driver settings as port vfcID=1 of the dedicated FC. However, with the exception of "Connection Type" and "Data Rate", vfcID=2 onward do not take the same settings.

Shared FC

The features of shared FCs for LPAR manager are as follows:

- One fibre channel adapter is shared by multiple LPARs, and the LPARs to which the adapter is assigned are able to use it concurrently.
- A shared FC can be assigned in the following ways. You can configure a shared FC on the Shared FC Assignment screen.
 - When a fibre channel adapter incorporates two or more ports, you can assign LPARs to ports on a one-to-one basis.
 - You can assign a fibre channel adapter port to multiple LPARs.
- For shared FCs, you can set HBA-core dedicated mode.
 - With HBA-core dedicated mode, an HBA core that sends and receives data is dedicated to a single LPAR.

- This mode allows you to obtain stable performance that is not affected by other LPARs.

Related topics

- [Maintaining the I/O performance by using the HBA dedicated core mode of shared FCs on page 6-20](#)

Management path and operation path

A network path configured to manage LPAR manager and LPARs is called a management path. A network path configured to process server operations is called an operation path.

- To start LPAR manager, a management path that enables communication between LPAR manager and management modules is required.
- For the NIC to be used by the management path, be sure to set the scheduling mode to the shared mode.

IPv4 addresses and IPv6 addresses can be used as management paths. As such, network operation by using IPv6 addresses is supported between LPAR managers and system consoles.

To communicate with the management module, LPAR manager directly uses physical NICs during startup. After startup, LPAR manager uses shared NICs in the network segments to which the physical NICs belong to communicate with it. The NIC used for the communication with the management module is called the management NIC. The IP address assigned to the management NIC is called the LP IP address.

Network devices supported by LPAR manager

Network devices used by LPAR manager for management communications support the following hardware.

- Onboard LAN
- Broadcom 1Gb 4-port LAN mezzanine card
- 1000BASE-T 4-port LAN adapter
- 10GBASE-SR 2-port LAN adapter
- Emulex 10Gb 2-port converged network adapter

Connection to the management LAN

Depending on the network device used by LPAR manager for management communications, arrange network cabling between the management LAN and the management LAN module as follows: When using LPAR manager, you cannot directly connect the system console to the management LAN module.

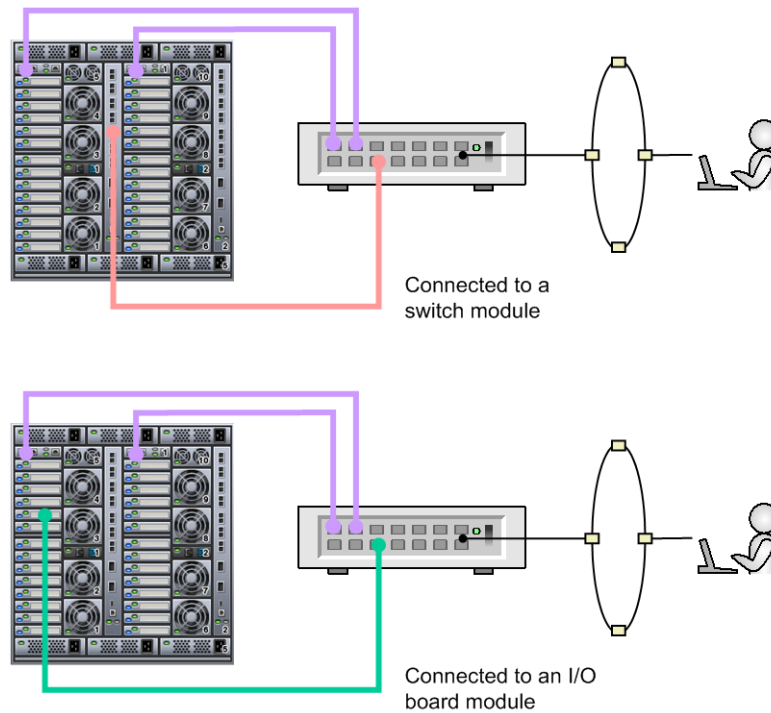


Figure 1-6 Connection to the management LAN

Related topics

- [NIC to be used for management path communication on page 1-13](#)
- [When omit configure the NIC for management path communication on page 1-14](#)
- [Notes on communication on the management path on page 1-17](#)
- [System Configuration screen on page 10-47](#)

NIC to be used for management path communication

You can select a maximum of two ports from among the ports of the NICs that are installed in a server blade. On the same NIC, you can specify the ports to be used for communications for each management path. However, by specifying ports on different NICs, you can configure port redundancies and enhance fault tolerance. Note that the primary management path does not become active instead of the secondary management path even if the primary management path recovers when the secondary management path works. A redundant configuration is maintained after recovery of the primary management path.

If you do not specify a NIC to be used for management path communication, LPAR manager determines the NIC. See the Related topics.



Note:

To specify a NIC to be used for management path communication, the requirements for the versions of LPAR manager firmware, management module firmware and server blade firmware must be met. If the requirements

for their firmware versions are not met due to one of the following events, LPAR manager cannot start.

- LPAR manager firmware, management module firmware and server blade firmware was downgraded by mistake.
- N+M cold standby switched to a standby system that does not meet the requirements for the firmware versions.

Keep the versions of LPAR manager firmware, management module firmware and server blade firmware up-to-date on both the active and backup systems. For details on the firmware versions required for specifying NICs to be used for management path communication, see the related topics.

Related topics

- [Setting the ports to be used for management path communication on page 8-3](#)

When omit configure the NIC for management path communication

If you omit the configuration of NIC and port to use for management path communication, NIC is determined by the LPAR manager. The following is a feature of the NIC that has been determined by the LPAR manager.

- The physical NIC to be used for communication on the management path is determined by LPAR manager and cannot be changed.
- LPAR manager sets the physical NIC used by the management path to shared mode and reserves the NIC for communication by the management module. You cannot set the NIC to dedicated mode.
- Ports 0 and 1 (virtual network segments 1a and 1b) of the first NIC that is authenticated by LPAR manager are communication ports used for the management path.

In this case, LPAR manager will select the first NIC that was identified by LPAR manager (the NIC that has the lowest number from among the NICs displayed on the PCI Device Information screen). The following is identification order.

Note that, if the LPAR manager firmware version is 02-2x or earlier, when installing a 10GBASE-SR 2-port LAN adapter, locate the 10GBASE-SR 2-port LAN adapter in a slot so that the LPAR manager recognizes the network device on which ports are set as the management paths by default, as a lower number of network device in identification order.



Note:

- We strongly recommend that you explicitly specify the NIC to be used for management path communication.
 - If you do not explicitly specify a NIC to be used for management path communication, the scheduling mode of the NIC to be selected as a management path needs to be able to be set to the shared mode. If the NIC cannot be set to the shared mode, LPAR manager cannot start.
-

Identification order of network devices in CB 520X

CB 520X identifies network devices in the order below. In an SMP configuration for CB 520X, hardware resources are identified in the order of the server chassis slot numbers.

The I/O board module slot numbers listed below are for the server blade installed in slot 1.

The slot numbers differ depending on the slot in which the server blade is installed.

- CB 520X B1 with a mezzanine card

1. Mezzanine card slot 1
2. I/O board module slot 01A
3. I/O board module slot 01B
4. Mezzanine card slot 3
5. I/O board module slot 02A
6. I/O board module slot 02B

- CB 520X B1 with an onboard LAN

1. I/O board module slot 01A
2. I/O board module slot 01B
3. Onboard LAN
4. I/O board module slot 02A
5. I/O board module slot 02B

- CB 520X B2 with a mezzanine card

1. Mezzanine card slot 1
2. I/O board module slot 01A
3. I/O board module slot 01B
4. Mezzanine card slot 3
5. I/O board module slot 02A
6. I/O board module slot 02B

- CB 520X B2 with an onboard LAN

1. Onboard LAN
2. I/O board module slot 01A
3. I/O board module slot 01B
4. I/O board module slot 02A
5. I/O board module slot 02B

- CB 520X B3 with a mezzanine card

1. Mezzanine card slot 1
2. I/O board module slot 01A

3. I/O board module slot 01B
 4. Mezzanine card slot 3
 5. I/O board module slot 02A
 6. I/O board module slot 02B
- CB 520X B3 with an onboard LAN
1. Onboard LAN
 2. I/O board module slot 01A
 3. I/O board module slot 01B
 4. I/O board module slot 02A
 5. I/O board module slot 02B

Identification order of network devices in CB 520H

CB 520H identifies network devices in the order below.

The I/O board module slot numbers listed below are for the server blade installed in slot 1.

The slot numbers differ depending on the slot in which the server blade is installed.

- CB 520H B3/B4
1. Mezzanine card slot 1 or onboard LAN
 2. I/O board module slot 01A
 3. I/O board module slot 01B

Related topics

- [PCI Device Information screen on page 10-26](#)

Influence when management path communication is not available

The following table describes the influence when the management module and LPAR manager cannot communicate with each other.

Table 1-2 Influence when the management module and LPAR manager cannot communicate with each other

Item		Impact	Recovery
LPAR manager screen		N	--
Web console		Y	1
HCSM	LPAR manager operation	Y	1
	Alert notification	Y	1
HVM Navigator		Y	1

Item		Impact	Recovery
Virtual COM console		Y	1
LP Web system	Logical VGA snapshot	Y	1
HvmSh execution		Y	1
LPAR manager configuration information and LPAR configuration information	Auto	Y	1
	Manual	Y	1
Times handled by LPAR manager		Y	1
NTP server time synchronization	Management module synchronization	Y	1
LPAR manager dump collection	Auto	Y	1
	Manual	Y	1
N+M cold standby		Y	2
HA monitor	Health check	Y2	3
	Failover from active to standby	Y2	4
<p>Legend:</p> <p>N: Guest OSs and the operation of LPAR manager are not affected.</p> <p>Y: Guest OSs are not affected but the operations and functions of LPAR manager are affected.</p> <p>Y2: Guest OSs and LPAR manager are affected. Guest OS operations are required even after the recovery of the management path.</p> <p>1: The operation fails but the function can be used after the recovery of the management path. The function is automatically resumed after the recovery of the management path.</p> <p>2: For standby blades in an N+M cold standby configuration, an LPAR is automatically activated in the last saved state in the LPAR manager configuration information.</p> <p>3: HA monitor on the guest OS detects that the reset path is in the error state. The <code>monrp</code> command is required after the recovery of the management path.</p> <p>4: When system failover occurs on the guest OS by the HA monitor, system reset fails. At that time, if the reset function on physical partition is effective, forcibly reset of the server blade is performed (LPAR manager and all LPARs are down).</p> <p>--: Not applicable</p>			

Notes on communication on the management path

For details about network cabling of the management path, see the descriptions in the manual *Hitachi Compute Blade 2500 Series Getting Started Guide*. This subsection describes notes on network cabling.

- Route cables so that all communications between the management module and LPAR manager are passed over an external network of the system unit.

Configure settings so that LPAR manager and the management module can communicate with each other, because LPAR manager accesses the management module when LPAR manager starts.

- Do not perform the following operations when the management module and LPAR manager cannot communicate with each other:
 - Performing the Force Recovery operation
 - Changing the scheduling mode of a PCI device
 - Changing VNIC system numbers
 - Changing an LP ID
 - Changing the port number of a virtual COM console port
 - Setting FC driver options by HvmSh

If you perform one of the above operations when the management module and LPAR manager cannot communicate with each other, the operation fails and an LPAR manager Assist failure occurs. If an LPAR manager Assist failure occurs, make sure that the management module and LPAR manager can communicate with each other, and then perform the operation again.

You can use the following logs to check whether the management module and LPAR manager can communicate with each other.

- LP system logs
 - If "LPAR manager detected error of network communication for SVP access" is output to the log, the management module and LPAR manager cannot communicate with each other.
 - However, if "LPAR manager detected recovery of network communication at SVP access" is output to the log after the above message, communication has already been recovered.
- System event log (SEL)
 - If "LPAR manager detected error of network communication for SVP access" is output to the log, the management module and LPAR manager cannot communicate with each other.
 - However, if a log entry about the recovery of communication between LPAR manager and a management module is output to the log, communication has already been recovered.
- System Service State screen, which is one of the LPAR manager screens
 - If `Connect:Fail` is displayed for SVP Network Path State, the management module and LPAR manager cannot communicate with each other.
 - If `Connect:Success` is displayed, communication is possible.
 - If there is no management path for which `Active` is displayed for `State` for SVP Network Path State, the management module and LPAR manager cannot communicate with each other.
- If the performance of the management path is reduced, check the processor usage for network communication in SYS2 of the LPAR Usage screen.

If the value of Dsp (ms) of SYS2 is 1800 ms or higher, the problem is most likely caused by the overloading of the shared NIC. To reduce the load, review the network configuration of the shared NIC or remove the cause of the heavy load on the shared NIC.

Related topics

- [System Configuration screen on page 10-47](#)
- [System Service State screen on page 10-58](#)
- [LPAR Usage screen on page 10-81](#)

CB 520X NIC configuration and assignment example

The following table shows how the ports and controllers of physical NICs installed in CB 520X are assigned to the network segments of LPAR manager.

Table 1-3 CB 520X B1/B2/B3 configuration example 1

Hardware	Physical port number ¹	Logical port number ²	Controller assignment sequence	Network segment
Mezzanine card 1 (Broadcom 1Gb 4-port LAN mezzanine card)	0	0	1	1a
	1	1		1b
	2	2		1c
	3	3		1d
I/O board module slot 01A (Emulex 10Gb 2-port converged network adapter)	0	0	2	2a
	1	1		2b
I/O board module slot 01B (Emulex 10Gb 2-port converged network adapter)	0	0	3	3a
	1	1		3b
Onboard LAN	Not used (disabled)			
Mezzanine card 3	Not installed			
I/O board module slot 02A (Hitachi 8Gb 2-port fibre channel adapter)	0	0	None ³	None ³
	1	1		
I/O board module slot 02B (Hitachi 8Gb 2-port fibre channel adapter)	0	0		
	1	1		
Notes:				

Hardware	Physical port number ¹	Logical port number ²	Controller assignment sequence	Network segment
<ol style="list-style-type: none"> Physical port numbers that actually exist in the system. Logical port numbers displayed on the LPAR manager screen. Controller numbers are not assigned to fibre channel adapters. In addition, fibre channel adapters are not recognized as NICs, and therefore they do not have dependent network segments. 				

Table 1-4 CB 520X B1/B2/B3 configuration example 2

Hardware	Physical port number ¹	Logical port number ²	Controller assignment sequence	Network segment
Mezzanine card 1	Not installed			
I/O board module slot 01A (Hitachi 8Gb 2-port fibre channel adapter)	0	0	None ³	None ³
	1	1		
I/O board module slot 01B (Hitachi 8Gb 2-port fibre channel adapter)	0	0		
	1	1		
Onboard LAN	0	0	1	1a
	1	1		1b
	2	2		1c
	3	3		1d
Mezzanine card 3	Not installed			
I/O board module slot 02A (Emulex 10Gb 2-port converged network adapter)	0	0	2	2a
	1	1		2b
I/O board module slot 02B (Emulex 10Gb 2-port converged network adapter)	0	0	3	3a
	1	1		3b
Notes:				
1. Physical port numbers that actually exist in the system.				
2. Logical port numbers displayed on the LPAR manager screen.				
3. Controller numbers are not assigned to fibre channel adapters. In addition, fibre channel adapters are not recognized as NICs, and therefore they do not have dependent network segments.				

Table 1-5 CB 520X B1/B2/B3 configuration example 3

Hardware	Physical port number ¹	Logical port number ²	Controller assignment sequence	Network segment
Mezzanine card 1	Not installed			
I/O board module slot 01A (Emulex 10Gb 2-port converged network adapter)	0	0	1	1a
	1	1		1b
I/O board module slot 01B (Emulex 10Gb 2-port converged network adapter)	0	0	2	2a
	1	1		2b
Onboard LAN	0	0	3	3a
	1	1		3b
	2	2		3c
	3	3		3d
Mezzanine card 3	Not installed			
I/O board module slot 02A (Hitachi 8Gb 2-port fibre channel adapter)	0	0	None ³	None ³
	1	1		
I/O board module slot 02B (Hitachi 8Gb 2-port fibre channel adapter)	0	0		
	1	1		
Notes:				
1. Physical port numbers that actually exist in the system.				
2. Logical port numbers displayed on the LPAR manager screen.				
3. Controller numbers are not assigned to fibre channel adapters. In addition, fibre channel adapters are not recognized as NICs, and therefore they do not have dependent network segments.				

CB 520H NIC configuration and assignment example

The following table shows how the ports and controllers of network devices installed in CB 520H are assigned to the network segments of LPAR manager.

Table 1-6 CB 520H B3/B4 configuration example

Hardware	Physical port number ¹	Logical port number ²	Controller assignment sequence	Network segment
Mezzanine card 1 (Broadcom 1Gb 4-port LAN mezzanine card) or onboard LAN	0	0	1	1a
	1	1		1b
	2	2		1c
	3	3		1d
I/O board module slot 01A (Emulex 10Gb 2-port converged network adapter)	0	0	2	2a
	1	1		2b
I/O board module slot 01B (Hitachi 8Gb 2-port fibre channel adapter)	0	0	None ³	None ³
	1	1		
Notes:				
1. Physical port numbers that actually exist in the system.				
2. Logical port numbers displayed on the LPAR manager screen.				
3. Controller numbers are not assigned to fibre channel adapters. In addition, fibre channel adapters are not recognized as NICs, and therefore they do not have dependent network segments.				

Configuration example of a network path on which VLANs are used

To use VLANs on a network path for an LPAR manager environment, make sure the path is an operation path. This subsection provides an example of a network path on which VLANs are used.



Note:

- The management NIC cannot send or receive VLAN tagged frames. Configure the LAN switches so that the management NIC can send and receive untagged frames.

Using different NICs for the management and operation paths

In the following figure, the ports a and b on the physical NIC 1 are used for management paths, and the ports a and b on the physical NIC 2 are used for operation paths. A square indicates a port on a shared NIC, a physical NIC, or a LAN switch. Amber ports connect to the management LAN, and light blue ports connect to the operation LAN. Squares inside LPAR manager indicate ports on the management NIC. LPAR manager uses physical NIC ports (1a) and (1b) without VLAN.

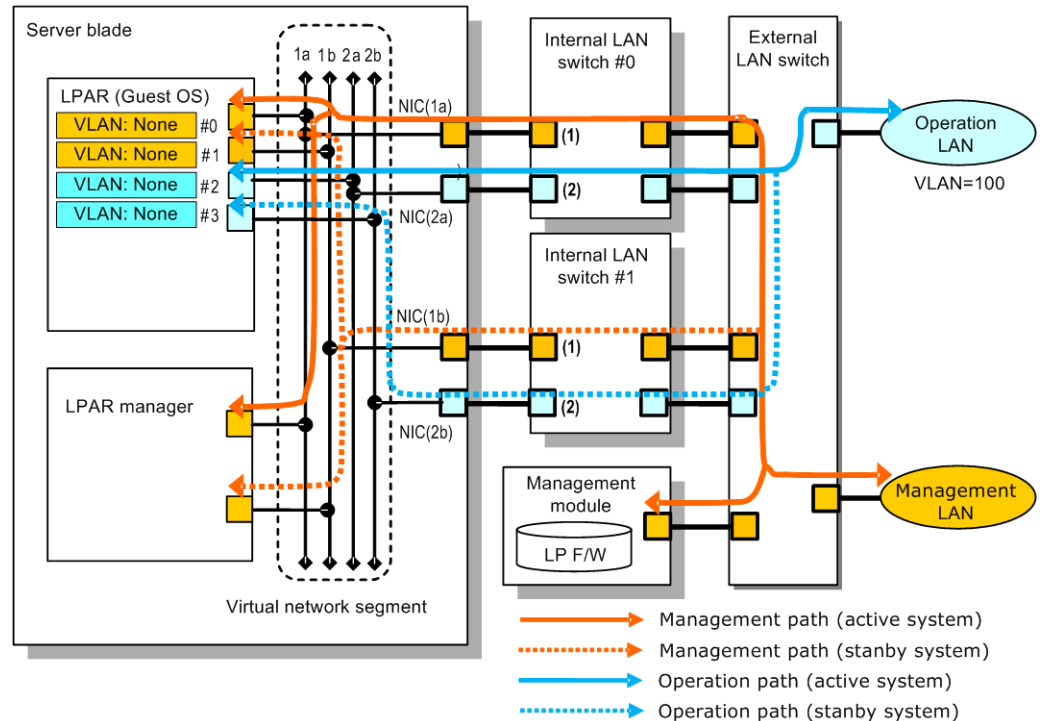


Figure 1-7 Configuration example where different NICs are used for the management and operation paths

Table 1-7 VLAN settings for management path and operation path (1)

LPAR (guest OS)	Shared NIC	Internal LAN switch (The same settings are applied to #0 and #1)	
VLAN: None (management path)	Undef (VLAN: None)	(1)	VLAN: None
VLAN: None (operation path)		(2)	Access port settings VLAN ID: 100

Using the same NIC for the management and operation paths

The following shows a configuration example where the same NIC is used for communication on the management and operation paths.

In the following figure, a square indicates a port on a shared NIC, a physical NIC, or a LAN switch. Amber ports connect to the management LAN, and light blue ports connect to the operation LAN. Green ports connect to both the management and operation LANs but are functionally divided by using different VLAN settings (1) and (2). Squares inside LPAR manager indicate ports on the management NIC. LPAR manager uses physical NIC ports (1a) and (1b) without VLAN.

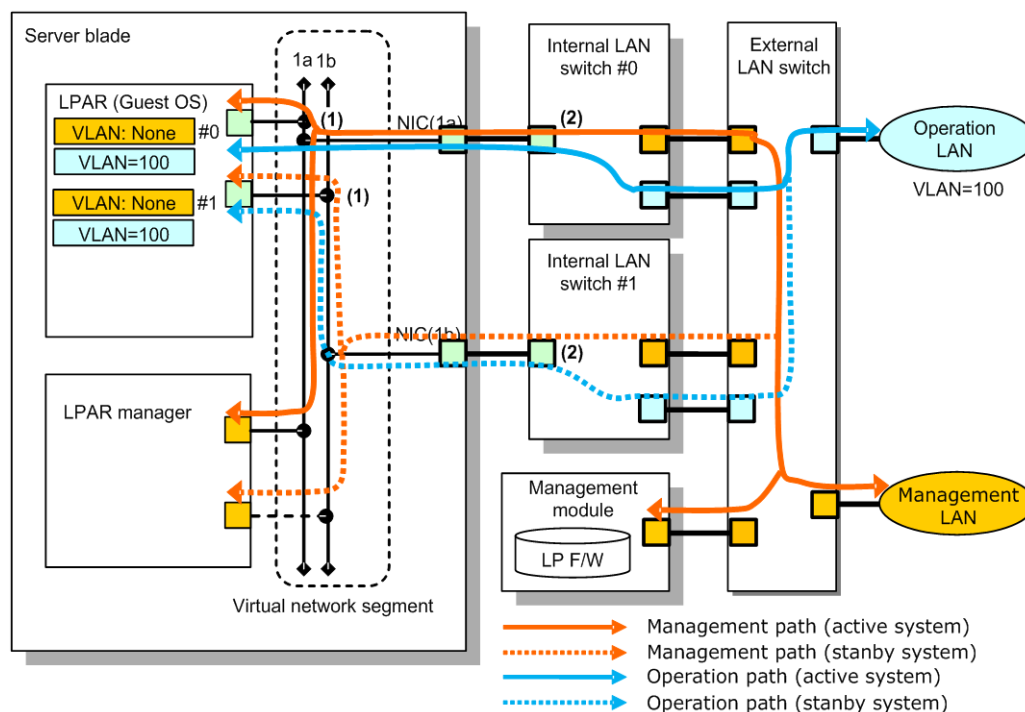


Figure 1-8 Configuration example where the same NIC is used for the management and operation paths

Table 1-8 VLAN settings for management path and operation path (2)

LPAR (guest OS)	Shared NIC		Internal LAN switch (The same settings are applied to #0 and #1)	
VLAN: None (management path) VLAN ID: 100 (operation path)	(1)	Tagged VLAN ID: 100	(2)	Trunk port settings VLAN IDs: 1, 100 Native VLAN ID: 1 (default)

LPAR manager system requirements

This section describes the support requirements for systems running LPAR manager and LPARs.

Server blades supported by LPAR manager

The following table shows the server blades supported by LPAR manager

Table 1-9 Server blades supported by LPAR manager

Server blade ^{1, 2}	Support specification	Supported version
CB 520X B1	Y	02-00 or later

Server blade ^{1, 2}	Support specification	Supported version												
CB 520X B2	Y	02-27 or later												
CB 520X B3	Y	02-46 or later												
CB 520H B3	Y	02-05 or later												
CB 520H B4	Y	02-50 or later												
PCI expansion blade ³	Y	02-55 or later												
Notes: 1. Internal disks (HDD and SSD) of server blades cannot be used. 2. Enable hyper-threading if you are using a server blade with a quad-core CPU. 3. Note the following when using a PCI expansion blade. <ul style="list-style-type: none"> The target blade is as follows: <ul style="list-style-type: none"> CB 520H B4 The following versions of firmware are supported: 														
Table 1-10 Firmware versions <table> <tr> <th colspan="2">Firmware</th><th>Version</th></tr> <tr> <td colspan="2">Management module firmware</td><td>A0165 or later</td></tr> <tr> <td>Server blade firmware</td><td>CB 520H B4</td><td>10-06 or later</td></tr> <tr> <td colspan="2">LPAR manager firmware</td><td>02-55 or later</td></tr> </table>			Firmware		Version	Management module firmware		A0165 or later	Server blade firmware	CB 520H B4	10-06 or later	LPAR manager firmware		02-55 or later
Firmware		Version												
Management module firmware		A0165 or later												
Server blade firmware	CB 520H B4	10-06 or later												
LPAR manager firmware		02-55 or later												
<ul style="list-style-type: none"> Mezzanine card slots for PCI expansion blades are not supported. 														

Guest OSs supported by LPAR manager

This section describes OSs supported as guest OSs on LPARs, and LPAR manager firmware versions.



Note:

- Secure Boot of a guest OS on an LPAR is not supported.

Supported Windows Server and LPAR manager firmware

Table 1-11 Guest OSs supported by the LPAR manager (Windows Server)

Server blade	LPAR manager firmware version			
	Windows Server 2008 R2	Windows Server 2008 R2 SP1	Windows Server 2012, 2012 R2	Windows Server 2016
CB 520X B1	Not supported	02-00 or later	02-00 or later	Not supported
CB 520X B2	Not supported	Not supported	02-27 or later	02-56 or later
CB 520X B3	Not supported	Not supported	02-55 or later	02-56 or later

Server blade	LPAR manager firmware version			
	Windows Server 2008 R2	Windows Server 2008 R2 SP1	Windows Server 2012, 2012 R2	Windows Server 2016
CB 520H B3	Not supported	Not supported	02-05 or later	02-56 or later
CB 520H B4	Not supported	Not supported	02-50 or later	02-56 or later

Supported Red Hat Enterprise Linux and LPAR manager firmware

Red Hat Enterprise Linux versions supported as guest OSs on LPARs are only 64-bit versions. 32-bit versions are not supported.

Table 1-12 Guest OSs supported by the LPAR manager (Red Hat Enterprise Linux 6)

Server blade	LPAR manager firmware version					
	RHEL 6.5	RHEL 6.6	RHEL 6.7	RHEL 6.8	RHEL 6.9 ¹	RHEL 6.10 ¹
CB 520X B1	02-00 or later	02-06 or later	02-45 or later	02-55 or later	02-59 or later	02-66 or later
CB 520X B2	Not supported	02-27 or later	02-45 or later	02-55 or later	02-59 or later	02-66 or later
CB 520X B3	Not supported	Not supported	Not supported	02-55 or later	02-59 or later	02-66 or later
CB 520H B3	02-05 or later	02-06 or later	02-45 or later	02-55 or later	02-59 or later	02-66 or later
CB 520H B4	Not supported	Not supported	Not supported	02-55 or later	02-59 or later	02-66 or later
Notes:						
1. There are some restrictions on supported functionality. For detailed restrictions, see Differences in supported items depending on the guest OSs on page B-22 .						

Table 1-13 Guest OSs supported by the LPAR manager (Red Hat Enterprise Linux 7)

Server blade	LPAR manager firmware version						
	RHEL 7.1	RHEL 7.2	RHEL 7.3 ¹	RHEL 7.4 ¹	RHEL 7.5 ¹	RHEL 7.6 ^{1, 2}	RHEL 7.7 ¹
CB 520X B1	02-40 or later	02-45 or later	02-59 or later	02-62 or later	Not supported	Not supported	Not supported
CB 520X B2	02-40 or later	02-45 or later	02-58 or later	02-62 or later	02-64 or later	02-67 or later	02-69 or later
CB 520X B3	Not supported	02-46 or later	02-58 or later	02-62 or later	02-64 or later	02-67 or later	02-69 or later
CB 520H B3	02-40 or later	02-45 or later	02-58 or later	02-62 or later	02-64 or later	02-67 or later	02-69 or later

Server blade	LPAR manager firmware version						
	RHEL 7.1	RHEL 7.2	RHEL 7.3 ¹	RHEL 7.4 ¹	RHEL 7.5 ¹	RHEL 7.6 ^{1, 2}	RHEL 7.7 ¹
CB 520H B4	Not supported	02-50 or later	02-58 or later	02-62 or later	02-64 or later	02-67 or later	02-69 or later
Notes: 1. There are some restrictions on supported functionality. For detailed restrictions, see Differences in supported items depending on the guest OSs on page B-22 . 2. When setting up the RHEL 7.6 environment, upgrade kernel from any older version of RHEL 7.x to RHEL 7.6 (3.10.0-957.12.2 or later). There is a known issue that a kernel panic occurs when RHEL 7.6 install media is booted. For more details, please refer to chapter of the <i>Restrictions when using RHEL 7 in an LPAR manager environment</i> in the manual <i>Hitachi Compute Blade Series OS Installation Guide for Red Hat Enterprise Linux</i> .							

Memory for LPAR manager

LPAR manager running on a server blade uses the physical memory of that server blade.

Of the memory to be used by LPAR manager and LPARs, memory for operating LPAR manager is required.

Table 1-14 Memory necessary for operating LPAR manager

Server blade type	Amount of memory necessary for operating LPAR manager
CB 520X B1/B2	3,072 MB
CB 520X B3	6,144 MB
CB 520H B3	2,560 MB
CB 520H B4	4,096 MB (when MM Config Base is set to 2GB ¹)
	6,144 MB (when MM Config Base is set to 3GB ¹)
Notes: 1. For the value of MM Config Base, see Table 2-1 Server Blade and EFI settings on page 2-2 .	

In addition, memory to be allocated to LPARs is required.

Related topics

- [Features of memory that is logically partitioned by LPAR manager on page 1-5](#)

General procedure from installing LPAR manager to operating LPARs

The following figure shows the general procedure for creating LPARs by using the Web console.

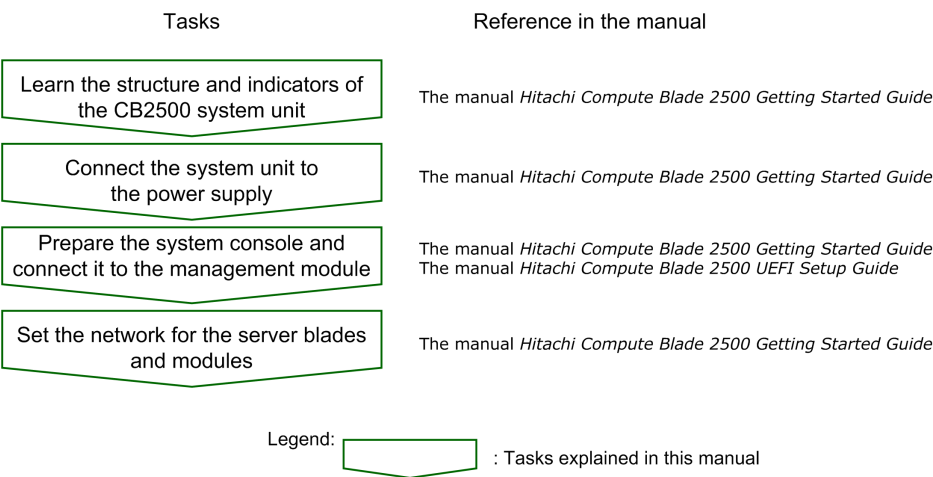


Figure 1-9 General procedure for the initial settings

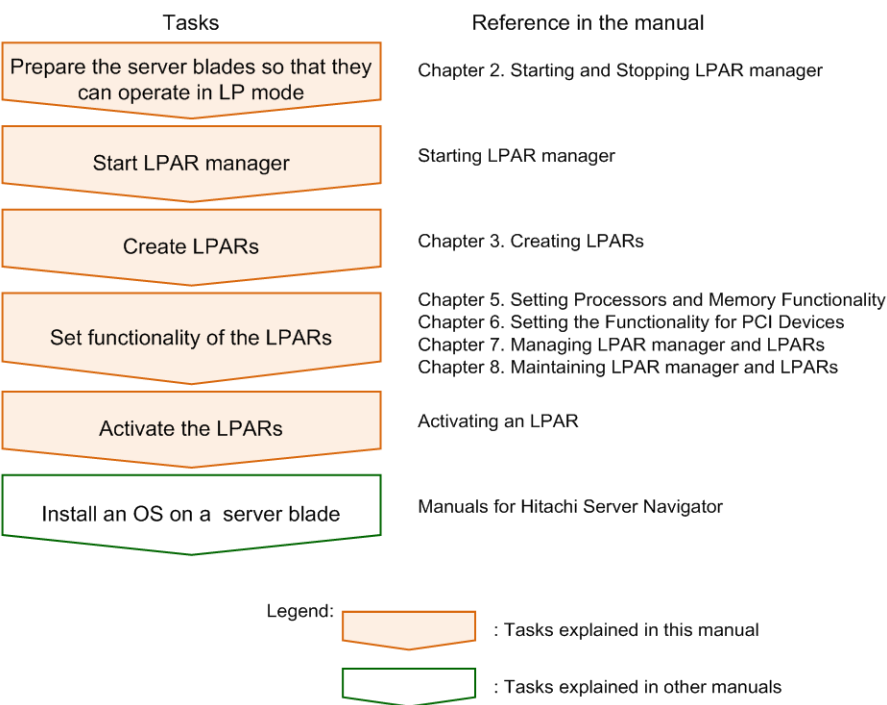


Figure 1-10 General procedure from powering on a server blade to setting up the OS

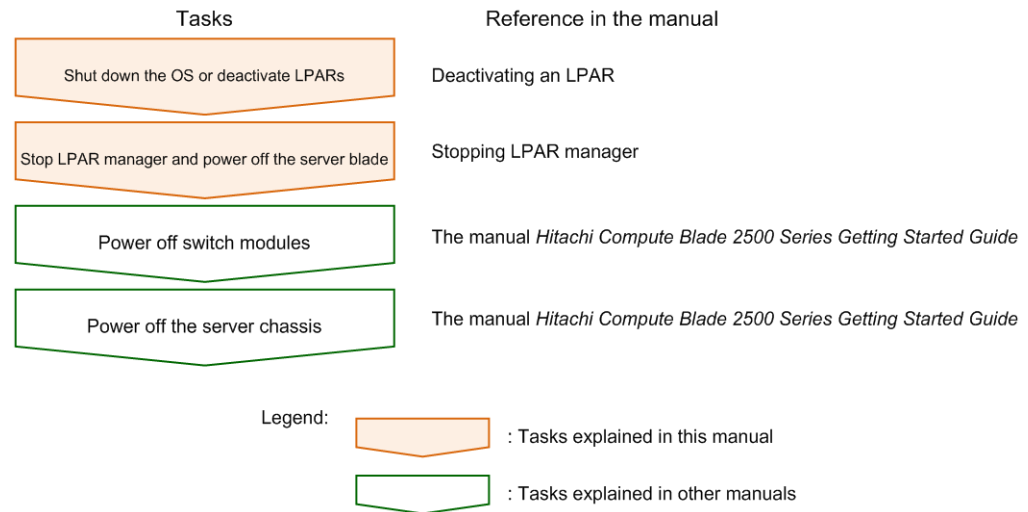


Figure 1-11 General procedure for stopping the system unit

Notes on configuring and operating logical environments

Be sure to read the notes provided in this section before configuring logical environments by using LPAR manager.

Notes when hardware resources are blocked or enter reduced-operation mode

- System event log (SEL) collection for a system unit or alert notice for SC/BSM is performed when isolation/degradation occurs in a CPU, a memory, or a PCI device.
- Some devices cannot be recognized at the next LPAR manager startup time, and some LP configuration information are deleted or reconfigured when isolation/degradation occurs in a CPU, a memory, or a PCI device. Note that, by using the KeepConfig option, the LPAR manager holds the LPAR manager configuration in the management module. For details, see [Backing up the LPAR manager configuration as of a time before device isolation on page 8-16](#).
- To block the device or put the device into reduced-operation mode for hardware replacement or other reasons, first back up the LPAR manager configuration information before stopping LPAR manager. To restore the device from a blocked state or from reduced-operation mode, restore the LPAR manager configuration information that you backed up before restarting LPAR manager. If no backup is available, check whether the LPAR configuration has changed after you start LPAR manager, and change the settings as needed.
- When you migrate an LPAR with one or more FC ports isolated on the source server blade to the destination server blade with FC ports with no errors in Concurrent Maintenance mode, the FC ports may be isolated even on the destination server blade.

For removing an FC port isolated, see the manual *Hitachi Compute Blade LPAR Migration Guide*.

Notes on logical NICs

This subsection provides notes on logical NICs that you need to know before configuring LPAR manager and LPARs.

Restrictions on use of Onboard LAN

Note the following restrictions when you use Onboard LAN on CB 520X B1/B2/B3 server blades.

- Disable a port on an OS when you do not desire to allow the OS to use the port.
 - Windows: Right-click on the target of the ports listed in Network adapters in the Device Manager window, and then select disabled.
 - Red Hat Enterprise Linux: Execute the "ifdown eth* (* shows a port number)" command to the target port.
- The Onboard LAN does not support the auto failback function for NIC teaming configurations with only Onboard LAN ports.

Limitations on using Emulex 10Gb NICs

When the following Emulex 10Gb NICs are used, there are limitations on the supported LPAR manager firmware versions depending on the firmware versions of these NICs:

- Onboard LAN
- Emulex 10Gb 2-port converged network adapter

Table 1-15 Emulex 10Gb NIC firmware (Emulex 10Gb 2-port converged network adapter) versions and supported LPAR manager firmware versions

NIC firmware version	LPAR manager firmware version	
	02-01 and later	02-45 and later
10.2.340.10 and later	Supported	Supported
10.6.144.2702 and later	Not supported	Supported
11.1.215.0 and later	Not supported	Not supported

Table 1-16 Emulex 10Gb NIC firmware (Onboard LAN) versions and supported LPAR manager firmware versions

NIC firmware version	LPAR manager firmware version	
	02-01 and later	02-45 and later
10.2.370.16 and later	Supported	Supported
10.6.144.2704 and later	Not supported	Supported

Logical NIC information output by using the ethtool command

When you use the Linux `ethtool` command to display information about a logical NIC, the following information appears for both onboard and mezzanine cards:

Table 1-17 Logical NIC information output by using the ethtool command

Item	Displayed information
Supported ports	FIBRE
Supported link modes	1000baseT/Full

Notes on using shared NICs

- LPAR manager uses the shared NIC functionality to emulate LAN controllers. An emulated LAN controller has poorer communication performance than a physical LAN controller, and its performance is influenced by environmental factors such as processor usage. Also, in communication with external networks, the difference in communication performance between the emulated and physical LAN controllers becomes more pronounced and performance fluctuations more extreme as the number of emulated LAN controllers sharing the physical LAN controller increases.
To mitigate this issue, we recommend that you balance the use of emulated LAN controllers and physical LAN controllers as the situation demands, taking into account factors such as the network environment and available bandwidth.
In an environment that has a large number of physical LAN controllers or uses high-speed 10 Gbps physical LAN controllers, a shared LAN might not make sufficient use of the available bandwidth.
- You cannot add or delete a shared NIC if any LPAR is activated. When changing the configuration of a shared NIC, deactivate all LPARs. Make sure that you configure a shared NIC before activating the LPARs.
- When a failure such as a link down occurs on a physical NIC, the shared NICs that share the physical LAN controller where the failure occurred can no longer communicate with the external network or with other LPARs. When a hardware failure occurs from which the system can automatically recover, communication might be temporarily interrupted while recovery

is being performed. In this case, shared NICs will be unable to communicate for approximately 60 seconds. This might cause some applications to detect a communication abnormality and terminate abnormally.

To prepare for a communication failure like this, make sure that you make the system redundant.

- When LPAR manager starts, undergoes forced recovery, or unexpectedly restarts, external devices might detect a temporary link-down status of the shared NIC.

Restrictions on the number of NICs that can be installed in a 4-blade SMP configuration

In a 4-blade SMP configuration, there are restrictions on installing Intel 1Gb NICs depending on the number of CPU cores.

Table 1-18 Restrictions on installing NICs in a 4-blade SMP configuration

Number of CPU cores	Hyper-threading	Number of Intel 1Gb NICs that can be installed
10 cores	Enabled	8 or less
	Disabled	5 or less
15 cores	Enabled	Unlimited
	Disabled	7 or less

Restrictions on the number of assigned NICs in Windows

If guest OS is Windows, there are restrictions on the number of ports that you can assign to a single LPAR. If you assign NICs in a way that exceeds this limit, the following issues might occur:

- OS installation fails or takes a very long time.
- A temporary link-down event occurs while the OS is running.

Table 1-19 NIC assignment in Windows (Windows Server 2008 R2, Windows Server 2012, 2012 R2)

Item	Windows Server 2008 R2	Windows Server 2012, Windows Server 2012 R2
A maximum of eight ports can be assigned for each core.	Y	Y
Each port of a dedicated NIC (an onboard LAN or Emulex 10Gb 2-port converged network adapter) uses the equivalent resources of four ports. Make sure that you	Y	--

Item	Windows Server 2008 R2	Windows Server 2012, Windows Server 2012 R2
account for this use of resources when assigning a dedicated NIC.		
Each port of a dedicated NIC (an onboard LAN or Emulex 10Gb 2-port converged network adapter) uses the equivalent resources of two ports. Make sure that you account for this use of resources when assigning a dedicated NIC.	--	Y
Each port of a dedicated NIC (1000BASE-T 4-port LAN adapter) uses the equivalent resources of two ports. Make sure that you account for this use of resources when assigning a dedicated NIC.	Y	Y
Each port of a dedicated NIC (10Gb 2-port LAN adapter) uses the equivalent resources of two ports. Make sure that you account for this use of resources when assigning a dedicated NIC.	Y	Y
When the number of assigned processors is 32 or less: Each port of a dedicated NIC (10GBASE-T 2-port LAN adapter) uses the equivalent resources of three ports. Make sure that you account for this use of resources when assigning a dedicated NIC.	Y	Y
When the number of assigned processors is 33 or more: Each port of a dedicated NIC (10GBASE-T 2-port LAN adapter) uses the equivalent resources of five ports. Make sure that you account for this use of resources when assigning a dedicated NIC.		
Each port of a shared NIC, virtual NIC, and VF NIC uses the equivalent resources of one port. Make sure that you account for this use of resources when assigning a shared NIC, virtual NIC, or VF NIC.	Y	Y
Four FC ports use the equivalent resources of one port. Make sure that you account for this use of resources when assigning an FC port.	--	Y
Legend: Y: Applicable --: Not applicable		

Table 1-20 NIC assignment in Windows (Windows Server 2016)

Item	Windows Server 2016
A maximum of six ports can be assigned for each core.	Y

Item	Windows Server 2016
Each port of a dedicated NIC (1000BASE-T 4-port LAN adapter) uses the equivalent resources of one port. Make sure that you account for this use of resources when assigning a dedicated NIC.	Y
Each port of a dedicated NIC (10Gb 2-port LAN adapter) uses the equivalent resources of two ports. Make sure that you account for this use of resources when assigning a dedicated NIC.	Y
Each port of a dedicated NIC (10GBASE-T 2-port LAN adapter) uses the equivalent resources of two ports. Make sure that you account for this use of resources when assigning a dedicated NIC.	Y
Each port of a shared NIC, virtual NIC, and VF NIC uses the equivalent resources of one port. Make sure that you account for this use of resources when assigning a shared NIC, virtual NIC, or VF NIC.	Y
Four FC ports of a Hitachi 8Gb FC adapter use the equivalent resources of one port. Make sure that you account for this use of resources when assigning an FC port.	Y
Three FC ports of the Hitachi 16Gb FC adapter use the equivalent resources of one port. Make sure that you account for this use of resources when assigning an FC port.	Y
Legend: Y: Applicable	

Multicast communication errors

When all of the following occurrence conditions are met, multicast packets that use shared NIC cannot be sent or received:

- When the firmware version of LPAR manager being used is 02-02 to 02-20.
- When the external switch settings on the multicast communication route match No. 2 in the following table:

Table 1-21 The external switch settings on the multicast communication route

No.	External switch settings		Communication error
	IGMP Snooping	IGMP Querier	
1	Enabled	Enabled	None
2	Enabled	Disabled	Occurred
3	Disabled	Enabled	None
4	Disabled	Disabled	None

Apply the following workaround if the occurrence conditions above are met:

1. Set IGMP Querier for the external switch to "Enable". (Recommended)

This setting is required for the external switch that is connected to the virtual switch on the LPAR manager. However, if this workaround is performed and the external switch is using IGMP Membership Query of IGMPv2, the IGMPv3 function (source filtering) cannot be used.

2. Set IGMP Snooping for the external switch to "Disable".

The same setting is required for all external switches on the multicast communication route. However, if this workaround is performed, the network performance might decrease because the multicast packets are sent to all ports. If you want to decrease the load, set VLAN for the virtual and external switches.

Notes on FC configurations

This section provides notes on the configuration of fibre channel adapters.

Notes on using fibre channel switches

- To use a shared FC, enable NPIV on the ports of the connected fibre channel switch.
You can check whether NPIV is enabled by using the `portcfgshow` command for the fibre channel switch. You can enable NPIV by using the `portcfgnpivport` command for the fibre channel switch. For details about commands, see the documentation for the fibre channel switch you are using.
- When Auto Negotiation is set as the speed of an FC port of the fibre channel switch (the default setting), the transfer speed of the FC port might not match that of the Fibre Channel card. This discrepancy can make the storage LUs inaccessible. In this scenario, use the `portcfgspeed` command to set the transfer speed of the FC port to the same speed as the Fibre Channel card that you are using.

Notes on using fibre channel adapters

- The following table shows the availability of shared FC under the connection configurations.

Table 1-22 Whether a shared FC is available for each connection configuration

Connection configuration			Can shared FC be used?	
			8Gb fibre channel adapter	16Gb fibre channel adapter
Connects with storage via a fibre channel switch	The fibre channel switch supports NPIV.	PtoP connection	Yes	Yes
		FC-AL (Loop) connection	No	No
	The fibre channel switch	PtoP connection	No	No

Connection configuration			Can shared FC be used?	
			8Gb fibre channel adapter	16Gb fibre channel adapter
	does not support NPIV.	FC-AL (Loop) connection	No	No
Connects directly to storage		PtoP connection	No	Yes ^{1,2}
		FC-AL (Loop) connection	Yes	Yes ¹
Notes: 1. Set the Enable to Multiple Port ID. 2. This connection configuration is available when supported by connection destination disk array devices. For information about support specifications of disk array devices to be connected, see the manuals for them.				

- In an environment in which a 16Gb fibre channel adapter and a Hitachi disk array controller (Hitachi Virtual Storage Platform) are connected in the Fabric Emulation method, the following operations cause a shared fibre channel port to be down. In this case, the system log message of LPAR manager "LP detected Link Down error for Shared FC." may be logged.
Also, if this log message is logged when a guest OS is booting, the error log "(ErrNo: 14, Error name: HFC_ERRB, Contents: Link Down Detected Link Down interruption)", indicating a fibre channel adapter is down on a guest OS, may be logged.
- If you configure the PtoP connection when disk array devices that do not support the PtoP connection in the storage direct connection configuration are connected, booting the guest OS might take long or fail, which causes a phenomenon like a hang-up. In such cases, change the Connection Type setting on the HBA side. For the setting procedure, see the manual Hitachi Gigabit Fibre Channel Adapter User's Guide (BIOS/EFI Edition).
- If Boot Function is enabled and the HBA settings are not correct, the error might occur in the Boot order settings dialog box of the LPAR selected in the LPAR tab on the Web console. In such cases, in the Set HBA port dialog box of the LPAR, disable Boot Function, and then in the Boot order settings dialog box of the LPAR, select the HBA tab and click the HBA boot settings button to check and change the settings.

Notes on USB devices

This subsection describes notes on USB devices.

Notes on attaching a USB device in exclusively shared mode to an LPAR

- To use a USB device in exclusively shared mode in an LPAR, assign the USB device to the LPAR before activating the LPAR. You cannot select an

LPAR to which a USB device is not assigned as the LPAR to which the USB device is to be attached.

- An LPAR must be already activated when you attach a USB device in exclusively shared mode to the LPAR.

If an LPAR is deactivated or cannot be used (in a failure state), you cannot select the LPAR as the LPAR to which a USB device is to be attached.

If an LPAR to which a USB device is attached enters a failure state, you might no longer be able to detach the USB device from the LPAR and attach it to another LPAR.

Notes on detaching a USB device in exclusively shared mode

- Before detaching the USB device in exclusively shared mode, make sure that the following conditions are met:
 - The OS is not booting or rebooting.
 - After the USB device is recognized by the OS or firmware and is made available, you detach the USB device from the OS by performing a safe hardware removal operation for Windows or an unmount operation for Linux.
 - Do not hold **Alt**, **Windows**, **Ctrl**, and **Shift** keys down while the remote console is displayed.

If you detach the USB device while these conditions are not met, the following problems might occur.

- The firmware and OS become unstable, or the OS hangs.
- An attempt to read and write data fails, or the display of the USB device remains on the OS.
- Keyboard operations cannot be performed properly.

If detaching the USB device causes the above problems to occur, perform the procedure appropriate for the problem.

- If the firmware and OS become unstable, or the OS hangs, attach the USB device.
If this does not restore proper operation of the OS, deactivate the LPAR and then activate it again.
- If the display of the USB device remains on the OS, attach the USB device, and then detach it again.
- If keyboard operations cannot be performed properly, some key might be held down on the OS. In this case, perform the following operation.
 - For Windows, display the OS from the remote console or the remote desktop in full-screen mode, and then press all of the **Alt**, **Windows**, **Ctrl**, and **Shift** keys, which are on the right and left sides.
 - For Linux, display the OS from the remote console, and then press all of the **Alt**, **Ctrl**, and **Shift** keys, which are on the right and left sides.

- An error message might appear when you detach a USB device in Linux. Unless the USB device was mounted, this will not affect the data on the USB device or the subsequent operation of the OS.

Notes on recognizing a USB device

- If you attach a USB device in exclusively share mode to an LPAR, the running OS on the LPAR recognizes the USB device automatically. However, depending on the OS status or if the USB device is not detached successfully, the OS might be unable to recognize the USB device automatically. If the USB device is not recognized for a while, perform the following procedure:
 - Detach the USB device and then attach it again.
 - Physically disconnect and connect the USB device to the server blade.
 - For Windows, uninstall the driver of the USB device, and then install it again.
 - If an error related to recognition of the USB controller is displayed on the OS, restart the OS.
- A CD/DVD drive might not be recognized if you use a different USB port from the one used when registering the EFI boot option. In this scenario, register the boot option again.
- If you right-click on the USB device in Windows Explorer and select Eject, the USB device might not be recognized even after you attach the USB device again or restart the OS, depending on the USB device you are using. In such cases, disconnect and connect the USB device to make it recognized.

Other

- An error message might appear when you detach a USB device in Linux. Unless the USB device was mounted, this will not affect the data on the device or the subsequent operation of the OS.
- Do not connect a disk with a GUID partition table (GPT) to the front USB port on the server blade, the USB port of the KVM cable, or the virtual media on the remote console when LPAR manager is starting. If LPAR manager fails to start with a GPT disk connected, disconnect the GPT disk and then restart LPAR manager.
- Do not use devices that are not supported by LPAR manager. If you use an unsupported device, problems such as the EFI on the LPAR not recognizing the device or the OS failing to boot might occur. For devices supported by LPAR manager, see [List of PCI devices supported by LPAR manager on page B-2](#).

SMP configuration

- Of the server blades that make up the SMP configuration, the server blade that has the lowest slot number acts as the primary server blade. The other server blades act as non-primary server blades.

- If different LPAR manager models (Essential, Advanced, and Enterprise) are used for the server blades in the SMP configuration, the lower model is used for startup.
- If the expiration dates of the LPAR manager licenses are not the same, the license with the earliest expiration date will be used to start the server blade.
Note that if the expiration date has passed, a server blade will start as the Essential model.
- For the LPAR manager firmware, the firmware assigned to the primary server blade is used.
- For the LPAR manager configuration information, the configuration information set on the primary server blade is used.
- USB devices connected to the front USB ports on the primary server blade or non-primary server blades, USB devices connected to the primary server blade via a KVM cable, and the remote console of the primary server blade can be used in LPARs.
- When using CB 520X B1 in a 4-blade SMP configuration, disable SAS controller on the EFI setup menu. If all the following conditions are met, the server blade might get stuck in a reboot loop and fail to boot.
 - a. SAS controller is enabled.
 - b. Either of the following operation is performed.
 - Updating the LPAR Manager Firmware to version 02-45 or higher
 - Adding a configuration such as LPAR or shared NIC when the Firmware version is 02-45 or higher

Maximum resolution of a remote console

The maximum window size that can be displayed on the remote console is 1024 x 768 pixels. If you use the remote console to remotely control a guest OS installed on an LPAR, the recommended settings for resolution and color depth of the guest OS are as follows:

Table 1-23 Recommended resolution and color depth

Guest OS	Recommended resolution	Recommended color depth
Windows	1024 x 768	32 bit
Red Hat Enterprise Linux		24 bit



Tip:

- To use remote connection software other than the remote console, see the software documentation or Help for details about the OS and the window size that can be displayed.
- For example, when using Windows Remote Desktop Connection, the maximum Windows size for the guest OS that can be displayed is equal to the maximum resolution.

**Note:**

- If you are using Windows Server 2012 or later, the recommended settings for resolution and color depth of the guest OS are 1024 x 768 pixels and 32 bits, respectively. You cannot change these window settings.
- If you specify a resolution that is 1024 x 768 or higher, a scroll bar will appear in the remote console window.
- If the resolution for the guest OS is not 1024 x 768, window drawing by using the remote console and mouse operations is less responsive.
- If you use the GUI for the guest OS to set the resolution for Red Hat Enterprise Linux, the resolution and color depth might not be set correctly. Alternatively, window drawing might be scrambled after they are set.

In such cases, edit the `/etc/X11/xorg.conf` file to set the resolution and color depth for the OS.

Editing `/etc/X11/xorg.conf` to set the resolution and color depth for Red Hat Enterprise Linux

Use a text editor to edit the `/etc/X11/xorg.conf` file as follows:

1. Verify that `vesa` is entered in the `Driver` line in the `Device` section.
If a value other than `vesa` is specified, change it to `vesa`.

```
Section "Device"
    Identifier "Videocard0"
    Driver     "vesa"
EndSection
```

2. Check whether the `Monitor` section exists.
If the `Monitor` section does not exist, add it based on the following setting example:

```
Section "Monitor"
    Identifier "Monitor0"
    ModelName  "LCD Panel 1024x768"
    HorizSync  31.5 - 48.0
    VertRefresh 56.0 - 65.0
    Option     "dpms"
EndSection
```

3. Edit the `Screen` section as follows:
 - Enter the resolution 1024x768 to the `Modes` line of the `Display` subsection in the `Screen` section.
If the `Modes` line does not exist, add the line.
 - Enter the color depth 24 to the `DefaultDepth` line in the `Screen` section.
Similarly, enter the color depth 24 to the `Depth` line of the `Display` subsection in the `Screen` section.

```
Section "Screen"
  Identifier      "Screen0"
  Device          "Videocard0"
  Monitor         "Monitor0"
  DefaultDepth    24
  SubSection "Display"
    Viewport      0 0
    Depth         24
    Modes         "1024x768"
  EndSubSection
EndSection
```

4. To apply the resolution setting, restart the guest OS.

Starting and Stopping LPAR manager

This chapter describes how to start and stop LPAR manager running on server blades. This chapter also describes how to restart LPAR manager.

- ☐ [Preparing the server blades so that they can operate in LP mode](#)
- ☐ [Checking the status of a server blade](#)
- ☐ [Starting LPAR manager](#)
- ☐ [Restarting LPAR manager](#)
- ☐ [Stopping LPAR manager](#)

Preparing the server blades so that they can operate in LP mode

The following items must be configured to operate the server blade in LP mode.

1. Ensure the appropriate LPAR manager firmware is selected.
2. Set the operation mode and network address for the server blade on which LPAR manager is applied.



Note:

- When using CB 520X B1 in a 4-blade SMP configuration, disable SAS controller on the EFI setup menu.
- When using the server blades in the following table, change the EFI settings as shown below.
If you do not change the settings, you might not be able to start the LPAR manager.

Table 2-1 Server Blade and EFI settings

Server Blade	IOEU	PCI 64-bit Resource Allocation	MM Config Base
CB 520X B1	No	Enable (default)	2GB (default)
	Yes	Disable	2GB (default)
CB 520X B2	No	Enable (default)	3GB (default) ¹
	Yes	Disable	3GB (default) ¹
CB 520X B3	No	Enable (default)	3GB (default)
CB 520H B3	No	Enable (default)	2GB (default)
	Yes	Disable	2GB (default)
CB 520H B4	No	Enable (default)	2GB (default)
Notes:			
1. In a 1-blade or 2-blade SMP configuration, the LPAR manager can be started even when MM Config Base is set to 2 GB. In a 4-blade SMP configuration, make sure to change to 3 GB.			

Related topics

- Manual *Hitachi Compute Blade 2500 Series UEFI Setup Guide*

Connecting to the management paths

To configure the management paths so that the LPAR manager can communicate with the management module and the management servers.

- To configure the network, LPAR manager can communicate with the management module via the management paths.

- For detail the NIC to use in the management paths and how to configure, see the Related topics.

Related topics

- [Management path and operation path on page 1-12](#)
- [Setting the operation mode and network address on page 2-3](#)

Checking and setting the LPAR manager firmware

Ensure the appropriate is selected. You can use the management module to check and set the LPAR manager firmware to be applied to the server blade.

The procedure for checking the LPAR manager firmware from the management module is described below.

1. From the global taskbar in the Web console, select the **Resources** tab. In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the server blade that you wish to start in LP mode. In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab, and from the **Edit** menu, select **Assign firmware to Server Blade**. The **Assign firmware to Server Blade** dialog box is displayed.
4. In the **Assign firmware to Server Blade** dialog box, check the value selected in the **LP firmware version** drop-down list. If the value is correct, click the **Next** button. A dialog box is displayed, prompting you to confirm the content of the settings. Respond appropriately and close the dialog box. Checking and setting the LPAR manager firmware is now complete.

Setting the operation mode and network address

On the server blade to which LPAR manager is applied, configure the following settings.

You must set at least either an IPv4 address or an IPv6 address for LPAR managers. Note that you can set both an IPv4 address and an IPv6 address for LPAR managers.

- LP mode
- LP IP address (IPv4 or IPv6)
- LP-Management module communication (management module firmware version: A0130 or later)
- VNIC System No.
- time zone

- Management paths (management module firmware version: A0120 or later)



Tip:

- When you desire to allow an LPAR manager to communicate with the management module in IPv6, you must set an IPv6 address for the LPAR manager and the management module in advance. In addition also set LP-Management module communication.
- Set an LP IP address in an internet protocol in which you desire to allow manager servers to communicate with LPAR managers. You can also set two LP IP addresses in both IPv4 and IPv6 for an LPAR manager.
- Take the following points into account when you use an IPv6 address as management paths:
 - The following versions of firmware are supported:

Table 2-2 Firmware versions

Server blade	Server blade firmware	Management module firmware	LPAR manager firmware
CB 520X B1	07-34 or later	A0130 or later	02-25 or later
CB 520X B2	09-17 or later	A0135 or later	02-27 or later
CB 520X B3	11-04 or later	A0165 or later	02-55 or later
CB 520H B3	08-35 or later	A0130 or later	02-25 or later
CB 520H B4	10-03 or later	A0160 or later	02-50 or later

- The following table shows whether each console supports LP IP addresses in IPv6.

Table 2-3 Supporting IP addresses of the consoles in IPv6

Console	Supporting IP addresses in IPv6
HCSM	N
Web console	Y
HVM Navigator	N
Virtual COM console	Y
LP web system	N
Legend: Y: Supported N: Not supported	

- Before you set an IPv6 address from the Web console, turn off the server blade.
- To downgrade one of the above firmware versions to a previous version, disable the IPv6 setting beforehand.

- In an N+M cold standby configuration, the firmware versions of LPAR manager, the management module, and server blade on the standby blade must be equal to or later than those versions on the active blade. If any of the versions is older than the supported version that is mentioned above, LPAR manager starts in an unexpected state or does not start when the blade is switched.
-

Use the management module to set these items. The procedure for configuring the setting items from the management module is described below. You must first log in to the management module via the Web browser on the system console.

1. From the global taskbar in the Web console, select the **Resources** tab. In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the server blade that you wish to start in LP mode. In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab, and from the **Edit** menu, select **System settings**. The **System settings** dialog box is displayed.
4. In the **System settings** dialog box, under **Logical partitioning**, click the LP mode option button. Additional configurable items are displayed.
5. In the **System settings** dialog box, check and set the following items:
 - For IPv4
 - **IP address**
 - **Subnet mask**
 - **Default gateway**
 - **LP-Management module communication**
 - **VNIC system No.**
 - **Time zone**
 - **Management path**
 - For IPv6
 - **Static address**
 - **IP address**
 - **Prefix len**
 - **Default gateway**
 - **Address**
 - **Stateless address**
 - **LP-Management module communication**
 - **VNIC system No.**
 - **Time zone**

- **Management path**
- 6. In the **System settings** dialog box, click the **Confirm** button.
Close the windows that are displayed one by one to complete the setting.

Related topics

- [NIC to be used for management path communication on page 1-13](#)
- [Setting the ports to be used for management path communication on page 8-3](#)

Checking the status of a server blade

This section describes how to check the virtual WWN and virtual MAC address of a server blade where LPARs are to be configured.

Checking the virtual WWN of a server blade

The procedure below shows how to check the virtual WWN of a server blade on which LPARs are to be configured. Note that, if you perform LPAR migration, the virtual WWN changes.

1. From the **Systems** tree view in the **Resources** tab, click **WWN Management**.
2. Select the server blade on which LPARs are to be configured and then, from the **Show details** menu, select **Virtual WWN**.
The **Original Virtual WWN List** dialog box appears.
3. Check the virtual WWN information.
To output the virtual WWN information to a CSV file, click **Export to CSV**.

Checking the virtual MAC address of a server blade

The procedure below describes how to check the virtual MAC address of a server blade on which LPARs are to be configured. Note that if you perform LPAR migration, the virtual MAC address changes.

1. From the **Systems** tree view in the **Resources** tab, click **MAC Management**.
2. Select the server blade, and from the **Show details** menu, click **Virtual MAC**.
The **Original Virtual MAC List** dialog box appears.
3. Check the virtual MAC address information.
To output the virtual MAC address information to a CSV file, click **Export to CSV**.

Configuring the address for communication between a management tool and LPAR manager

To perform operations on LPAR manager by using an external management tool such as HVM Navigator or the command HvmSh, you need to configure settings so that the management tool can communicate with LPAR manager.

Configure the LP CLI IP address by using the Web console.

1. Use the Web console to log in to the management module.
2. From the **Modules** tree view in the **Resources** tab, select the target server blade on which LPAR manager is running.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. From the **Edit** menu, select **Edit LP CLI**.
The **Edit LP CLI** dialog box appears.
4. If necessary, specify the IP addresses of the management tools that communicate with LPAR manager, for **CLI1** to **CLI8**.

Click **Confirm** to close the **Edit LP CLI** dialog box. The settings are applied.



Tip:

- Set an LP IP address in an internet protocol in which you desire to allow manager servers to communicate with LPAR managers. You can also set two LP IP addresses in both IPv4 and IPv6 for an LPAR manager.
-

Starting LPAR manager

When you power on a server blade where LPAR manager is installed and whose operation mode is LP mode, LPAR manager also starts.

- Depending on the configuration state of the server blade, it might take approximately 10 to 15 minutes for the server blade to complete startup after it is powered on.
- During the period from when the server blade is powered on to when LPAR manager completes startup, the startup status of LPAR manager is displayed in the LPAR tab. To check the most recent startup status, click the Refresh button on the Web console.
- If you check the startup status immediately after powering on the server blade, acquisition of the startup status might fail. In such a case, you can acquire the correct startup status by clicking the Refresh button on the Web console again.

This section describes how to use the Web console to access the management module and start LPAR manager.

Before starting LPAR manager, be sure to set up the network cabling for the management path and to set the operation mode for the server blade. For details, see the description in the manual *Hitachi Compute Blade 2500 Series Getting Started Guide*.

For an FCoE boot, specify the following settings before starting the LPAR manager.

- Set Personality of the Emulex adapter to FCoE.
- Specify FCoE for the Emulex adapter.

For details on how to specify these, see the manual *Hitachi Compute Blade Emulex Adapter User's Guide for Hardware*.

Using the Web console to power on a server blade

You must first log in to the management module via the Web browser on the system console.

1. From the global task bar of the Web console, select the **Resources** tab. In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the target server blade. In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **State** tab and click the **Power On** button.



Tip:

- Powering server blades on or off by using the remote console
You can use the remote console to power server blades on or off. For a server blade on which LPAR manager is running, powering the server blade on or off affects all LPARs running on LPAR manager. For this reason, you cannot use the remote console to power on or power off server blades running in LP mode. To power on or power off server blades running in LP mode, use the Web console.



Note:

- For the LPAR manager firmware version 02-62 or later, the LPAR manager system time is reset to 2000/01/01 00:00:00 when LPAR manager starts, unless the physical RTC time is set within the range from years 2000 to 2099. Then, the reset time is saved in the physical RTC. In the LPAR manager system log, system event log, and HCSM alert, you can check that the LPAR manager system time is reset.
-

Related topics

- Manual *Hitachi Compute Blade 2500 Series Getting Started Guide*
- Manual *Hitachi Compute Blade 2500 Series Management Module User Guide*
- Manual *Hitachi Compute Blade Emulex Adapter User's Guide for Hardware*

Restarting LPAR manager

This section describes how to restart LPAR manager from the Web console. Note that you can only restart LPAR manager when the status of all LPARs associated with that LPAR manager are in Deactivate status.

To restart LPAR manager from the Web console:

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. On the **LPAR** tab, from the **Action** menu, select **Restart LPAR manager**.
3. In the **Restart LPAR manager** dialog box, click **OK**.



Note:

- If you are unsure as to whether you have saved the configuration information, save the information before shutting down LPAR manager. If you shut down or restart LPAR manager before saving the configuration information, the settings you entered will be lost.
-

Stopping LPAR manager

This section describes how to stop LPAR manager. Note that you can only stop LPAR manager when the status of all LPARs associated with that LPAR manager are in Deactivate status.

To stop LPAR manager, use the Web console.

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. From the **Action** menu in the **LPAR** tab, select **Shutdown LP**.
3. In the **Shutdown LP** dialog box, click **OK**.
Processing to stop LPAR manager starts. After LPAR manager stops, the server blade is powered off.



Note:

- If you are unsure as to whether you have saved the configuration information, save the information before shutting down LPAR manager. If you shut down or restart LPAR manager before saving the configuration information, the settings you entered will be lost.
-

Creating LPARs

This chapter describes how to create LPARs.

- ☐ [Creating LPARs](#)
- ☐ [Setting NUMA](#)
- ☐ [Setting the boot order for LPARs from the Web console](#)
- ☐ [Setting the boot order for LPARs from UEFI](#)
- ☐ [Changing the configuration of an LPAR](#)
- ☐ [Saving the LPAR manager configuration](#)
- ☐ [Deleting LPARs](#)

Creating LPARs

The following describes how to create LPARs from the Web console.

Tasks to complete before creating LPARs

- Start the server blade in LP mode

To create an LPAR from the Web console:

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
For an FCoE boot, on the **LPAR** tab, click **Scheduling mode** from the **Action** menu, and then set the NIC scheduling mode to dedicated mode.
2. On the **LPAR** tab, click **Add LPAR**.
The **Add LPAR** dialog box appears.
3. Set the LPAR name, the number of processors to allocate, the scheduling mode of the processors, and the memory to allocate to the LPAR.



Note:

- You can allocate a maximum of 64 processors. The maximum amount of memory you can allocate is the total installed memory minus the memory used by LPAR manager (in GB).
- The LPAR name assigned by default is "LPARX_xx" (where X is the LPAR number and xx is the VNIC System Number assigned to LPAR manager).

-
4. In the **HBA** panel in the **Add LPAR** dialog box, click the **Set Port** button.
The **Set HBA port** dialog box appears.
For an FCoE boot, you do not need to specify the HBA port settings.
 5. Specify the following items, and then click **OK**.
 - Select the check boxes for the ports to be assigned. You can assign as many ports as the number of installed ports.
 - Select the WWPN you want to use.
 - Disable the boot functionality.

The **Set HBA port** dialog box closes and the **Add LPAR** dialog box reappears.

For an FCoE boot, you do not need to specify the HBA port settings.



Note:

- Do not enable the boot functionality until you perform the procedure in Setting up the HBA boot driver on [Setting up the HBA boot driver on page 3-6](#) or [Setting up the UEFI driver on page 3-7](#). If you enable the boot functionality before you set the HBA settings appropriately, a phenomenon like a hang-up might occur. In this case, nothing is displayed on the screen of the LPAR.

-
6. In the **NIC** panel of the **Add LPAR** dialog box, click the **Set Port** button.
The **Set NIC port** dialog box appears.

7. Select the ports and network segments you want to assign, and then click **OK**.

The maximum number of ports (segments) you can assign is 16 (1a, 1b, and so on) for a shared NIC, 16 (1av, 1bv, and so on) for a VF NIC, and 4 (Va, Vb, and so on) for a virtual NIC.

If you close the **Add LPAR** dialog box by clicking the **Confirm** button or by another method, LPARs are created.

Related topics

- [LPAR manager Menu screen on page 10-5](#)
- [PCI Device Assignment screen on page 10-30](#)
- [Virtual NIC Assignment screen on page 10-34](#)
- [Shared FC Assignment screen on page 10-42](#)

Setting NUMA

To apply NUMA to the LPAR manager, you must configure NUMA settings for the LPARs. In addition, you must configure settings so that the memory-interleaving NUMA can be used on server blades. The memory interleaving of the server blade can be set by using the UEFI.

For details about how to enable NUMA on server blades and LPARs, see the related topics.



Note:

- If you change the MM Config Base setting for the EFI, the memory amount that can be allocated to each node is changed. Therefore, the activation of an LPAR with a specified memory node might fail due to a memory shortage in the node. If you change the MM Config Base settings, review the memory node numbers and the memory amount that is allocated to each LPAR. For details about how to check memory node numbers and the memory amount that is allocated to each LPAR, see the description of the Logical Partition Configuration screen.
- When NUMA is set, the default method for setting logical processors is binding physical processors.
In addition, physical processors are bound by default in the following cases:
 - When NUMA is enabled for an LPAR
 - When the LPAR configuration information saved by the LPAR manager whose version is earlier than 02-40 is inherited

Related topics

- Manual *Hitachi Compute Blade 2500 Series UEFI Setup Guide*
- [Applying NUMA to an LPAR on page 5-14](#)
- [Logical Partition Configuration screen on page 10-8](#)

Setting the boot order for LPARs from the Web console

This section describes how to set the boot order by using the Web console, to set up a guest OS on an LPAR. You can also use UEFI to set the boot order

To set or change the boot order, make sure that the LPAR is deactivated.



Note:

- After installing the guest OS, if you set up a multi-path configuration for the connection with storage systems, create a boot order for each path. Note that, if the boot mode is logical EFI (X64.UEFI) mode, installing the guest OS automatically creates a boot order. This boot order can be used for each path in the multi-path configuration, so you do not need to create individual boot orders for each path.

Setting the boot order

The following describes how to set the boot order from the Web console.

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. In the **Server Blade** panel, select the **LPAR** tab.
3. On the **LPAR** tab, select the LPAR whose boot order you want to set, and then click the LPAR name.

The **LPAR Information** dialog box appears.

4. Check the settings of the LPAR, and click the **Boot order settings** button.

After you respond to the confirmation window, the **Boot order settings** dialog box appears.

5. In the **USB** tab, select the devices you want to add, and then click the **Add to boot order** button.

If required devices are not displayed, make sure the devices are recognized by following the procedure in [Connecting virtual drives on page 3-5](#).

6. Make sure that required devices are displayed in the **HBA** tab.

If required devices are not displayed, make sure the devices are recognized by following the procedure in [Setting up the HBA boot driver on page 3-6](#).



Tip:

- If the boot mode is UEFI mode, you do not need to add an HBA device because the device is automatically added to the boot order when the OS is installed.

7. Use **Move selection up** and **Move selection down** to change the boot order to the following sequence.
 - CD/DVD-KVM
 - EFI-SHELL

Close the dialog box to finish the setting the boot order.

Related items

- [Connecting virtual drives on page 3-5](#)
- [Setting up the HBA boot driver on page 3-6](#)

Connecting virtual drives

If you want to access a CD/DVD drive or virtual media from the activated LPAR, you need to make the server blade recognize them by using the virtual media functionality of the remote console. This section describes how to connect a CD/DVD drive or virtual media to a server blade as a virtual drive.

For details about the remote console and the virtual media console, see the descriptions in the manual *Hitachi Compute Blade 2500 Series Getting Started Guide*.

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. In the **Server Blade** panel, select the **LPAR** tab.
3. On the **LPAR** tab, select the LPAR whose boot order you want to set, and then click the LPAR name.
The **LPAR Information** dialog box appears.
4. Check the settings of the LPAR, and click **Boot order settings**.
After you respond to the confirmation window, the **Boot order settings** dialog box appears.
5. In the **Boot order settings** dialog box, select the **USB** tab.
6. Select the USB device, and start the remote console by using the **Start remote console** button.
7. Execute the **Tools - Launch Virtual Media** command of the remote console.
The Virtual Media Session window appears.
8. Select the **Mapped** column check box for the CD/DVD drive or image file you want to use as a boot device.
After you respond to the message dialog box, a virtual drive is added as a boot device to the USB device in the **Boot order settings** dialog box.



Note:

- Do not use the Exit button or x button to close the virtual media console window while using a virtual drive. Also, do not shut down the remote console. If you close the virtual media console window or the remote console, the virtual media session is terminated. At this point, all virtual drives are disconnected from the server blade and are no longer recognized.



Tip:

- If you perform the Attach operation or start a remote console on the Web console when USB Auto Allocation to LPAR is set to Disable, the USB Auto Attach setting is enabled for the target LPAR. After the USB Auto Attach setting is enabled for the target LPAR, a USB device is automatically assigned to the LPAR if the LPAR is activated for the first time to install OS or if the OS is rebooted for the first time.

If you detach a USB device from an LPAR on the Web console, the USB Auto Attach setting is disabled for the LPAR.

Related topics

- Manual *Hitachi Compute Blade 2500 Series Getting Started Guide*

Setting up the HBA boot driver



Note:

- For an FCoE boot, you do not need to specify the HBA boot driver settings.
-

If necessary devices are not displayed in the HBA tab, perform the following procedure to set up the HBA boot driver.

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. In the **Server Blade** panel, select the **LPAR** tab.
3. On the **LPAR** tab, select the LPAR whose boot order you want to set, and then click the LPAR name.
The **LPAR Information** dialog box appears.
4. Check the settings of the LPAR, and click **Boot order settings**.
After you respond to the confirmation window, the **Boot order settings** dialog box appears.
5. In the **Boot order settings** dialog box, select the **HBA** tab.
6. Select the HBA port, and click the **HBA boot settings** button.
The **HBA boot settings** dialog box appears.
7. Specify the items as follows in the **Set HBA boot** dialog box.
 - For **Boot Function**, specify **Enabled**.
 - For **Select Boot Device**, specify **Enabled**.
 - When N+M cold standby (LUID mode) is used, specify **Enabled** for **LUID Scan Mode**. When N+M cold standby (LUID mode) is not used, specify **Disabled** for **LUID Scan Mode**.
If **LUID Scan Mode** does not appear, this setting is not required.
 - For **Boot Device List**, specify the port information of an external disk array device to be connected.
For **WWN**, specify the WWN of the port. For **LUN**, specify the LU number of the port.

- For **Connection Type**, specify the value shown in [Table 3-1 Fibre channel adapter and connection types on page 3-9](#).
- When the connection configuration is connects directly to storage, specify the values for **Multiple PortID** and **Data Rate** show in [Table 3-1 Fibre channel adapter and connection types on page 3-9](#) according to the link speed of the storage.

When you are changing **Connection Type**, **Multiple PortID** and **Data Rate**, the following conditions must be met.

- If the management module firmware version is A0113 or earlier, the target fibre channel adapter must be in dedicated mode. When in shared mode, switch to dedicated mode temporarily.
- If the management module firmware version is A0120 or later and the target fibre channel adapter is in shared mode, all LPARs must be deactivated.

Close the dialog boxes in order and finish the HBA boot driver settings.

Related topics

- [Using N+M cold standby \(LUID mode\) to start LPARs on page 6-22](#)
- Manual *Hitachi Gigabit Fibre Channel Adapter User's Guide (BIOS/EFI Edition)*

Setting the boot order for LPARs from UEFI

This section describes how to use UEFI to set the boot order, to set up and boot the guest OS on the LPAR. You can also use the Web console to set the boot order

Set the boot order to allow the guest OS to boot on the LPAR.

Setting up the UEFI driver



Note:

- For an FCoE boot, you do not need to specify the UEFI driver settings.

To use SAN boot, you must set up the UEFI driver.

First start the remote console and display the guest screen for which SAN boot is to be used.

To check the boot order of EFI Internal Shell:

1. From the menu of the guest screen, select **Boot Maintenance Manager**. The Boot Maintenance Manager window appears.
2. Select **Boot Options**, and then in the displayed window, select **Change Boot Order**.
3. Check the boot order of **EFI Internal Shell**.

If **EFI Internal Shell** is displayed first, quit Boot Maintenance Manager and go to the procedure "To set the fibre channel adapter" below.

If **EFI Internal Shell** is not displayed first, perform the following operations.

4. Select **Change the order** and change the boot order so that the EFI Internal Shell boot option is displayed first.
5. Select **Commit Changes and Exit**. Press the **Esc** key to quit Boot Maintenance Manager.

To set the fibre channel adapter:

1. From the menu of the guest screen, select **Continue** to start EFI Shell.
2. Execute the `drivers` command and then check the Hitachi Fibre Channel Driver handle.

Depending on the type of a fibre channel adapter, either of the following is displayed in the command results:

8Gb FC adapter: Hitachi PCI-X/PCIe Fibre channel Driver

16Gb FC adapter: Hitachi PCI-X/PCIe Fibre channel Driver

For example, if the command results display `78 10000206 D X - 1 - Hitachi PCI-X/PCIe Fibre channel Dr ScsiBusFive`, the driver handle is "78".

3. Execute the command `drvcfg` with the driver handle specified for the argument and then check the controller handle.

For example, if the command results display `Drv[78] Ctrl[84] Lang[eng]`, the controller handle is "84".

If multiple FC ports are allocated, multiple controller handles are displayed. You can select any one of the displayed controller handles.

4. Execute the command `drvcfg -s` with the driver handle and the controller handle specified for arguments.
The display prompt switches to "hfcfg>".
5. Use the `select` command to select the fibre channel adapter to be used for booting.
6. Use the `set` command to set the items below. Depending on the environment, set other required settings.

- o Boot Function = Enabled
- o Select Boot Device = Enabled
- o When N+M cold standby (LUID mode) is used: `LUID scan mode = Enabled`
When N+M cold standby (LUID mode) is not used: `LUID scan mode = Disabled`
If `LUID scan mode` does not appear, this setting is not required.
- o For Boot Device List, set the WWPN of the port to be used on the target external disk array device and the LUN number (usually "0" because LU0 is the boot LU).
- o For **Connection Type**, specify the value shown in [Table 3-1 Fibre channel adapter and connection types on page 3-9](#).

- When the connection configuration is connects directly to storage, specify the values for **Multiple PortID** and **Data Rate** show in [Table 3-1 Fibre channel adapter and connection types on page 3-9](#) according to the link speed of the storage.

For details on the configuration procedure, see the manual *Hitachi Gigabit Fibre Channel Adapter User's Guide (BIOS/EFI Edition)*.

When you are changing **Connection Type**, **Multiple PortID** and **Data Rate**, the following conditions must be met.

- If the management module firmware version is A0113 or earlier, the target fibre channel adapter must be in dedicated mode. When in shared mode, switch to dedicated mode temporarily.
- If the management module firmware version is A0120 or later and the target fibre channel adapter is in shared mode, all LPARs must be deactivated.

Table 3-1 Fibre channel adapter and connection types

Connection configuration	Setting values	
	8Gb fibre channel adapter	16Gb fibre channel adapter
Connects with storage via a fibre channel switch	Connection Type: Auto or PtoP	
Connects directly to storage	Connection Type: FC-AL (Loop)	Connection Type: PtoP Multiple PortID: Enable Data Rate (Link Speed): 16Gbps
		Connection Type: FC-AL (Loop) Multiple PortID: Enable Data Rate (Link Speed): 8Gbps or less

- Use the `save` command to save the settings and then use the `exit` command to return to EFI Shell.
 - Execute the command `reconnect -r`.
 - Execute the command `map -r`.
- The displayed content vary depending on the environment. Use the `exit` command to finish setting up the fibre channel adapter.



Note:

- If the HBA device is not recognized, check and, if necessary, revise the settings of the disk array.

Related topics

- [Using N+M cold standby \(LUID mode\) to start LPARs on page 6-22](#)
- Manual *Hitachi Gigabit Fibre Channel Adapter User's Guide (BIOS/EFI Edition)*.

Creating a boot option

Create a boot option based on how the system is to be used.

Table 3-2 Boot device and boot type

Boot device	Boot type	Usage
<ul style="list-style-type: none">NO VOLUME LABEL¹SYSTEM¹	SAN boot	Starting the guest OS
<ul style="list-style-type: none">EFISECTOR¹ANACONDA¹	CD/DVD boot	Using CD/DVD
Load File	Network boot	Using the deployment manager of HCSM
Note: 1. The displayed information might vary depending on the boot medium.		



Note:

- After installing the guest OS, if you set up a multi-path configuration for the connection with storage systems, create a boot option for each path. Note that, if the boot mode is logical EFI (X64.UEFI) mode, installing the guest OS automatically creates a boot option. This boot option can be used for each path in the multi-path configuration, so you do not need to create individual boot options for each path.

Use the remote console to create boot options. First start the remote console and log in to the LPAR for which SAN boot is to be used.

For OS setup:

- From the menu of the guest screen, select **Boot Maintenance Manager**. The Boot Maintenance Manager window appears.
- Select **Boot Options**, and then in the displayed window, select **Add Boot Option**. The File Explorer window appears.
- Select the boot device for the boot option to be created.
 - If the CD and DVD devices are not recognized, set up virtual drives.
 - For the boot device, select **EFISECTOR** or **ANACONDA**.
Note that the displayed information might vary depending on the boot medium.
The example of **EFISECTOR** following:
EFISECTOR,
[Acpi (PNP0A08, 0x0) /Pci (0x1D, 0x0) /USB (0x0, 0x0) /USB (0x0, 0x0) /USB (0x2, 0x0) /Unit (0x0) /CDROM (0x1, 0x958, 0x1C11 9B)]
In addition, select <EFI>, then <BOOT>, and then BOOTX64.EFI in the subsequent windows.
- Select **Input the description** and then enter a boot device name.

- You can enter a character string of 2 to 75 characters.
- The string can contain alphanumeric characters and the following special characters: ! " # \$ % & ' () = ~ | { } _ ? * ` + > < , . / ¥ :] ; [@ ^ -

5. Select [Commit Changes and Exit] to finish creating the boot option.

If you need to re-create a boot option, perform the procedure below.

If you need to re-create a boot option because, for example, the boot option was deleted by mistake, perform the procedure below.



Note:

In Windows for which the boot mode is logical EFI (X64.UEFI) mode, a new boot option is automatically added when the guest OS starts up. This boot option is the same as the one that was automatically created when the guest OS was installed. The option can be used for each path in a multi-path configuration.

For guest OS boot:

1. From the menu of the guest screen, select **Boot Maintenance Manager**. The Boot Maintenance Manager window appears.
2. Select **Boot Options**, and then in the displayed window, select **Add Boot Option**.
The File Explorer window appears.
3. Select the boot device for the boot option to be created.

- If the HBA device is not recognized, check and, if necessary, revise the settings of the disk array.
- For the boot device, select **NO VOLUME LABEL** or **SYSTEM**.
Note that the displayed information might vary depending on the boot medium.

The example of **NO VOLUME LABEL** following:

```
NO VOLUME LABEL,
[Acpi (PNP0A08, 0x0) /Pci (0x3, 0x0) /Pci (0x0, 0x0) /Fibre (0
x50060E801024EEC3, 0x0) /HD (2, GPT, 6911384B-9BDF-4EB9-9
52E-BD8F58EAF0C7, 0x96800, 0x31800) ]
```

In Windows, select <EFI>, then <Microsoft>, then <Boot>, and then bootmgfw.efi in the subsequent windows.

For Linux, select <EFI>, <redhat>, and grub.efi.

4. Select **Input the description** and then enter a boot device name.
 - You can enter a character string of 2 to 75 characters.
 - The string can contain alphanumeric characters and the following special characters: ! " # \$ % & ' () = ~ | { } _ ? * ` + > < , . / ¥ :] ; [@ ^ -
5. Select **Commit Changes and Exit** to finish creating the boot option.

Changing the boot order

To change the priority of boot devices, reconfigure the boot order.

For OS setup:

1. From the menu of the guest screen, select **Boot Maintenance Manager**. The Boot Maintenance Manager window appears.
2. Select **Boot Options**, and then in the displayed window, select **Change Boot Option**.
The Boot Maintenance Manager window appears.
3. Select the priority of boot devices in the following order: **CD/DVD** and then **EFI Internal Shell**.
4. Select **Commit Changes and Exit** to finish changing the boot order.
If you select **Continue** from the menu of the guest screen, CD/DVD boot starts. When the screen displays **Press any key to boot from CD or DVD**, respond by pressing any key.



Tip:

- If your response is too slow, reading of CD/DVD media might fail. In such a case, deactivate and then reactivate the LPAR.
 - If you press a key multiple times, Windows Boot Manager might start. In such a case, select Windows Setup [EMS Enabled] and continue the setup procedure.
-

For guest OS boot:

1. From the menu of the guest screen, select **Boot Maintenance Manager**. The Boot Maintenance Manager window appears.
2. Select **Boot Options**, and then in the displayed window, select **Change Boot Option**.
The Boot Maintenance Manager window appears.
3. Depending on the OS running on the LPAR, set the priority of boot devices as follows:
 - In Windows: **Windows Boot Manager** and then **EFI Internal Shell**
 - In Linux: **Red Hat Enterprise Linux** and then **EFI Internal Shell**
4. Select **Commit Changes and Exit** to finish changing the boot order.



Tip:

- When the guest OS is Linux, you can change or reset the boot order by using the `efibootmgr` command of the guest OS.
-

Deleting a boot option

By deleting the boot option of a boot device, you can prevent unnecessary devices from being started.

1. From the menu of the guest screen, select **Boot Maintenance Manager**. The Boot Maintenance Manager window appears.

2. Select **Boot Options**, and then in the displayed window, select **Delete Boot Option**.
The Boot Maintenance Manager window appears.
3. Select the boot device to be deleted and execute **Commit Changes and Exit**.

Changing the configuration of an LPAR

This section describes how to change the configuration of an LPAR from the Web console. Note that you can only change the configuration of an LPAR that is in Deactivate status.

To change the configuration of an LPAR from the Web console:

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. On the **LPAR** tab, click the LPAR name of the LPAR whose configuration you want to change.
The **LPAR Information** dialog box appears.
3. Review the settings, and then click **Edit LPAR**.
The **Edit LPAR** dialog box appears.
4. Enter the required settings, and then click **Confirm**.



Note:

- After configuring the LPAR, save the updated LPAR manager configuration.
-

Related topics

- [Saving the LPAR manager configuration on page 3-13](#)

Saving the LPAR manager configuration

If you initialized or changed the configuration of LPAR manager, save the configuration. LPAR manager applies the saved configuration the next time it starts.

If you do not save LPAR manager configuration, LPAR manager returns to the non-configured state or to the previously saved configuration the next time it starts.

- If LPAR manager or the system unit is under a heavy load, the processing to save the configuration might time out. The processing to save the configuration times out after 13 minutes.
- In the LPAR Usage screen, if the Dsp value of SYS2 is 1800 ms or higher in the LPAR Usage screen, LPAR manager is under a heavy load. Save the LPAR manager configuration when LPAR manager is not under a heavy load.

To save the LPAR manager configuration from the Web console:

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. On the **LPAR** tab, click **Save settings** in the bottom right **Action** box. The **Save LPAR settings** dialog box appears.
3. Click **OK**, and then click **Close**.
The configuration information is now saved.



Tip:

- You can also use the Pre-State Auto Activation functionality to automatically save the configuration.
When an LPAR is activated or deactivated, and the status is confirmed, the LPAR status is saved. If a power failure occurs, or LPAR manager is restarted after a server blade is forcibly turned off, the LPAR is activated automatically in the saved state and the status before restarting the LPAR is restored.
To enable the Pre-State Auto Activation functionality, specify the setting in the LP Options screen.
-

Related topics

- [LP Options screen on page 10-74](#)
- [LPAR Usage screen on page 10-81](#)

Deleting LPARs

This section describes how to delete an LPAR from the Web console. Note that you can only delete an LPAR that is in Deactivate status.

To delete an LPAR from the Web console:

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. On the **LPAR** tab, select the LPAR you want to delete, and click **Delete LPAR** in the bottom right **Action** box.
3. In the **Delete LPAR** dialog box, click **OK**.

Related topics

- [LPAR manager Menu screen on page 10-5](#)

Starting and Stopping LPARs

This chapter describes how to start and stop LPARs. This chapter also describes how to restart LPARs.

- ☐ [Activating an LPAR](#)
- ☐ [Reactivating an LPAR](#)
- ☐ [Deactivating an LPAR](#)

Activating an LPAR

The following describes how to activate an LPAR from the Web console.

To activate an LPAR from the Web console:

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. On the **LPAR** tab, select the LPAR you want to activate, and then click **Activate**.

After you respond to the confirmation window, the LPAR activates.

Related topics

- [LPAR manager Menu screen on page 10-5](#)



Note:

- If the management module firmware version is earlier than A0190, when an error occurs in the server blade, the message "Check the status of the server blade." appears and the LPAR tab does not work. Eliminate the error cause, and then perform the operation again.
-

Reactivating an LPAR

If you reactivate an LPAR from the Web console, the guest OS running on the LPAR is also forcibly restarted. Remember to check the status of the guest OS before reactivating an LPAR. You can restart the guest OS normally by using the restart function in the guest OS.

The following describes how to reactivate an LPAR.

To reactivate an LPAR from the Web console:

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. On the **LPAR** tab, select the LPAR that you want to reactivate, and select **Reactivate** in the bottom right **Action** box.
3. In the **Reactivate LPAR** dialog box, click **OK**.

Related topics

- [LPAR manager Menu screen on page 10-5](#)

Deactivating an LPAR

When you deactivate an LPAR from the Web console, the guest OS on the LPAR is forcibly shut down. Remember to check the status of the guest OS before deactivating an LPAR. You can shut down the guest OS normally by using the standard shutdown process in the guest OS.

The following describes how to deactivate an LPAR.

To deactivate an LPAR from the Web console:

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. On the **LPAR** tab, select the LPAR you want to deactivate, and click **Deactivate** in the bottom right **Action** box.
3. In the confirmation window, click **OK**.

Related topics

- [LPAR manager Menu screen on page 10-5](#)

Setting Processors and Memory Functionality

This chapter describes processors that are assigned to LPARs, the functionality that can be set for memory, and how to set the functionality.

- ☐ [Setting the service ratio of a physical processor](#)
- ☐ [Setting the idle-detection functionality for processors](#)
- ☐ [Setting up processor capping](#)
- ☐ [Setting up a processor group](#)
- ☐ [Performance tuning options](#)
- ☐ [Enabling hyper-threading](#)
- ☐ [Enabling the PRTE function](#)
- ☐ [Applying NUMA to an LPAR](#)
- ☐ [Specifying a memory node](#)
- ☐ [Applying the L3 cache allocation functionality](#)

Setting the service ratio of a physical processor

Service ratio

This subsection describes how to set the service ratio of processors in shared mode. You can dynamically change the service ratio while LPARs are running.

Specify a value from 1 to 999 as the service ratio, for each LPAR. The total of these values determines the allocation ratio for each LPAR.

For example, processors in shared mode are allocated to four LPARs (LPAR 1 to LPAR 4) one by one, and the service ratio of all LPARs is set to 200. The total service ratio of the four LPARs is 800. The service ratio of LPAR 1 is 200, and the allocation rate of LPAR 1 is 25%. If the service ratio of LPAR 1 is changed from 200 to 400, the total service ratio of the four LPARs becomes 1000. The service ratio of LPAR 1 is 400, and the allocation rate of LPAR 1 increases to 40%. On the other hand, the allocation rates of LPAR 2, LPAR 3, and LPAR 4 decrease from 25% to 20%.

Table 5-1 Service ratio of processors and allocation rate of LPARs

LPAR	Before change		After change	
	Service rate	Allocation rate	Service rate	Allocation rate
LPAR 1	200	25%	400	40%
LPAR 2	200	25%	200	20%
LPAR 3	200	25%	200	20%
LPAR 4	200	25%	200	20%

Notes on service ratio

- LPAR manager partitions the performance of the physical processors used in shared mode in units of 1%.
- LPAR manager calculates the relative allocation rate of the service time with 10-millisecond time-slice accuracy, which equals 1% of the unit processor time (1 second).
- If the calculated allocation rate per logical processor is less than 1% (10 milliseconds), the service ratio is corrected so that the allocation rate is equal to 1%.
- If the number of logical processors assigned to the LPAR is less than the assigned allocation rate, the allocation rate is corrected to a rate based on the number of logical processors.

Setting the service ratio

1. Use the OS console to connect to the LPAR manager screen and then open the **Logical Partition Configuration** screen.

2. Move the cursor to the **Srv** column of the row of an LPAR to which a service ratio is to be set, and then press the **Enter** key.
The service ratio sub-screen appears.
3. Specify the service ratio.

Related topics

- [Logical Partition Configuration screen on page 10-8](#)

Setting the idle-detection functionality for processors

What is the detection of an idle state?

If the processor usage is low compared to the allocation rate, the processor idle time is given to another LPAR that requires a processor. For logical processors in shared mode, the processor time is given from LPARs whose processor usage is low to LPARs requiring a lot of processor usage.

LPARs for which the idle-detection functionality is enabled can use more processors than the allocation rate. This allows the system to use processors more efficiently.

In Figure 5-1, the idle-detection functionality is set for the processors shared by LPAR1 and LPAR2. If the processor usage is high for LPAR1 and low for LPAR2, you can increase the workload of LPAR1 by giving LPAR1 the processor time that is to be allocated to LPAR2. In contrast, if the processor usage is high for LPAR2 and low for LPAR1, you can increase the workload of LPAR2 by adjusting the processor time for the LPARs.

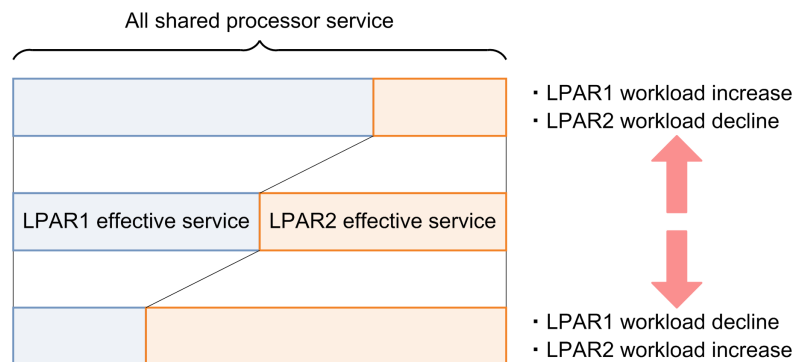


Figure 5-1 Workload of LPARs

Detecting an idle state

Configure settings so that the idle state of a processor can be detected.

1. Use the OS console to connect to the LPAR manager screen and then open the **Logical Partition Configuration** screen.
2. Move the cursor to the **ID** column of the row of the LPAR whose idle state is to be detected, and then press the **Enter** key.

The **Processor Idle Detection** sub-screen appears.

3. Select Yes.

Related topics

- [Logical Partition Configuration screen on page 10-8](#)

Setting up processor capping

What is processor capping?

For the LPARs in shared mode, processor capping suppresses processor usage within the assigned allocation rate regardless of the LPAR's busy state.

The LPARs for which processor capping is enabled do not request processor usage that is more than the allocation rate even if they require more processors (busy state).

Even if processor capping is set, a maximum of 1% of the allocation rate might be exceeded, because the service ratio control allows a tolerance of 1%.

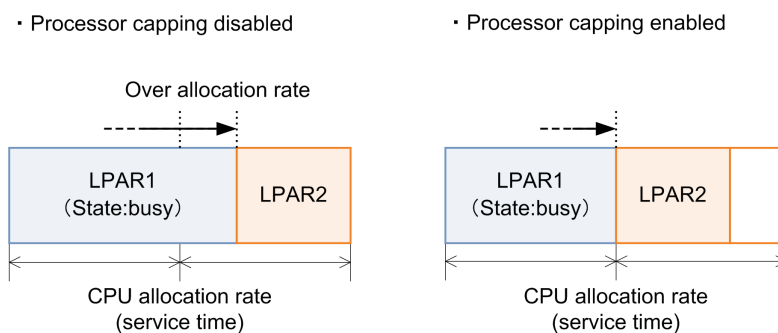


Figure 5-2 Example when processor capping is applied

Setting up processor capping

1. Use the OS console to connect to the LPAR manager screen and then open the **Logical Partition Configuration** screen.
2. Move the cursor to the **PC** column of the row of the LPAR to which processor capping is to be set, and then press the **Enter** key. The **Processor Capping** sub-screen appears.
3. Select Yes.

Related topics

- [Logical Partition Configuration screen on page 10-8](#)

Setting up a processor group

What is a processor group?

You can reduce the effect of load fluctuations by defining processors as groups and then assigning the group to LPARs that share the processors.

In addition, if you define a processor group for each user department that uses the LPAR, you can charge for the allocated processor performance.

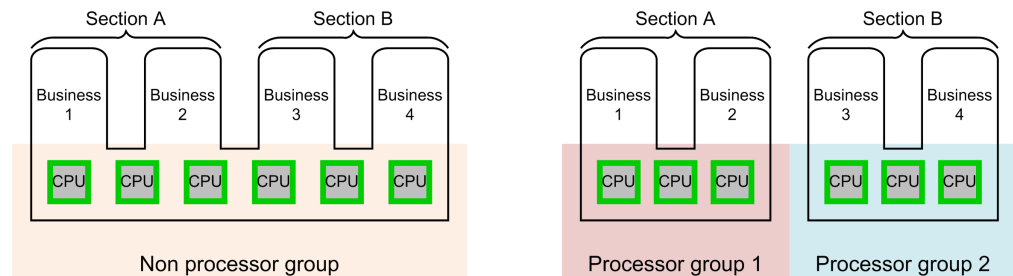


Figure 5-3 Example when a processor group is used

- When not using a processor group
You can prepare a large resource pool, and share resources among many businesses. It is difficult to ensure performance for a specific business.
- When using a processor group
You can allocate stable performance to businesses by dividing a resource pool, and you can easily predict performance for each business. In addition, if a resource pool is divided for each department, you can easily charge for resource usage.

Adding a processor group

Add a new processor group.

1. Use the OS console to connect to the LPAR manager screen and then open the **Physical Processor Configuration** screen.
2. Press the **F1** key.
The **Add Group** sub-screen appears.
3. Select a number for the processor group you want to add.

Related topics

- [Physical Processor Configuration screen on page 10-23](#)

Assigning an LPAR to a processor group

Assign an LPAR to a processor group.

1. Use the OS console to connect to the LPAR manager screen and then open the **Logical Partition Configuration** screen.

2. Move the cursor to the **Grp** column of the row of the LPAR to which a processor group is to be assigned, and then press the **Enter** key.
A sub-screen appears.
3. Specify the number of the processor group to which the LPAR is to be assigned.

Related topics

- [Logical Partition Configuration screen on page 10-8](#)

Assigning a physical processor to a processor group

Assign a physical processor to a processor group and configures a processor group.

1. Use the OS console to connect to the LPAR manager screen and then open the **Physical Processor Configuration** screen.
2. Select the target processor, move the cursor to the Group# column under the **Physical Processor Configuration** screen, and then press the **Enter** key.
The **Group Number Assignment** sub-screen appears.
3. Select the number of the processor group to which the physical processor is to be assigned.

Related topics

- [Physical Processor Configuration screen on page 10-23](#)

Setting a name for a processor group

Set a name for a processor group.

1. Use the OS console to connect to the LPAR manager screen and then open the **Physical Processor Configuration** screen.
2. Select the target processor group, move the cursor to the Name column, and then press the **Enter** key.
The **Group Name** sub-screen appears.
3. Specify a processor group name.

Related topics

- [Physical Processor Configuration screen on page 10-23](#)

Deleting a processor group

Delete an existing processor group. Note, however, that you cannot delete processor group 0.

1. Use the OS console to connect to the LPAR manager screen and then open the **Physical Processor Configuration** screen.
2. Press the **F2** key.
The **Remove Group** sub-screen appears.
3. Select the number of the processor group you want to delete.

Related topics

- [Physical Processor Configuration screen on page 10-23](#)

Performance tuning options

Performance tuning options are functions that are used to create a system that can process large amounts of data effectively. Performance tuning options are set for individual LPAR manager systems. You cannot set Performance tuning options for individual LPARs. Note that the settings of the processors, NICs, and FCs to be allocated to LPARs must be in dedicated mode. In addition, allocate memory to LPARs in units of 1GB.

System requirements

The following table describes the system requirements for using performance tuning options.

Table 5-2 System requirements for using performance tuning options

Category		Support condition		
		CB 520X B2	CB 520X B3	CB 520H B4
Management module firmware		A0135 or later	A0155 or later	A0160 or later
LPAR manager firmware		02-27 or later	02-46 or later	02-50 or later
LPAR manager model		Enterprise model	Enterprise model	Enterprise model
Guest OS ¹	Windows	Not supported	Not supported	Not supported
	Red Hat Enterprise Linux	Not supported	Not supported	Supported
Notes: 1. If the performance tuning options are enabled, only guest OSs that support the performance tuning options can be created as the guest OSs of LPARs running on the LPAR manager. Therefore, guest OSs that support the performance tuning options and guest OSs that do not support the performance tuning options cannot be mixed as guest OSs of LPARs.				

The following table lists the PCI devices supported for the performance tuning options.

Table 5-3 PCI devices supported for the performance tuning options

PCI device		Support specification		
		Dedicated	Shared	Exclusively shared
NIC	10GBASE-SR 2-port LAN adapter	Y	Y ¹	N
FC	Hitachi 16Gb 2-port fibre channel adapter	Y	Y	N
Legend: Y: Can be used N: Cannot be used Notes: 1. VF NICs are supported.				

How the set values change due to the application of Performance tuning options

The set values are changed if Performance tuning options are applied. The following table describes how the set values change.

Table 5-4 How the set values change due to the application of Performance tuning options

Function		Support specification	
		Performance tuning option	
		Disabled	Enabled
Resource allocation	Processor allocation	Dedicated/Shared	Dedicated
	NIC allocation	Dedicated/Shared/VF	Dedicated [02-2x or earlier] Dedicated/VF [02-40 or later]
	Dedicated port functionality	Supported	Not supported
	FC allocation	Dedicated/Shared	Dedicated [02-2x or earlier] Dedicated/Shared [02-40 or later]
	FCoE allocation	Dedicated	Not supported
	L3 cache allocation	Not supported	Supported
Logical processor settings	Idle Detection ¹	Y/N	N
	Guest Idle Mode ³	HALT	MWAIT ²

Function		Support specification	
		Performance tuning option	
		Disabled	Enabled
	Low Latency ³	N	Y
	EPT 1GB ³	N	Y
LPAR migration	Shutdown	Supported	Not supported
	Concurrent maintenance	Supported	Not supported
N+M cold standby		Supported	Not supported
Notes: 1. If Y is set for Idle Detect, the Guest Idle Mode is fixed to HALT. 2. To set Guest Idle Mode to MWAIT, the processor allocation setting must be dedicated, and the Idle Detect setting must be N. If MWAIT is set for Guest Idle Mode, changes to processor allocation and Idle Detect settings are restricted. 3. The setting can be referenced by using the HvmSh command only.			

Related topics

- [Changing scheduling mode of a physical NIC to dedicated mode or shared mode for a port on page 6-4](#)
- [Performing an FCoE boot by enabling the FCoE functionality on page 6-4](#)
- [Applying the L3 cache allocation functionality on page 5-19](#)

Notes

Note the following when using Performance tuning options:

- If Performance tuning options are enabled, the LPAR settings that can be activated are limited as shown below. Do not use combinations other than those described in the following table when you specify the settings.

Table 5-5 Combinations of available LPAR settings if Performance tuning options are enabled

Processor	Idle Detect	Guest Idle Mode	Low Latency
Dedicated	Y	HALT	N
	N	HALT	N
		MWAIT	Y
		MWAIT	N
Shared	Y	HALT	N

Processor	Idle Detect	Guest Idle Mode	Low Latency
	N	HALT	N

- To downgrade the version of the LPAR manager firmware, management module firmware, etc, to the previous version, disable Performance tuning options in advance.

Enabling Performance tuning options

Use the Web console to enable Performance tuning options. Make sure that you power off the server blade on which LPAR manager runs in advance.

Using the Web console to enable Performance tuning options

1. From the global task bar of the Web console, select the **Resources** tab. In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the target server blade. In the application area, the **Server Blades x** view is displayed. A unique number that identifies the server blade is displayed for x.
3. In the **Server Blades x** view, select the **LPAR Manager** tab, and then from the **Edit** menu, select **System Settings**. The **System Settings** dialog box appears.
4. In **Performance tuning options**, select **Enable**.

Enabling hyper-threading

Features of processors for which hyper-threading is enabled

If you enable the processor functionality hyper-threading, the number of physical processors assigned to an LPAR is twice the number of cores.

- Use the server blade UEFI to enable or disable hyper-threading.
- To ensure the performance of processors, be sure to assign physical processors on the same core to the same LPAR. If you assign processors on the same core to different LPARs, the load on one LPAR affects the processing performance of the other LPARs.
- You can check information about physical processors (such as core information) in the Physical Processor Configuration screen.



Note:

- If you enable the core scheduling and assign physical processors on the same core to different LPARs, the LPARs can not be activated.
-

Related topics

- [What is a core scheduling? on page 5-11](#)

- [Logical Partition Configuration screen on page 10-8](#)
- [Physical Processor Configuration screen on page 10-23](#)
- Manual *Hitachi Compute Blade 2500 Series UEFI Setup Guide*

Checking the core information of physical processors

Check the core information of physical processors.

1. Use the OS console to connect to the LPAR manager screen and then open the **Physical Processor Configuration** screen.
2. Check the information displayed for the columns Socket#, Core#, and Thread#.

If the numbers in the columns Socket# and Core# match the numbers in the Thread# columns, this indicates that the physical processors are on the same core.

Related topics

- [Physical Processor Configuration screen on page 10-23](#)
- Manual *Hitachi Compute Blade 2500 Series UEFI Setup Guide*

What is a core scheduling?

The core scheduling is a function to suppress running multiple LPARs within a physical core when hyper-threading is enabled.

This function is disabled by default. To enable this, use the HVM management command (HvmSh). For details, see the manual *HVM Management Command (HvmSh) Operation Guide*.

The following conditions must be met. The LPARs do not meet them can not be activated, and the processor do not meet them can not be switched the processor scheduling mode dynamically.

- Assign even number of logical processors to every LPAR.
- When specifying physical processor numbers, assign both threads within a processor core to the same LPAR.
- When applying NUMA and binding physical NUMA node to an LPAR, set even number of logical processors to every NUMA node in the LPAR.



Note:

- Enabling the core scheduling may cause following impact on the LPARs in shared mode.
Performance evaluation is recommended before using this function.
 - If the processor utilization differs for each logical processor on an LPAR, there is a difference in the used time between the two threads within a processor core. In core scheduling, an idle thread can not be allocated to other LPARs while the other thread is used. This may decrease the time the LPARs use threads, and degrade performance.
-

The following figure shows scheduling example of executing the same tasks when the core scheduling is disabled or enabled.

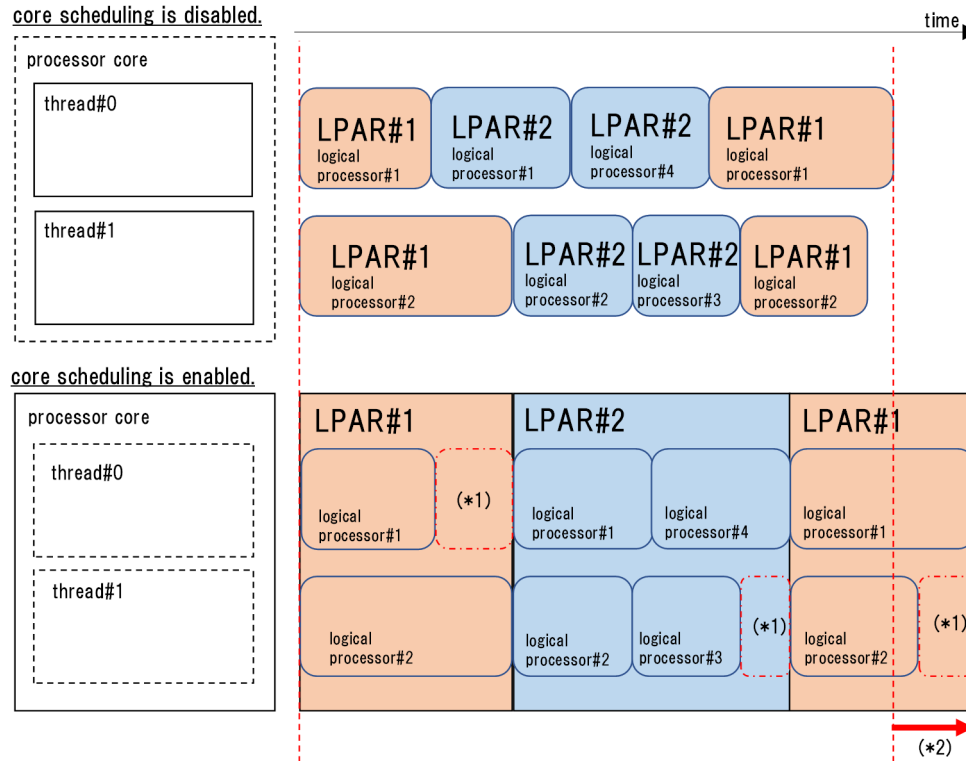


Figure 5-4 Scheduling example when core scheduling is disabled / enabled

Notes of Figure:

(*1) The period while the thread can not be allocated to another LPAR.

(*2) Delay time of completion compared to when the core scheduling is disabled.

Related topics

- Manual *HVM Management Command (HvmSh) Operation Guide*

Enabling the PRTE function

The PRTE function provides a timer that can be referred without intervention of the LPAR manager.

We recommend that you basically set the PRTE function to "No": a default value.

Enabling the PRTE function may bring performance improvement of programs that frequently retrieve time, in Windows.



Note:

- Enabling this function brings guest OS operation different from that with this function disabled. When you enable or disable the PRTE function, we recommend that you evaluate guest OS behavior in advance.
-

Restriction

The following shows restrictions for this function.

- Do not assign more than 64 of logical processors to an LPAR with its PRTE function enabled.
- Do not use the NIC teaming functionality an LPAR with its PRTE function enabled.

Supported OS

The following OSs support the PRTE function.

Make sure not to set the PRTE function to "Yes" for other OSs.

- Windows Server 2012
- Windows Server 2012 R2

To enable the PRTE function from the LPAR manager screen:

You are able to change the setting of the PRTE function only for deactivated LPARs.

The method of setting the PRTE function is as follows.

1. Use the OS console to connect to the LPAR manager screen, and then display the **Logical Partition Configuration** screen.
2. Use the **F11** or **F12** key to scroll the page horizontally, position the cursor at the **PRTE** column on the **LPAR** row, and then press the **Enter** key.
The **Setting PRTE** sub-screen appears.
3. Select **Yes**, and then press the **Enter** key.

Enabling the PRTE function with HvmSh

Execute the `set LPARMshyp` command of the HVM management command (HvmSh) to enable the PRTE function.

Related topics

- [Logical Partition Configuration screen on page 10-8](#)

Applying NUMA to an LPAR

Applying NUMA

NUMA is the processor functionality that improves memory access and memory bandwidth. We recommend that you operate LPARs on server blades for which NUMA is enabled, because NUMA can improve performance easily.

- To apply a NUMA configuration to the LPAR, you need to specify UEFI settings on the server-blade side and settings on the LPAR side.
For details about the UEFI settings on the server-blade side, see the manual *Hitachi Compute Blade 2500 Series UEFI Setup Guide*. You can specify the settings on the LPAR side by using the Logical Partition Configuration screen.
- If you configure NUMA on the server-blade side UEFI but not configured on the LPAR side, you cannot activate an LPAR in the following conditions:
 - Automatic allocation is used to allocate memory to the LPAR, and the total amount of available memory on all nodes is less than the amount of memory required for the LPAR.
 - Manual allocation is used to allocate memory to the LPAR, and the amount of available memory on the specified node is less than the amount of memory required for the LPAR.

Setting a logical processor for NUMA

The LPAR manager supports the following two logical processor assignment methods in NUMA configurations:

- Binding physical processors (02-0X and later)
This method maps logical processors to physical processors.
Set the number of logical processors for the entire LPAR. To map logical processors to physical processors, the user manually assigns processors by specifying physical processor numbers before activating the LPAR.
- Binding physical NUMA nodes (02-40 and later)
This method maps logical processors to physical NUMA nodes.
Set the number of logical processors for each NUMA node. To map logical processors to physical processors, LPAR manager automatically assigns processors when the LPAR is activated. For the unassigned physical processors in the NUMA node, the physical processor with the smallest processor number is assigned first.



Note:

- When NUMA is enabled, the default method for setting logical processors is binding physical processors.
As a result, when NUMA is disabled and then enabled for an LPAR, even if the LPAR specifies a method to set logical processors for NUMA, logical processors are mapped to physical processors.

- For LPARs for which NUMA is enabled and logical processors are bound to physical NUMA nodes, you cannot use the Logical Partition Configuration screen to set the number of logical processors.

To set the number of logical processors per node, use the HVM management command (HvmSh). For details, see the manual *HVM Management Command (HvmSh) Operation Guide*.

- For an LPAR for which the method for configuring logical processors for the LPAR is physical processor binding, when this configuration method is changed to physical NUMA node binding, all configuration information for the LPAR changes to "Auto".

If you change the method used to set logical processors back to binding physical processors, or if you disable NUMA for the LPAR, you must save the configuration information again.

- For LPARs for which NUMA is enabled and logical processors are bound to physical NUMA nodes, physical processors cannot be assigned to logical processors.

Related topics

- [Saving the LPAR manager configuration on page 3-13](#)
- [Logical Partition Configuration screen on page 10-8](#)
- [Logical Processor Configuration screen on page 10-20](#)
- Manual *Hitachi Compute Blade 2500 Series UEFI Setup Guide*
- Manual *HVM Management Command (HvmSh) Operation Guide*

Enabling NUMA for an LPAR

Configure settings so that the LPAR runs in a NUMA configuration

1. Enable NUMA by using the UEFI for the server blade on which the LPAR is running.
2. Confirm that the version of the LPAR manager firmware matches the method to be used to set logical processors for NUMA.
When LPAR manager firmware version is 02-2x earlier, always set to bind physical processors. you can not change the method for setting logical processors, following steps.
To bind physical processors, the LPAR manager firmware version must be 02-0X or later.
To bind physical NUMA nodes, the LPAR manager firmware version must be 02-40 or later.
3. Deactivate the target LPAR.
4. In the **Logical Partition Configuration** screen, set a NUMA configuration for the LPAR.
5. Select the method used to set logical processors.
Use the HVM management command (HvmSh) to select the method used to set logical processors. For details, see the manual *HVM Management Command (HvmSh) Operation Guide*.

6. In the **Logical Partition Configuration** screen, set the processor scheduling mode to dedicated mode.
7. Set the number of processors.
 - To bind physical processors, use the **Logical Processor Configuration** screen.
 - To bind physical NUMA nodes, use the HVM management command (HvmSh).
For details, see the manual *HVM Management Command (HvmSh) Operation Guide*.
8. Assign processors to the LPAR.
This step is required to bind physical processors. In the **Logical Processor Configuration** screen, specify settings.
9. In the **Logical Partition Configuration** screen, allocate memory to the processors.

The following are explanations of the configuration procedures that use the LPAR manager screen from the workflow above:

Setting a NUMA configuration for the LPAR

1. Use the OS console to connect to the LPAR manager screen, and then display the **Logical Partition Configuration** screen.
2. Scroll through the **Logical Partition Configuration** screen to display the **NUMA** column.
3. Move the cursor to the **NUMA** column of the row for the LPAR for which you want to enable NUMA, and then press the **Enter** key.
The **Setting NUMA** sub-screen appears.
4. Specify **Yes**.
The **Setting NUMA** sub-screen is closed.

Setting the processor scheduling mode

1. Use the OS console to connect to the LPAR manager screen, and then display the **Logical Partition Configuration** screen.
2. Scroll through the **Logical Partition Configuration** screen to display the **Scd** column.
3. Move the cursor to the **Scd** column of the row for the LPAR for which you want to set the scheduling mode, and then press the **Enter** key.
The **Logical Processors Scheduling mode Assignment** sub-screen appears.
4. Specify **D**.
The **Logical Processors Scheduling mode Assignment** sub-screen is closed.

Setting the number of processors

1. Use the OS console to connect to the LPAR manager screen, and then display the **Logical Partition Configuration** screen.

2. Scroll through the **Logical Partition Configuration** screen to display the **Pro** column.
3. Move the cursor to the **Pro** column of the row for the LPAR for which you want to set the number of processors, and then press the **Enter** key.
The **The number of Logical Processors** sub-screen appears.
4. Specify the number of processors that you want to assign.
If you assign physical processors from multiple NUMA nodes, make sure that the number of physical processors to be assigned is the same among NUMA nodes.
The **The number of Logical Processors** sub-screen is closed.

Assigning processors to the LPAR

1. Use the OS console to connect to the LPAR manager screen, and then display the **Logical Processor Configuration** screen.
2. Move the cursor to the **Logical Processor Number** column of the row for the LPAR to which you want to assign processors, and then press the **Enter** key.
In addition, scroll through the **Logical Partition Configuration** screen to display the target **Logical Processor Number** column.
The **The number of Logical Processors** sub-screen appears.
3. Specify the numbers of the physical processors that you want to assign.
The **The number of Logical Processors** sub-screen is closed.

Allocating memory to the LPAR

1. Use the OS console to connect to the LPAR manager screen, and then display the **Logical Partition Configuration** screen.
2. Scroll through the **Logical Partition Configuration** screen to display the **Mem** column.
3. Move the cursor to the **Mem** column for the target LPAR, and then press the **Enter** key.
The **NUMA Mem Allocation** sub-screen appears.
4. Move the cursor to the node of the memory that you want to allocate, and then press the **Enter** key.
5. Use the arrow keys to specify the size of the memory that you want to allocate, and then press the **Enter** key.
The **NUMA Mem Allocation** sub-screen is closed.

Related topics

- [Displaying the LPAR manager screen and the guest screen on page 8-8](#)
- [Logical Partition Configuration screen on page 10-8](#)
- *Manual HVM Management Command (HvmSh) Operation Guide*

Specifying a memory node

This section describes logical partitioning of memory.

Automatic memory allocation and specification of a node

There are two types of memory allocation: Automatic memory allocation in which the node of the physical processor is considered, and memory allocation by a specified memory node in which the user manually allocates memory. Memory allocation by a specified memory node allocates physical memory from one node manually specified by the user.

The following table describes the operations of automatic memory allocation and memory allocation by a specified memory node.

Table 5-6 Memory allocation and its operation

Memory allocation	Operation
Automatic memory allocation	<ul style="list-style-type: none">• If the activating LPAR is in dedicated mode, LPAR manager allocates to the LPAR the memory in the node to which the assigned processor belongs. If the activating LPAR is in shared mode and the processor group is configured, LPAR manager allocates to the LPAR the memory in the node included in the processor group to which the LPAR belongs. If the activating LPAR is in shared mode and no processor group is configured, LPAR manager allocates to the LPAR the memory in a node included in any processors.• LPAR manager preferentially allocates to the LPAR the available physical memory that belongs to the same node as the physical processor assigned to the LPAR.• If the amount of available physical memory in the same node is less than the required amount, LPAR manager allocates memory to make up the shortage from another node. LPAR manager determines from which node the memory is allocated. <p>If the total amount of available memory in all nodes is less than the amount of required memory, LPAR activation will fail.</p>
Memory allocation by a specified memory node (manual allocation)	<ul style="list-style-type: none">• LPAR manager allocates to the LPAR the free physical memory in the node specified by the user. <p>If the amount of available physical memory in the specified node is less than the required amount, LPAR manager does not search another node and LPAR activation will fail.</p>



Tip:

- When an LPAR is activated, the physical memory to be allocated to the LPAR is determined. You cannot allocate different amount of physical memory after the LPAR is activated.
- If a NUMA configuration is applied, you cannot perform memory allocation by memory node specification.

Related topics

- [Logical Partition Configuration screen on page 10-8](#)

Setting a memory allocation type for an LPAR

Select the memory allocation type for the memory to be allocated to the LPAR: automatic memory allocation or memory allocation by memory node specification.

1. Use the OS console to connect to the LPAR manager screen and then open the **Logical Partition Configuration** screen.
2. Move the cursor to the **MN** column of the row of the LPAR for which a memory allocation type is to be set, and then press the **Enter** key.
The **Setting 'A' or NUMA Memory Node Number** sub-screen appears.
3. Enter **A** or a numerical value.
If you want to enable automatic memory allocation, specify A. If you want to enable memory allocation by memory node specification, enter the number of the node.

Related topics

- [Logical Partition Configuration screen on page 10-8](#)

Applying the L3 cache allocation functionality

What is the L3 cache allocation functionality?

You can use the L3 cache allocation functionality to divide the L3 cache among multiple LPARs and allocate part of the divided cache to each LPAR. This functionality uses Cache Allocation Technology (CAT), which is provided as part of Intel Resource Director Technology (RDT).

If, for example, you operate an LPAR that requires response performance (web server) and an LPAR that puts a high load on the memory (database) at the same time, data of the LPAR (web server) might be forced out from the L3 cache, and degradation or variance in response performance might occur. You can prevent such degradation or variance in response performance by using the L3 cache allocation functionality to secure the L3 cache space required for the LPAR (web server).

By default, the entire L3 cache is allocated to each LPAR, but you can dynamically change the size of the L3 cache space that is allocated to each LPAR. Note, however, that you can change the L3 cache allocation only for LPARs to which processors have been allocated in dedicated mode.

You can allocate L3 cache space to LPARs by using the capacity bit mask (CBM) format (a mask value format). By using a CBM, you can specify not only the size of the L3 cache space to be allocated to LPARs, but also detailed settings such as the distance and overlapping of L3 cache allocation among LPARs. Each specified CBM value must be in the range of the implemented bit

width of the CBM and must be a combination of consecutive ones (1). For example, if the implemented bit width of the CBM is 20, FFFFFh, 0FF00h, and 0003Ch are acceptable, but values such as 10001h, 00100h, and 0F0F0h are not acceptable. As shown below, there are three possible combinations of CBMs for multiple LPARs. In the following figure, the implemented bit width of CBMs is 8.

(1) Default bit mask

	M7	M6	M5	M4	M3	M2	M1	M0
LPAR1	A	A	A	A	A	A	A	A
LPAR2	A	A	A	A	A	A	A	A
LPAR3	A	A	A	A	A	A	A	A

(2) Duplicated bit mask

	M7	M6	M5	M4	M3	M2	M1	M0
LPAR1	A	A	A	A	A	A	A	A
LPAR2					A	A	A	A
LPAR3							A	A

(3) Isolated bit mask

	M7	M6	M5	M4	M3	M2	M1	M0
LPAR1	A	A	A					
LPAR2				A	A	A		
LPAR3							A	A

Figure 5-5 Example when a processor group is used

In the case indicated by (1), all three LPARs can access the entire L3 cache. In the case indicated by (2), the L3 cache space allocated to the LPAR of lower priority can be shared with the LPAR of higher priority. In the case indicated by (3), the cache can be divided among isolated LPARs.

To allocate L3 cache space to LPARs, use the HVM management command (HvmSh). You can also use the HVM management command (HvmSh) to display the CAT-related configuration information required to use the L3 cache allocation functionality, and the usage status of the L3 cache allocation functionality. For details, see the manual *HVM Management Command (HvmSh) Operation Guide*.

Enabling the L3 cache allocation functionality

To enable the L3 cache allocation functionality:

1. From the Web console, enable Performance tuning options.
2. Specify the L3 cache allocation settings by using the HVM management command (HvmSh), execute the `opr LparCatCbm` command.

Related topics

- [Performance tuning options on page 5-7](#)

- Manual *HVM Management Command (HvmSh) Operation Guide*

Setting the Functionality for PCI Devices

This chapter describes the functionality that can be set for the PCI devices that are assigned to LPARs, and describes how to set up the functionality.

- ☐ [Enabling the SR-IOV functionality and using VF NICs](#)
- ☐ [Performing an FCoE boot by enabling the FCoE functionality](#)
- ☐ [Creating more segments than there are physical NICs](#)
- ☐ [Changing scheduling mode of a physical NIC to dedicated mode or shared mode for a port](#)
- ☐ [VLAN functionality using shared and virtual NICs](#)
- ☐ [Using inter-LPAR communication](#)
- ☐ [Using teaming functionality to build redundancy into the NIC configuration](#)
- ☐ [Monitoring data by using promiscuous mode](#)
- ☐ [Maintaining the I/O performance by using the HBA dedicated core mode of shared FCs](#)
- ☐ [Using N+M cold standby \(LUID mode\) to start LPARs](#)

Enabling the SR-IOV functionality and using VF NICs

To use SR-IOV, which is a hardware functionality of a physical NIC, use VF NICs. This section describes how to use VF NICs.

1. If the SR-IOV functionality of Emulex 10Gb NICs is used, you need to enable the SR-IOV functionality according to the manual *Hitachi Compute Blade Emulex Adapter User's Guide for Hardware*. Note that in LP mode you cannot set up SR-IOV. Change to Basic mode before setting up SR-IOV.

If the SR-IOV functionality of 10GBASE-SR 2-port LAN adapters is used, you do not need to enable the SR-IOV functionality because it is always enabled.

2. Set the shared mode.
Set the NIC scheduling mode to the shared mode on the **PCI Device Assignment** screen of the LPAR manager screen.
3. Configure VF NICs.
Set the following information on the **Virtual NIC Assignment** screen.
 - VF NIC (such as 1av) assignment (mandatory)
 - Transmission band limitation settings (optional)

Related topics

- [PCI Device Assignment screen on page 10-30](#)
- [Virtual NIC Assignment screen on page 10-34](#)
- [SR-IOV functionality supported by LPAR manager on page B-12](#)
- Manual *Hitachi Compute Blade Emulex Adapter User's Guide for Hardware*
- Manual *Hitachi Compute Blade Emulex Adapter User's Guide for Driver*

Notes on using the SR-IOV functionality

Note the following when using the SR-IOV functionality:

- Notes on using Emulex adapters in a Windows environment
In a Windows environment, you cannot use LPARs to which both a dedicated NIC and a VF-NIC are allocated.
- Notes on using teaming interfaces for Windows
Note the following when configuring a teaming interface with VF NIC ports.
 - When you configure a teaming interface, you need to specify the MAC address originally set for one of the VF NIC ports to be set in the same team, for all of the VF NIC ports.
Also, when you remove a teaming interface, reset the original MAC address for each VF NIC port.
 - If HCSM detects duplication of a MAC address, HCSM does not allow you to migrate the LPARs on an LPAR manager.

- HVM Navigator does not allow you to set a MAC address for multiple VF NIC ports.

For the method for configuring a teaming interface and that for removing a teaming interface, see the following.

Configuring a teaming interface

- Boot a guest OS to which VF NIC ports assigned, with the original MAC address set for each of the VF NIC ports to be set in a team.
Note that, when you remove a teaming interface, you need to reset the original MAC address for each of the VF NIC ports. We recommend that you take a note of the original MAC addresses.
- Confirm that each VF NIC port can communicate by issuing the `ping` command.
- Shut down the guest OS.
- Push **F6** on the **Virtual NIC Assignment** screen. Then, specify the MAC address originally set for one of the VF NIC ports, for all of the VF NIC ports.
For example, to configure a team with VNIC#0 and VNIC#1, specify the MAC address of VNIC#0 for VNIC#1.
- Boot the guest OS.
- Confirm that the same MAC address is set for all of the VF NIC ports to be set in a team.
For confirming a MAC address, select [Start]-[Control Panel]-[Network and Internet]-[Network and Sharing Center]-[Change adapter settings], and then double-click a network device. In the opened dialog, push [Details], and then see the value of "Physical Address".
- Configure a teaming interface with the VF NIC ports.
- Configure the driver option for the teaming interface, and then confirm operation of the teaming interface.

Removing a teaming interface.

- Remove a teaming interface on a guest OS.
 - Shut down the guest OS.
 - Push **F6** on the **Virtual NIC Assignment** screen. Then, reset the original MAC address for each of the VF NIC ports in the team.
 - Boot the guest OS.
- Notes on using Emulex adapters in a Linux environment
When VF NICs of Emulex 10Gb 2-port converged network adapter are assigned and RHEL7.1 or RHEL7.2 is booted as a guest OS, the following message might be output. However, operation of the guest OS is not affected.
`be2net 0000:XX:XX.X: VF is not privileged to issue opcode 125-1`
`XX:XX.X : Bus:Dev.Func`

Performing an FCoE boot by enabling the FCoE functionality



Note:

- The FCoE functionality is supported only by onboard LANs (Onboard LAN).
- If the FCoE functionality is enabled, the SR-IOV functionality is disabled on LPAR manager.
- When you activate an LPAR in FCoE boot, the OS boot process may not be performed after the UEFI screen is displayed.
In this case, reactivate the LPAR to boot the OS.

To perform an FCoE boot, which is hardware functionality of a physical NIC, enable "FCoE".

1. Enable the FCoE functionality, and then specify the FCoE functionality settings.
For details, see the manual *Hitachi Compute Blade Emulex Adapter User's Guide for Hardware*.
2. Set dedicated mode.
Set the NIC scheduling mode to dedicated mode in the **PCI Device Assignment** screen of the LPAR manager screen.
3. Assign a dedicated NIC.
Assign a dedicated NIC to an LPAR in the **PCI Device Assignment** screen of the LPAR manager screen.

Related topics

- [PCI Device Assignment screen on page 10-30](#)
- Manual *Hitachi Compute Blade Emulex Adapter User's Guide for Hardware*
- Manual *Hitachi Compute Blade Emulex Adapter User's Guide for Driver*

Creating more segments than there are physical NICs

By assigning the same physical NIC port to more than one LPAR, you can create more segments than there are physical NICs.

Related topics

- [Virtual NIC Assignment screen on page 10-34](#)

Changing scheduling mode of a physical NIC to dedicated mode or shared mode for a port

To change scheduling mode of a physical NIC to dedicated mode or shared mode for a port, the dedicated port functionality must be enabled.

Dedicated port functionality

Using the dedicated port functionality enables a PCI device to be dedicated to an LPAR for a port. If the dedicated port functionality is enabled for a PCI device, that PCI device is regarded as an independent PCI device for each port, and you can set scheduling mode (dedicated mode or shared mode) for each port.

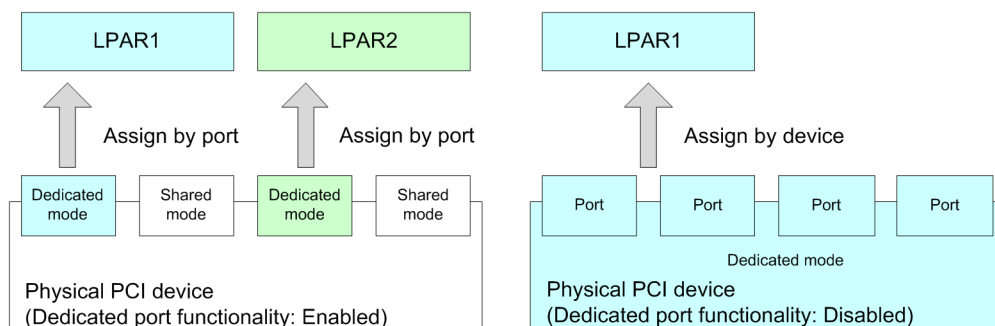


Figure 6-1 Example of assigning ports in dedicated mode

Support requirements for the dedicated port functionality

For details about support requirements, see [Dedicated port functionality supported by LPAR manager on page B-19](#).

Related topics

- [Dedicated port functionality supported by LPAR manager on page B-19](#)

Enabling the dedicated port functionality

The following procedure describes how to enable the dedicated port functionality:

1. Use the HvmSh command to enable the dedicated port functionality for the target PCI device.
2. Open the **PCI Device Assignment** screen. All the ports of the target PCI device are displayed.
3. In the **PCI Device Assignment** screen, set scheduling mode of the target port to dedicated mode, and then assign the port to an LPAR.
4. In the **System Service State** screen, perform the Force Recovery operation.
5. Save the LPAR manager configuration information.

Related topics

- [PCI Device Assignment screen on page 10-30](#)
- [System Service State screen on page 10-58](#)

Disabling the dedicated port functionality

The following procedure describes how to disable the dedicated port functionality:

1. Shut down the guest OS on the LPAR to which a port dedicated NIC is assigned.
2. In the **PCI Device Assignment** screen, set scheduling mode of all the ports of the target PCI device to either shared mode or dedicated mode, and then press the **F10**key.
3. Use the HvmSh command to disable the dedicated port functionality for the target PCI device. This clears the entire port assignment information. An error occurs if the same scheduling mode is not set for all the ports of the target PCI device.
In the **System Service State** screen, perform the Force Recovery operation.
4. Save the LPAR manager configuration information.

Related topics

- [PCI Device Assignment screen on page 10-30](#)
- [System Service State screen on page 10-58](#)

Notes on the dedicated port functionality

Note the following when using the dedicated port functionality:

- LPAR migration of an LPAR to which a port dedicated NIC is assigned cannot be performed.
- When you downgrade an LPAR manager to a version not supporting the dedicated port functionality, disable the dedicated port functionality in advance.
- If a port dedicated NIC is assigned, in addition to the assigned port, a dummy device will be generated on the LPARs to which a port other than port 0 is assigned, and the following device will be recognized by each OS:

For Windows: Intel(R) 82599 Multi-Function Network Device

For Linux: Intel Corporation 82599EB 10-Gigabit Dummy Function

The above devices are not used, and you do not need to assign a driver.

VLAN functionality using shared and virtual NICs

In LPAR manager, you can use the VLAN functionality that complies with IEEE802.1Q.

- You can create multiple broadcast domains using a single physical NIC.
- You can use IEEE 802.1Q-format tags as the interface to an external switch.

VLAN functionality

LPAR manager supports three types of VLAN modes for the VLAN functionality. The VLAN mode can be specified for each logical NIC.

Undef

Neither the guest OS nor LPAR manager uses VLAN tags. The untagged frames sent by the guest OS are transferred as they are.

Untagged

Only LPAR manager adds or removes VLAN tags. Only the frames that include any of the specified VLAN IDs can be received. Only untagged frames can be sent.

Tagged

Only the guest OS adds or removes VLAN tags. The guest OS can use VLAN tags within the range specified for a logical NIC. You can set a maximum of 16 VLAN IDs for one logical NIC. If you want to use 17 or more VLAN IDs, specify ALL, which allows the NIC to receive all VLAN IDs.

Table 6-1 VLAN mode

VLAN mode	Adds or removes VLAN tags	Sending frames	Receiving frames	Specifiable VLAN IDs
Undef	(VLAN is not used)	Untagged	Untagged	--
Tagged	Only guest OS	Untagged or tagged (VLAN ID within the specified range)	Untagged or tagged (VLAN ID within the specified range)	A maximum of 16 decimal IDs within the range from 1 to 4094. Alternatively, all VLAN IDs.
Untagged	Only LPAR manager	Untagged	Tagged (specified VLAN ID)	A single VLAN ID within the range from 1 to 4094.
Legend: --: None				

VLAN handling

- Sending frames
A frame is sent when VLAN mode and VLAN ID of the frame match those of the port.
The following table describes how frames are filtered.

Table 6-2 Filtering sending frames

VLAN mode of sending port	Sending frame		
	Untagged	Tagged (matches VLAN ID)	Tagged (does not match VLAN ID)
Undef	Sent	Discarded	Discarded
Tagged	Sent	Sent	Discarded
Untagged	Sent (tag added)	Discarded	Discarded

- Receiving frames

A frame is received when a destination port is found in the MAC address table of ports whose VLAN mode and VLAN ID match those of the frame. The following table describes how received frames are filtered.

Table 6-3 Filtering received frames

VLAN mode of receiving port	Receiving frame		
	Untagged	Tagged (matches VLAN ID) ¹	Tagged (does not match VLAN ID) ¹
Undef	Received	Discarded	Discarded
Tagged	Received	Received	Discarded
Untagged	Discarded	Received (tag removed)	Discarded
Note: 1. It includes the case where the VLAN tags are added to the frames by Untagged port.			

- Dividing a virtual network into several broadcast domains at the level of individual logical NICs

On the Virtual NIC Assignment screen, specify Untagged port mode for the logical NIC and specify the VLAN ID to which it belongs. There is no need to enter VLAN settings in the guest OS because the packets received by the logical NIC will be untagged.

By this process, you can divide a virtual network into broadcast domains at the level of individual logical NICs in a way that is transparent to the guest OS.

- Assigning a logical NIC to multiple broadcast domains in the same virtual network

By assigning a VLAN to a logical NIC from the guest OS, you can use functionality equivalent to a physical NIC to manipulate tags and filter frames. On the Virtual NIC Assignment screen, specify Tagged port mode for the logical NIC, and specify all of the VLAN IDs specified for the logical NIC in the guest OS.

This makes it possible for a single logical NIC to handle multiple VLAN IDs, and belong to more than one broadcast domain.

Example of using the VLAN functionality

- When VLAN is set in the OS
On the Virtual NIC Assignment screen of LPAR manager, set Tagged mode and VLAN IDs for applicable ports.
- When sending/receiving tagged packets to/from an external LAN without setting VLAN in the OS
On the Virtual NIC Assignment screen of LPAR manager, set Untagged mode and VLAN IDs for applicable ports.
- When sending/receiving untagged packets to/from an external LAN without setting VLAN in the OS
On the Virtual NIC Assignment screen of LPAR manager, set Undef mode for applicable ports.

Virtual switch images

The following shows and describes virtual switch images.

- Image of virtual NIC switch
When one of the network segments Va to Vd is assigned to a virtual NIC, the virtual NIC is connected to a virtual NIC switch.
The following image represents an example of a 128 port layer-2 switch in a configuration with 16 LPARs and 8 virtual NICs per LPAR.
Although the number of ports of a virtual NIC switch is variable, the image shows only the ports that are connected.

- Up to four switches can be configured, corresponding to network segments Va to Vd.
- All ports are configured as virtual NIC ports.

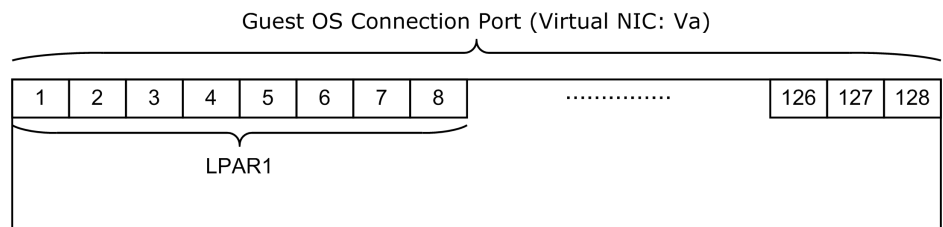


Figure 6-2 Image of virtual NIC switch

Table 6-4 List of switch functions of virtual NIC

Switch function	Affected port(s)	Settings
Port connection	Port 1 to Port 128	Assign the ports to LPARs on the Virtual NIC Assignment screen.
Port speed	Port 1 to Port 128	Auto Negotiation (this setting cannot be changed) 1000BASE-T

Switch function	Affected port(s)	Settings
VLAN	Port 1 to Port 128	<ul style="list-style-type: none"> VLAN mode Only one VLAN mode can be set per port. Undef (default) Tagged Untagged VLAN ID Tagged: Specify a maximum of 16 VLAN IDs in the range from 1 to 4094, or the All setting which permits all VLAN IDs. Untagged: Specify only one VLAN ID in the range from 1 to 4094.
Port mirroring	Port 1 to Port 128	<ul style="list-style-type: none"> If promiscuous mode is "Restricted": Only receives packets addressed to the particular LPAR (MAC address). If promiscuous mode is "Through" (default): Receives all packets in the same network segment.
Jumbo frame function	Port 1 to Port 128	Always enabled.
Uplink failover	Port 1 to Port 128	Always disabled. The ports are always linked up.
Flow control	Port 1 to Port 128	Always disabled.
IGMP Snooping	Port 1 to Port 128	Always disabled.
Spanning tree	Port 1 to Port 128	Always disabled.

- Image of shared NIC switch

When one of the network segments 1a, 1b, 2a, and so on is assigned to a shared NIC, the shared NIC is connected to a shared NIC switch.

The following image represents an example of a 17 port layer-2 switch (1 port per LPAR + physical NIC) in a configuration with 16 LPARs and 1 shared NIC per LPAR.

Although the number of ports of a shared NIC switch is variable, the image shows only the ports that are connected.

- A maximum of 16 switches can be configured, depending on the number of physical NICs set to shared mode.
 - The following image represents an example of a configuration in which Ports 1 to 16 are shared NIC ports and Port 17 is a physical NIC port.

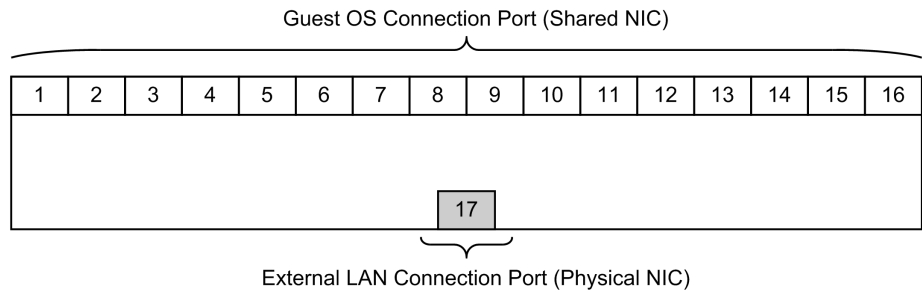


Figure 6-3 Image of shared NIC switch

Table 6-5 List of switch functions of shared NIC

Switch function	Affected port(s)	Settings
Port connection	Port 1 to Port 16	Assign the ports to LPARs on the Virtual NIC Assignment screen.
	Port 17	Physically connected via cable (no cable is required for the onboard NIC)
Port speed	Port 1 to Port 16	Auto Negotiation (this setting cannot be changed) 1000BASE-T
	Port 17	Auto Negotiation (this setting cannot be changed) 10/100/1000/10000BASE-TX
VLAN	Port 1 to Port 16	<ul style="list-style-type: none"> VLAN mode Only one VLAN mode can be set per port. If the following NIC is used as a shared NIC, there are restrictions on the VLAN modes that can be set. For Intel 10GBASE-SR 2-Port LAN adapter: <ul style="list-style-type: none"> Undef (default) Tagged (not supported) Untagged (not supported) VLAN ID Tagged: Specify a maximum of 16 VLAN IDs in the range from 1 to 4094, or the All setting which permits all VLAN IDs. Untagged: Specify only one VLAN ID in the range from 1 to 4094.
	Port 17	Tagged All (this setting cannot be changed) This setting relays all packets.
Port mirroring	Port 1 to Port 17	<ul style="list-style-type: none"> If promiscuous mode is "Restricted": Only receives packets addressed to the particular LPAR (MAC address). If promiscuous mode is "Through" (default): Receives all packets in the same network segment.

Switch function	Affected port(s)	Settings
Jumbo frame function	Port 1 to Port 17	Always enabled. Maximum value: 9000 bytes
Uplink failover	Port 1 to Port 17	Always enabled. If Port 17 is linked down, all the other ports from Port 1 to Port 16 are also linked down.
Flow control	Port 1 to Port 16	Always disabled.
	Port 17	Always enabled.
IGMP Snooping	Port 1 to Port 17	Always disabled.
Spanning tree	Port 1 to Port 17	Always disabled.

- Image of VF NIC switch

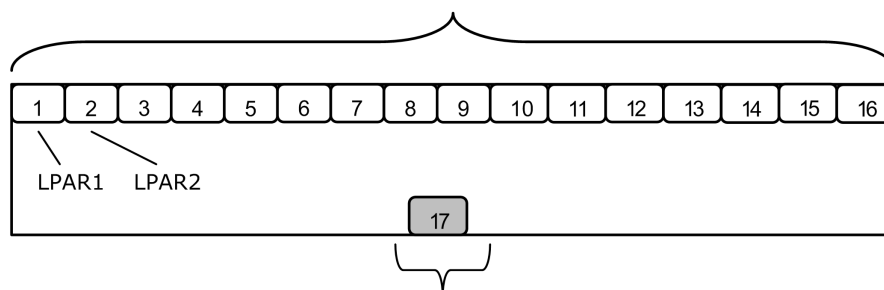
When one of the network segments 1av, 1bv, 2av, and so on is assigned to a VF NIC, the VF NIC is connected to a VF NIC switch.

The following image represents an example of a 17 port layer-2 switch (1 port per LPAR + physical NIC) in a configuration with 16 LPARs and 1 VF NIC per LPAR.

Although the number of ports of a VF NIC switch is variable, the image shows only the ports that are connected.

- A maximum of 16 switches can be configured, depending on the number of physical NICs set to shared mode.
- The following image represents an example of a configuration in which Ports 1 to 16 are VF NIC ports and Port 17 is a physical NIC port.

Guest OS connection port (VF NIC : 1av)



External LAN connection port (Physical NIC)

Figure 6-4 Image of VF NIC switch

Table 6-6 List of switch functions of VF NIC

Switch function	Affected port(s)	Settings
Port connection	Port 1 to Port 16	Assign the ports to LPARs on the Virtual NIC Assignment screen.
	Port 17	Physically connected via cable (no cable is required for the onboard NIC)
Port speed	Port 1 to Port 16	Auto Negotiation (this setting cannot be changed) <ul style="list-style-type: none"> 10GBASE-KR 1000BASE-KX
	Port 17	Auto Negotiation (this setting cannot be changed) <ul style="list-style-type: none"> 10GBASE-KR 1000BASE-KX
VLAN	Port 1 to Port 16	<ul style="list-style-type: none"> VLAN mode Only one VLAN mode can be set per port. For Emulex 10Gb 2-port converged network adapter and Onboard LAN: Undef (not supported) Tagged (default) Untagged¹ For Intel 10GBASE-SR 2-Port LAN adapter: Undef (default)² Tagged (not supported) Untagged³ VLAN ID Tagged: Specify the All setting which permits all VLAN IDs. Untagged: Specify only one VLAN ID in the range from 1 to 4094.
	Port 17	Tagged All (this setting cannot be changed) This setting relays all packets.
Port mirroring	Port 1 to Port 17	<ul style="list-style-type: none"> If promiscuous mode is "Restricted" (default): Only receives packets addressed to the particular LPAR (MAC address). Through Not supported
Jumbo frame function	Port 1 to Port 17	Always enabled. Maximum value: 9000 bytes

Switch function	Affected port(s)	Settings
Uplink failover	Port 1 to Port 17	Always enabled. If Port 17 is linked down, all the other ports from Port 1 to Port 16 are also linked down.
Flow control	Port 1 to Port 16	Always disabled.
	Port 17	Always enabled.
IGMP Snooping	Port 1 to Port 17	Always disabled.
Spanning tree	Port 1 to Port 17	Always disabled.
Note: 1. Untagged cannot be used in a VF NIC configuration where guest OSs are Red Hat Enterprise Linux 6.7/7.1/7.2. 2. Tagged packets can be sent and received. 3. When the guest OS on an LPAR is Red Hat Enterprise Linux 7.2/7.3/7.4/7.5/7.6/7.7 and is using bonding, note the following: <ul style="list-style-type: none"> Do not configure any VLAN settings for all NIC ports through NetworkManager in guest OSs. Do not configure any VLAN settings for all NIC ports with "ifcfg-eth" files in /etc/sysconfig/network-scripts in guest OSs. Register the 8021q module in the blacklist of the guest OS by adding <code>blacklist 8021q</code> to the /etc/modprobe.d/blacklist-LPAR.conf file. 		



Note:

- Logical NICs do not support advanced communication control functions (for example, IGMP snooping, access lists, and QoS). Use communication control functions of external switch modules. To control communications between LPARs on the same LPAR manager, use the VLAN function of a logical NIC or the Inter-LPAR communication packet filtering.
- Because IEEE 802.1Q tagged packets pass through external physical switches, the VLAN ID used by the virtual network corresponding to the shared physical NIC must be assigned as a Tagged port in the physical switch. Note that when you assign a VLAN in this way, communication with external networks will be slower than if a VLAN were not set.
- IEEE802.1p-format priority control is not supported.
- Keep the following considerations in mind when using the VLAN functionality for logical NICs at the same time as N+M cold standby:
LAN switch: Must be linked with Cm2/Network Element Configuration.
DCB switch: Uses the AMPP functionality of the DCB switch.

Related topics

- [Virtual NIC Assignment screen on page 10-34](#)

Using inter-LPAR communication

Inter-LPAR communication packet filtering

To ensure the independence of LPAR networks within the same server blade and to shield networks from external networks, communication packets between LPARs can be filtered. This subsection describes filtering setting values, descriptions of functionality, communication-destination environments, and behaviors.

Disable setting for inter-LPAR communication packet filtering

- This is the default value and the basic operation of the shared NIC.
- When the communication source and the communication destination are in the same network segment, LPAR manager transfers packets to the destination LPAR via the virtual switch.
- When the communication source and the communication destination are in different network segments, packets are transferred to the external network.

Enable setting for inter-LPAR communication packet filtering

- Even when the communication source and the communication destination are in the same network segment, LPAR manager disconnects inter-LPAR communication via the virtual switch.
- LPAR manager transfers all packets to the external network.
- Use this setting when systems that do not communicate each other are integrated into the same server blade.

Disable (ALL) setting for inter-LPAR communication packet filtering

- When the communication source and the communication destination are in the same network segment, LPAR manager transfers packets to the destination LPAR via the virtual switch, and then transfer the packets to the external network.
- When the communication source and the communication destination are in different network segments, LPAR manager transfers packets to the external network.
- Use inter-LPAR communication within the range of the maximum possible bandwidth of the LAN switch because all packets are transferred to the external network.
- Use this setting when employing a redundant network configuration through Intel(R) PROSet connection monitoring in Windows, Linux bonding, or similar. For details, see [Notes on using inter-LPAR communication in a redundant network configuration on page 6-17](#).

Related topics

- [Virtual NIC Assignment screen on page 10-34](#)

Configuring inter-LPAR communication packet filtering

To configure filtering of communication packets between LPARs:

1. Connect to the LPAR manager Screen by using the OS console and then open the **Virtual NIC Assignment** screen.
2. Press the **F8** key.
The **Inter-LPAR Packet Filtering** sub-screen appears.
3. Specify **Enable**, **Disable**, or **Disable(ALL)**.

Related topics

- [Virtual NIC Assignment screen on page 10-34](#)

Using teaming functionality to build redundancy into the NIC configuration

Teaming functionality

The functionality that distributes the network load and increases the fault-tolerance of the network by building redundancy into the NIC configuration is called teaming. The following table describes the teaming functionality (including channel bonding) supported by LPAR manager.

Table 6-7 Teaming functionality supported by LPAR manager

Item	Mode	Shared NIC/virtual NIC	VF NIC
Windows Server 2008 R2	AFT	Y	--
	SFT	Y	--
	ALB	Y	--
	RLB	Y	--
	LA/EC/3ad/Static	N	--
	Dyn3ad	N	--
Windows Server 2012	No dependency on the switch	Y	Y
Windows Server 2012 R2	Static teaming	Y	Y
Windows Server 2016	LACP	N	N
Linux Channel Bonding	balance-rr	N	N
	active-backup	Y	Y
	balance-xor	N	N
	broadcast	N	N
	802.3ad	N	N

Item	Mode	Shared NIC/virtual NIC	VF NIC
	balance-tlb	Y	N
	balance-alb	Y	N
Legend: Y: Can be used N: Cannot be used --: Not supported			

Notes on using inter-LPAR communication in a redundant network configuration

To use inter-LPAR communication with shared NICs within the same server blade, you must specify the settings below for applicable network segments (both primary and secondary).

If you do not specify the settings, inter-LPAR communication might not be possible during a link failover.

Table 6-8 Settings specified for network segments that use inter-LPAR communication

Communication source LPAR configuration / Guest OS		Communication destination LPAR configuration / Guest OS						
		Windows Server 2008		Windows Server 2012	RHEL			
		Intel(R) PROSet ¹	Intel(R) PROSet ²	OS standard teaming ³	bonding active-backup	bonding balance-tlb	bonding balance-alb	hbonding active-backup
Windows Server 2008	Intel(R) PROSet ¹	C	C	C	C	C	C	C
	Intel(R) PROSet ²	C	A	A	B	C	A	C
Windows Server 2012	OS standard teaming ³	C	A	A	B	C	A	C
RHEL	bonding active-backup	C	B	B	B	C	B	C
	bonding balance-tlb	C	C	C	C	C	C	C
	bonding	C	A	A	B	C	A	C

Communication source LPAR configuration / Guest OS		Communication destination LPAR configuration / Guest OS						
		Windows Server 2008		Windows Server 2012	RHEL			
		Intel(R) PROSet ¹	Intel(R) PROSet ²	OS standard teaming ³	bonding active-backup	bonding balance-tlb	bonding balance-alb	hbonding active-backup
	balance-alb							
	hbonding active-backup	C	C	C	C	C	C	C
<p>Legend:</p> <p>A: On the Inter-LPAR Packet Filtering sub-screen on the Virtual NIC Assignment screen, use the default, Disable.</p> <p>B: On the Inter-LPAR Packet Filtering sub-screen on the Virtual NIC Assignment screen, use the default, Disable. Set "fail_over_mac=1" for the bonding option of the guest RHEL. Only when "fail_over_mac=1" cannot be set, select Disable(ALL) on the Inter-LPAR Packet Filtering sub-screen.</p> <p>C: On the Inter-LPAR Packet Filtering sub-screen on the Virtual NIC Assignment screen, select Enable.</p> <p>Note:</p> <p>1 When Intel(R) PROSet connection monitoring function is enabled in Windows Server 2008 R2 SP1</p> <p>2 When Intel(R) PROSet connection monitoring function is disabled in Windows Server 2008 R2 SP1</p> <p>3 When OS standard teaming function is used in Windows Server 2012 or later Windows Server</p>								

Related topics

- [Virtual NIC Assignment screen on page 10-34](#)

Monitoring data by using promiscuous mode

LPAR manager supports promiscuous mode for monitoring data flowing on the network. You can specify this setting by using the Virtual NIC Assignment screen. The following table describes the packet reception status depending on the value set for the guest OS.

Table 6-9 Setting values for promiscuous mode

Setting		Frame acceptance
Guest OS	LPAR manager screen	
Disable	Restricted/Through	Only frames of which destination is the LPAR (MAC address) are received by the guest OS on the LPAR.
Enable	Restricted	Only frames of which destination is the LPAR (MAC address) are received by the guest OS on the LPAR. For a VF NIC, only Restricted can be set.
	Through	All frames in the same network segment are received.

Example of using promiscuous mode

In the usage environments shown in [Table 6-10 Promiscuous mode and its usage environment on page 6-19](#), you must change promiscuous mode from Restricted to Through.

Table 6-10 Promiscuous mode and its usage environment

Usage environment	Operation when promiscuous mode is Restricted
Bridging is implemented in the guest OS	Packets cannot be relayed.
NLB of Windows is used	NLB does not operate normally.
ALB of Windows Server 2008 R2 Intel(R) PROSet is used	ALB does not operate normally.
NIC teaming of Windows Server 2012 or later is used	Communication becomes impossible after a failover occurs.

Packet capturing

Packet capturing captures packets flowing through a network, and displays and analyzes the contents of the packets.

- Capturing packets in the same network segment
Setting promiscuous mode to Restricted prevents the capture of unicast packets transferred between LPARs and PCs on an external network. If you want to capture such unicast packets, set promiscuous mode to Through.
- Capturing packets in another network segment
You cannot capture packets in another network segment, even if it is in the same VNIC segment.

Related topics

- [Virtual NIC Assignment screen on page 10-34](#)

Maintaining the I/O performance by using the HBA dedicated core mode of shared FCs

HBA dedicated core mode of shared FCs

This is the mode in which a specific LPAR dedicatedly uses the HBA core that sends or receives data. This mode can be used to maintain a certain level of performance because a HBA core is not shared by other LPARs.

You can use HvmSh to set HBA-core dedicated mode to FC ports that are configured as Shared FC.

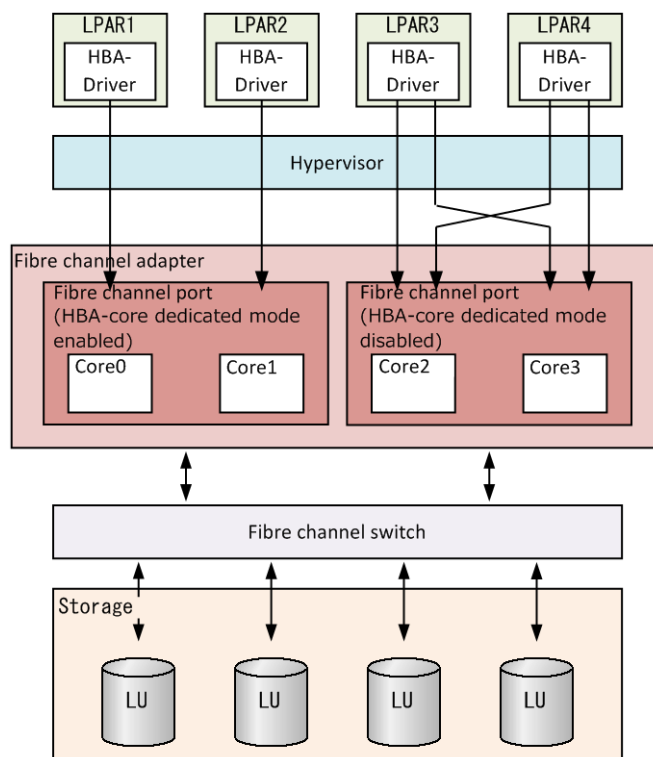


Figure 6-5 Concept of HBA-core dedicated mode

The following table lists the fibre channel adapters that support HBA-core dedicated mode. For information about the maximum number of vfcIDs that can be assigned, see the note in a later topic.

Table 6-11 Fibre channel adapters that support HBA-core dedicated mode

Item	Number of cores/port	Assignable vfcID
Hitachi 16Gb 1-port fibre channel adapter	4	1 to 4

Item	Number of cores/port	Assignable vfcID
Hitachi 16Gb 2-port fibre channel adapter	2	1 to 2

Requirements for HBA-core dedicated mode

Install a version of Fibre Channel driver and a version of Fibre Channel firmware supporting the HBA-core dedicated feature. For the versions of Fibre Channel driver and the versions of Fibre Channel firmware supporting the HBA-core dedicated feature, see the manual *HITACHI Gigabit Fibre Channel Adapter USER'S GUIDE (Support Matrix Edition)*.

Maintaining the I/O performance by using HBA-core dedicated mode

Enabling HBA-core dedicated mode does not fully prevent other LPARs from affecting the performance. To reduce the chances of other LPARs affecting the performance, consider the following before configuring your system:

- Make sure that fibre channel switch ports or storage ports are not shared with other LPARs or other systems, if connections to storage systems are made through fibre channel switches. Connect FC ports directly to storage ports in your system.
- Make sure that the RAID group for the LUs to be used is not shared with other LPARs or other systems.
- To reduce the chances of communication bandwidth affecting the LPARs that share the same FC port, set the maximum possible bandwidth to the FC port.
- In a system that runs on an LPAR sharing the same port, we recommend that a smaller number of I/O requests of larger size be sent to the storage system, and that a larger number of I/O requests of smaller size be sent.

Notes on HBA-core dedicated mode

The following shows restrictions of HBA-core dedicated mode:

- Setting the HBA-core dedicated mode
You must deactivate the LPARs to which an FC port is assigned in advance when you change HBA-core dedicated mode to the FC port from a value of "enabled" to that of "disabled", and vice versa.
- Maximum number of FCs that can be shared
The maximum number of vfcIDs that can be assigned is limited to the number of HBA cores in the fibre channel adapter. Although you can assign more vfcIDs than the number of HBA cores, if you do so, activation of LPARs is suppressed.
- Maximum performance

An LPAR cannot use HBA cores that are not allocated to the LPAR (even when they are idle). Therefore, the maximum IOPS that can be obtained with one core determines the overall maximum IOPS.

For example, if HBA-core dedicated mode is enabled for a fibre channel adapter that has 2 cores per port, the maximum IOPS is half the maximum IOPS obtained when HBA-core dedicated mode is disabled.

- Core allocation
Only one core can be allocated to an LPAR.
- Storage direct connection configuration
The storage direct connection configuration is supported only if the following EFI driver settings are specified:
 - Connection Type: Point to Point
 - Multiple PortID: Enable
- LPAR migration
The same vfcIDs that are used at the migration source must be unassigned at the migration destination. If the same vfcIDs are already assigned at the migration destination, LPAR migration fails.

Using N+M cold standby (LUID mode) to start LPARs

What is N+M cold standby (LUID mode)?

N+M cold standby (LUID mode) is used to store and inherit the unique identifier (LUID) of a boot volume when the WWNs and LUNs for storage ports are scanned and registered.

Alternatively, WWN/LUN inheritance requires manual operations to set and inherit the WWNs and LUNs for storage ports.

N+M cold standby (LUID mode) has the following features:

- N+M cold standby can be used in a storage direct connection configuration.
- LPAR migration can be used in a storage direct connection configuration.

Requirements to support N+M cold standby (LUID mode)

To use N+M cold standby (LUID mode), all of the following requirements must be met:

- The LPAR manager firmware version is 02-40 or later.
- A Hitachi 16Gb-fibre channel mezzanine card or 16Gb-fibre channel adapter is used.
- The boot mode is UEFI mode.
This requirement must be met when **64UEFI** is set for the **PB** item in the **Logical Partition Configuration** screen.

- The storage system is directly connected with CB 2500.

Setting N+M cold standby (LUID mode)

This subsection describes how to set N+M cold standby (LUID mode).

You can use the web console, the HVM management command (HvmSh), or the EFI shell interface to set N+M cold standby (LUID mode).

Using the web console to set N+M cold standby (LUID mode)

1. From the global task bar of the web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR** tab. Select the target LPAR name.
The **LPAR Information** dialog box appears.
4. Click the **Boot order settings** button.
The **Boot order settings** dialog box appears.
5. In the **HBA** tab, click the **HBA boot settings** button.
The **HBA boot settings** dialog box appears.
6. Specify **Enabled** for all of the following items:
 - **Boot Function**
 - **Select Boot Device**
 - **LUID Scan Mode**

If even one of the items above is not set to **Enabled**, WWN/LUN inheritance is used.

Using the EFI shell to set N+M cold standby (LUID mode)

Execute the `set` command, and then specify `Enabled` for all of the following items:

- `Boot Function`
- `Select Boot Device`
- `LUID Scan Mode`

If even one of the items above is not set to **Enabled**, WWN/LUN inheritance is used.

Using the HVM management command (HvmSh) to set N+M cold standby (LUID mode)

Execute the `set FcBootFunction` command, and then specify `Enabled` for all of the following items:

- `bootfunc`
- `SelectBootDevice`
- `LuidScanMode`

If even one of the items above is not set to **Enabled**, WWN/LUN inheritance is used.

Notes on N+M cold standby (LUID mode)

The following are notes on N+M cold standby (LUID mode):

- The boot order set by N+M cold standby (LUID mode) cannot be used when WWN/LUN inheritance is used. In addition, the boot order set by WWN/LUN inheritance cannot be used when N+M cold standby (LUID mode) is used.
This is applicable when WWN/LUN inheritance is used by downgrading the LPAR manager to a version that does not support N+M cold standby (LUID mode).
- If you change from N+M cold standby (LUID mode) to WWN/LUN inheritance, or from WWN/LUN inheritance to N+M cold standby (LUID mode), register the boot order again.
- If N+M switching or LPAR migration is performed in a storage direct connection configuration, an access to the storage system is made through the communication port specified in the LPAR after N+M switching or the LPAR on the migration destination. For this reason, you must verify the settings on the host group and the LUN security on the storage system in advance to confirm whether the LPAR can access the same boot volume before and after the N+M switching or before and after the migration.

Controlling access to the LPAR manager functions

This chapter describes the functionality that controls access to the various LPAR manager settings, and explains how to set the functionality.

- ☐ [Restricting LPAR manager operations by using Role Based Access Control](#)
- ☐ [Privileges of LPAR manager supported](#)
- ☐ [Performing operations on LPAR manager from the management module](#)
- ☐ [Notes on performing Role Based Access Control](#)
- ☐ [Authenticating LPAR manager users](#)
- ☐ [Authenticating a local user by using LPAR manager](#)
- ☐ [Authenticating a user by using LDAP](#)
- ☐ [Authenticating a user by using RADIUS](#)

Restricting LPAR manager operations by using Role Based Access Control

Role Based Access Control is functionality that restricts operations performed on LPAR manager according to the access privileges assigned to each user account. By applying Role Based Access Control, you can reduce risks such as invalid access to and incorrect operations on the security functionality of LPAR manager.

- LPAR manager supports access control based on roles (Role Based Access Control).
- If you enable user authentication of the LP CLI, Role Based Access Control is also enabled and you can control operations for the Web console, HVM Navigator, the LPAR manager screen, and the HVM management command (HvmSh).
- If you disable user authentication of the LP CLI, Role Based Access Control is also disabled and all operations can be performed.
- If you enabled user authentication of the LP CLI, Role Based Access Control is also applied to the operations on the CLI console. At this time, the same user permissions (role) as those of the user who logged in to the management module are applied.

A role is a group of one or more permissions assigned to a user. By using roles, you can efficiently manage the privileges assigned to each user account.

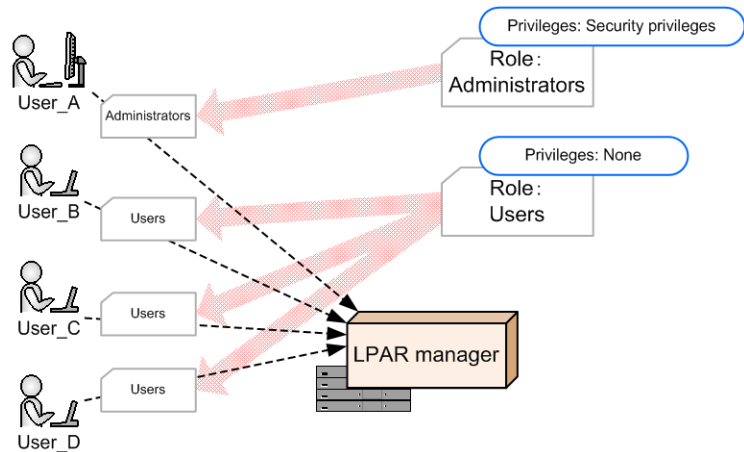


Figure 7-1 Roles and privileges

The following table lists the versions that support Role Based Access Control.

Table 7-1 Versions that support Role Based Access Control

Item	Version
Management module firmware	A0150 or later
LPAR manager firmware	02-45 or later
HvmSh	9.20 or later



Note: To use HVM Navigator, disable user authentication of the LP CLI or log in as a user with the LPAR manager security permission.

User and roles that can be assigned

Note that the roles that can be set differ as follows depending on the type of user:

- Local user
This users are authenticated by local authentication.
You can set a role for each Local user.
- LDAP authentication user
This users are authenticated by LDAP authentication.
You can set a common role for the LDAP authentication users. You cannot set a role for each the LDAP authentication user.
- RADIUS authentication user
This users are authenticated by RADIUS authentication.
You can set a common role for the RADIUS authentication users. You cannot set a role for each the RADIUS authentication user.
- Management module user
This users are authenticated by the management module, and are not authenticated by LPAR manager.
You can set a common role for the management module users. You cannot set a role for each the management module user.

Note that the user account is authenticated by LPAR manager specified as LPAR manager user account.

For details about how to assign a role to a user, see the following related topics:

Related topics

- [Setting a role for the management module users on page 7-5](#)
- [Overview of user authentication on page 7-9](#)
- [Creating a local user on page 7-13](#)
- [Setting LDAP information on page 7-21](#)
- [Setting RADIUS information on page 7-23](#)

Role types

LPAR manager supports the roles below. Manage the roles in units of running LPAR manager instances.

- Administrators role (Built-in role)
This role is built into the system. All privileges are assigned to this role.
The administrators role is a built-in role, so you cannot change the privileges set for this role.

- Users role (users-defined role)

This is a role for which the user can define any privileges.

The role name is the users role. By default, all privileges are assigned to this role.

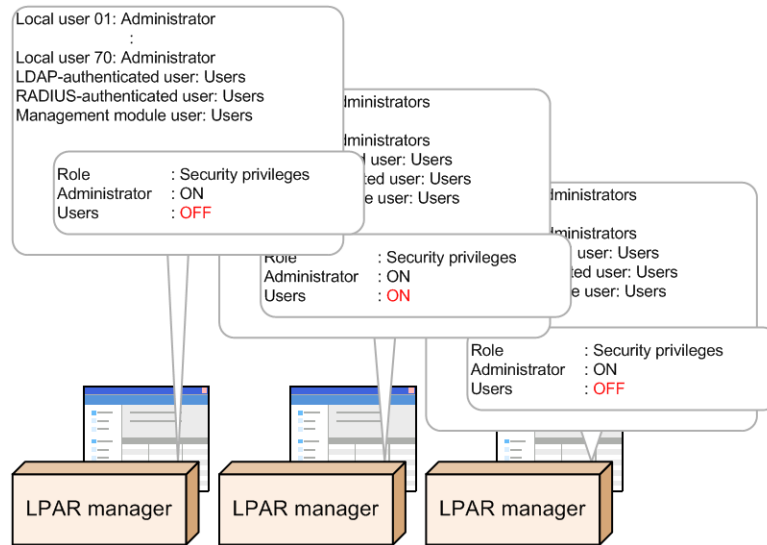


Figure 7-2 Setting and editing roles for each LPAR manager

Editing role privileges

This subsection describes how to edit the privileges to assign privileges to a role. By default, all privileges are assigned to all roles. To edit the privileges, use the Web console or the HVM management command (HvmSh).

Note that the Administrators role is a built-in role, so you cannot edit the privileges.

You must also have the LPAR manager security permission if you want to perform this operations.

Editing the privileges by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
The navigation area displays the **Modules** tree view.
2. In the **Modules** tree view, select the icon of the target server blade.
The application area displays the **Server Blade *n* Information** view. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR manager** tab. From the edit button, execute **User account management**.
The **User Account Management** dialog box is displayed.
4. Click the **Show and edit role settings** button.
The **Edit Role** dialog box is displayed.

5. Select the check boxes for the privileges that you want to assign to the role. Clear the check boxes for the privileges that you want to remove from the role.

Editing the privileges by using the HVM management command (HvmSh)

To use the HVM management command (HvmSh) to edit the privileges, execute the `opr RoleConfig` command.

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)

Setting a role for the management module users

Set a role for management module user. To set a role, use the Web console or the HVM management command (HvmSh).

The set role is applied to all the management module user. You cannot set a role in units of management module user.

In addition to this privilege, you must also have the LPAR manager security permission if you want to set role of management module user.

Setting a role for user accounts by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
The navigation area displays the **Modules** tree view.
2. In the **Modules** tree view, select the icon of the target server blade.
The application area displays the **Server Blade *n* Information** view. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR manager** tab. Click **LP login** button.
Use a user account that has the LPAR manager security permission to log in to LPAR manager. If the user account has already been used to log in to LPAR manager (if the **LP login** button is disabled), this step is not necessary.
4. From the edit button, execute **User account management**.
The **User Account Management** dialog box is displayed.
5. Click the **Edit management module user** button.
The **Management Module User Settings** dialog box is displayed.
6. Select a role that you want to assign.

Setting a role for user accounts by using the HVM management command (HvmSh)

To use the HVM management command (HvmSh) to set a role to the management module user, execute the `opr ManagementModuleUserRole` command.

Privileges of LPAR manager supported

LPAR manager supports the following privileges:

- LPAR manager security permission

For users for which the required privileges are not assigned, the operations by using the following interfaces are restricted:

- Web console
- LPAR manager screen
- HVM management command (HvmSh)

LPAR manager security permission

The LPAR manager security permission is required when you set the following LPAR manager functionality:

- Manage user accounts
- Set user authentication
- Role based access control
- Specify the audit log settings
- Specify the encrypted communication settings
- Manage certificates
- Obtain information that includes the security settings

Table 7-2 Functions that can be performed by using the LPAR manager security permission

Functions that can be performed	Function details
Manage user accounts	Viewing user information. Note that you can obtain the user information about your local user without the LPAR manager security permission.
	<ul style="list-style-type: none">• Adding a local user• Deleting a local user
	Changing the password of a local user. Note that you can change the password of your local user without the LPAR manager security permission.
	Setting a validity period for the password of a local user

Functions that can be performed	Function details
Set user authentication	<ul style="list-style-type: none"> Enabling user authentication Disabling user authentication
	Setting the user authentication method
	<ul style="list-style-type: none"> Setting up LDAP Setting up RADIUS
	Changing the valid login time by using HvmSh
	Obtaining the user authentication log (viewing the user authentication log)
Role based access control	Setting up roles
Specify the audit log settings	Setting up the audit log configuration (setting up syslog transfer)
Specify the encrypted communication settings	Changing the security strength (changing the permitted communication protocol)
	Setting up the connection mode for the virtual COM console
	Creating a host key for SSH connection of the virtual COM console
Manage certificates	<ul style="list-style-type: none"> Creating a CSR Obtaining a CSR
	<ul style="list-style-type: none"> Enabling certificate verification Disabling certificate verification
	<ul style="list-style-type: none"> Creating a certificate Registering a certificate Obtaining a certificate Deleting a certificate
Obtain information that includes the security settings	<p>Collective obtaining of the configuration information that includes the following information (displayed by the LPAR manager settings):</p> <ul style="list-style-type: none"> User authentication Role based access control Audit log Encrypted communication Manage certificates <p>You can obtain the configuration information that does not include the above information without the LPAR manager security permission.</p>
	Obtaining security configuration information.

Performing operations on LPAR manager from the management module

This section provides an overview of using a user logged in to the management module to perform operations on LPAR manager.

Note that if the LPAR manager firmware version is 02-45 than earlier or the user authentication of the LP CLI is disabled, you can change all of the LPAR manager settings.

Logging in to LPAR manager on the Web console

This subsection describes the overview and procedure of the operation in which the user who is operating the Web console uses an LPAR manager user account to log in to LPAR manager. If the operations on LPAR manager are restricted by Role Based Access Control, the user will be able to set the LPAR manager functions that require privileges if the user uses an LPAR manager user account that has the appropriate privileges to log in to LPAR manager.

Note the following points on logging in to LPAR manager:

- To log in to LPAR manager, you need a user account with the privilege that can operate the target LPAR manager functions.
- If the user authentication of the LP CLI is enabled, access to the LPAR manager functions is restricted according to the assigned role.
- If the role assigned to the management module users (all user accounts that can log in to the Web console) does not have the LPAR manager security permission, operations of the settings related to LPAR manager security are restricted.

At this time, if you use an LPAR manager user account that has the LPAR manager security permission to log in to LPAR manager, you will be able to operate the settings related to LPAR manager security.

- In addition, when it takes longer than 5 seconds to log into LPAR manager, a timeout occurs.
- In addition, when no operations are performed in LPAR manager for 30 minutes, you will be logged out

Logging in to LPAR manager by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR manager** tab, and then click the **LP login** button.
The **LP Login** dialog box is displayed.

4. Specify values for **User name** and **Password**, and then log in to LPAR manager.

Notes on performing Role Based Access Control

This section describes the notes on performing access control.

- The Administrators role needs to be assigned to one or more of local user. If only one local user has the Administrators role, you cannot delete that local user.
- If the user authentication of the LP CLI is disabled, you cannot remove the LPAR manager security permission from the management module user.
If the LPAR manager security permission is not assigned to the management module user, you cannot disable the user authentication of the LP CLI.
- If you use HVM Navigator, you must disable user authentication of the LP CLI or log in as a user with the LPAR manager security permission.

Authenticating LPAR manager users

This section describes user authentication of LPAR manager. By authenticating the users who access LPAR manager, you can secure LPAR manager.

Related topics

- [LPAR manager security permission on page 7-6](#)

Overview of user authentication

If you enable user authentication, invalid access to LPAR manager can be prevented. In addition, if you prepare an account for each user, you can manage the users who access LPAR manager.

LPAR manager supports the following authentication methods:

- Local authentication
It is the method that LPAR manager authenticates user. An user account must be registered for each LPAR manager.
- Combined use of Local authentication and LDAP authentication
With this method, usually LPAR manager authenticates the user. If the user is not registered in LPAR manager, an access to the LDAP server is made to authenticate the user. User information can be collectively managed by the LDAP server, not by LPAR manager.
- Combined use of Local authentication and RADIUS authentication
With this method, usually LPAR manager authenticates the user. If the user is not registered in LPAR manager, an access to the RADIUS server

is made to authenticate the user. User information can be collectively managed by the RADIUS server, not by LPAR manager.

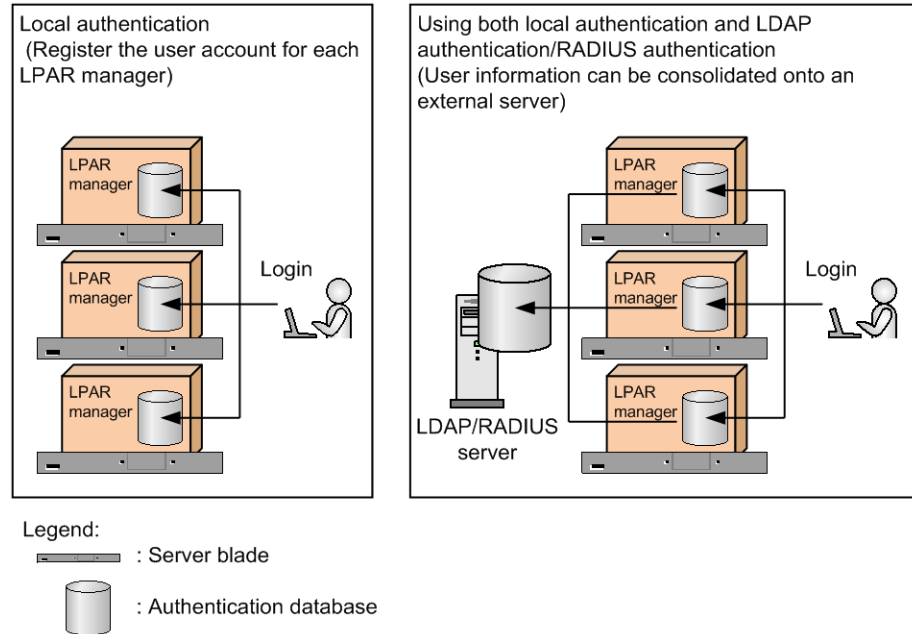


Figure 7-3 User authentication of LPAR manager

LPAR manager can perform user authentication by using the following functionality:

- HVM Navigator
- Virtual COM console
- LP web system
- HvmSh command



Tip:

User authentication is disabled for the virtual COM console and the HVM management command (HvmSh) by default. Enable user authentication for both.

For the interfaces below, the management module performs user authentication. Before using one of these interfaces, log in to the management module.

- Web console
- LPAR manager screen

The maximum number of users who can log in to LPAR manager at the same time from the Web console, the HVM Navigator, and the HVM management command (HvmSh) is 70. The 71st and subsequent users will be forcibly logged out even if they can log in to LPAR manager.

Enabling user authentication

This subsection describes how to enable user authentication. Use the Web console, the LPAR manager screen, or the HVM management command (HvmSh) to configure user authentication.

Because HCSM is connected to LPAR manager via a management module, you do not need to change HCSM settings even if you enable user authentication on LPAR manager.

You must also have the LPAR manager security permission if you want to perform this operations.

Enabling user authentication by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. From the edit button, execute **LP CLI Settings** or **Virtual COM Console Settings**.

Enabling user authentication by using the LPAR manager screen

1. Use the OS console to start the LPAR manager screen.
2. Move to the **System Configuration** screen. Press **F12** to switch to the right-hand page.
3. Set **Authentication**.
For enabling user authentication when connecting to the virtual COM console, set the **VC** column.
For enabling user authentication for LP CLI communication, set the **LP CLI** column.

Enabling user authentication by using the HVM management command (HvmSh)

If you enable user authentication by using the HVM management command (HvmSh), execute the `opr HvmIfAuthentication` command.



Tip:

To enable user authentication on the virtual COM console, change the settings to "Connection mode: Telnet" and "Telnet authentication: Enable". Alternatively, change the settings to "Connection mode: SSH".

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)

Collecting user authentication log data

LPAR manager logs a maximum of 9,000 events related to user authentication. You can collect the user authentication by using the Web console or the HVM management command (HvmSh).

User authentication log is cleared when LPAR manager restarts or shuts down. Collect the necessary authentication log data before shutting down LPAR manager.

You must also have the LPAR manager security permission if you want to perform this operations.

Collecting user authentication log data by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. From the edit button, execute **Show authentication Log**.

Collecting user authentication log data by using the HVM management command (HvmSh)

If you collect user authentication log data by using the HVM management command (HvmSh), execute the `get HvmAuthenticationLogs` command.

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)

Authenticating a local user by using LPAR manager

This section describes local authentication in which a local user is authenticated by using LPAR manager.

The following table lists the versions that support local authentication.

Table 7-3 Versions that support local authentication

Item	Version
Management module firmware	A0110 or later
LPAR manager firmware	02-05 or later
HvmSh	8.40 or later

Initially registered user account for local authentication

The following initially registered account can be used for local authentication:

- User name: admin
- Password: password



Tip:

If the version of LPAR manager is upgraded from a version that does not support the user authentication functionality to a version that supports the user authentication functionality, the initially registered account is the user name and password for the LP Web system.



Note:

For security reasons, create a new account and delete the initially registered account, or change the password of the initially registered account during the initial configuration of LPAR manager.

Creating a local user

This subsection describes how to create a local user. When creating a local user, you also need to set the role for the local user.

You can register up to 70 user accounts. Use the Web console, the LPAR manager screen, or the HVM management command (HvmSh) to create a local user.

Specifiable characters for user names and passwords

- You can specify a user name or a password consisting of a character string of 1 to 31 characters.
- For user names, alphanumeric characters, periods (.), hyphens (-), and underscores (_) can be specified. The first character must be an alphabetic character.
- For passwords, alphanumeric characters and symbols (excluding space characters) can be specified.
- User names and passwords are case sensitive.



Note:

- For security reasons, change the password during the initial configuration of LPAR manager.
 - You must also have the LPAR manager security permission if you want to perform this operations.
-

Creating a user account by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.

In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.

3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. From the edit button, select **User Account Management**. The **User Account Management** dialog box is displayed.
4. Click the **Create** button. The **Create User Account** dialog box is displayed.
5. Specify the user name, password, and role.

Creating a user account by using the LPAR manager screen

1. Use the OS console to start the LPAR manager screen.
2. Move to the **System Configuration** screen. Press **F12** to switch to the right-hand page.
3. Set **User List**.
To add a local user, press the **F1** key.
Note that you cannot use the LPAR manager screen to set a role for the local user.

Creating a user account by using the HVM management command (HvmSh)

To use the HVM management command (HvmSh) to create a local user and then assign a role, execute the `opr HvmUserAdd` command.

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)
- [System Configuration screen on page 10-47](#)

Deleting a local user

This subsection describes how to delete an local user created for local authentication.

Use a management module, the Web console, the LPAR manager screen, or the HVM management command (HvmSh) to delete a local user.

You must also have the LPAR manager security permission if you want to perform this operations.

Deleting a user account by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.

In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.

3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. From the edit button, select **User Account Management**. The **User Account Management** dialog box is displayed.
4. Select a user account that you want to delete, and then click the **Delete** button.

Deleting a user account by using the LPAR manager screen

1. Use the OS console to start the LPAR manager screen.
2. Move to the **System Configuration** screen. Press **F12** to switch to the right-hand page.
3. To delete a user account, place the cursor on the user account name (**Name**) that is displayed in the **User List**, and then press the **F2** key.

Deleting a user account by using the HVM management command (HvmSh)

To use the HVM management command (HvmSh) to delete a local user, execute the `opr HvmUserRemove` command:

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)

Changing a password or role for local user

Change the password or role used for local authentication.

- You can change the password by using the Web console, the LPAR manager screen, or the HVM management command (HvmSh).
To change the password of other local user when the LPAR manager firmware version is 02-45 or later, you need the LPAR manager security permission.
- You can change the role by using the Web console or the HVM management command (HvmSh).
To change the role of both your local user and other local user, you need the LPAR manager security permission.
- If you change the role assigned to a user account for local authentication, changes that occur in conjunction with this change are stored in the LPAR manager configuration information.
- You must also have the LPAR manager security permission if you want to perform this operations.

Changing the password or role by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
The navigation area displays the **Modules** tree view.
2. In the **Modules** tree view, select the icon of the target server blade.
The application area displays the **Server Blade *n* Information** view. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR manager** tab. From the edit button, execute **User Account Management**.
The User Account Management dialog box is displayed.
4. Click the **Edit** button.
The Edit User Account dialog box is displayed.
5. Change the password or role.

Changing the password of your account by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
The navigation area displays the **Modules** tree view.
2. In the **Modules** tree view, select the icon of the target server blade.
The application area displays the **Server Blade *n* Information** view. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR manager** tab. Click the **LP login** button to log in to LPAR manager.
4. From the **Edit** button, execute **Edit LP login account settings**.
The LP Login Account Settings dialog box is displayed.
5. Change the password.

Changing the password by using the LPAR manager screen

1. Use the OS console to start the LPAR manager screen.
2. Move to the **System Configuration** screen. Press **F12** to switch to the right-hand page.
3. To change the password of a user account, place the cursor on the user account name (**Name**) that is displayed in the **User List**, and then press the **F3** key.
The **Setting Password Expiry** sub-screen appears.
4. Enter the new password.
 - For the password, you can use alphanumeric characters and symbols. However, you cannot use space characters.
 - Specify a password consisting of a character string of 1 to 31 characters.
5. Re-enter the password for confirmation.

Changing the password or role by using the HVM management command (HvmSh)

To use the HVM management command (HvmSh) to change the password, execute the `opr HvmPasswdExpiry` command.

In addition, to use the HVM management command (HvmSh) to change the role of a local user, execute the `opr HvmUserConfig` command.

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)
- [When the password expires on page 7-18](#)
- [System Configuration screen on page 10-47](#)

Setting a validity period for the password of a local user

By setting a validity period for a password, you can improve the security of user authentication. This subsection describes how to set a validity period for the password of a local user.

- You can set the validity period of a password to unlimited or to a value from 1 to 365.
- The validity period of a password is set to unlimited by default.

You can specify the validity period of a password by using the Web console, the LPAR manager screen, or the HVM management command (HvmSh).

You must also have the LPAR manager security permission if you want to perform this operations.

Setting the validity period of a password by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. From the edit button, select **Authentication Settings** and specify the settings.

Setting the validity period of a password by using the LPAR manager screen

1. Use the OS console to start the LPAR manager screen.
2. Move to the **System Configuration** screen. Press **F12** to switch to the right-hand page.
3. Sets **Expiry**.

Setting the validity period of a password by using the HVM management command (HvmSh)

If you set the validity period of a user password by using the HVM management command (HvmSh), execute the `opr HvmPasswdExpiry` command.

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)
- [When the password expires on page 7-18](#)

When the password expires

When the password of an LPAR manager user account expires, the user account cannot be used to log in to LPAR manager. However, if the user has the LPAR manager security permission, the user can re-assign the password without logging in to LPAR manager.

You can re-assign the password by using the Web console or the HVM management command (HvmSh).



Note:

- If you forget the local user name or password of the user for which you set the LPAR manager security permission, you will be unable to add a local user or perform other operations. We recommend that you take a preventive measure such as setting the LPAR manager security permission for multiple users.
-

Re-assigning the password by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. From the edit button, select **Change expired password** and then execute **Edit**.
The **Change Expired Password** dialog box is displayed.
4. Specify settings for **User name**, **Current password**, and **New password** to re-assign the password.

Re-assigning the password by using the HVM management command (HvmSh)

To re-assign the password by using the HVM management command (HvmSh), execute the `opr HvmPasswdRecovery` command.

Related topics

- [Setting a validity period for the password of a local user on page 7-17](#)

Authenticating a user by using LDAP

This section describes LDAP authentication by using LDAP.

The following table lists the versions that support LDAP authentication.

Table 7-4 Versions that support LDAP authentication

Item	Version
Management module firmware	A0145 or later
LPAR manager firmware	02-40 or later
HvmSh	9.00 or later

Support requirements for LDAP authentication

This section describes the support requirements for LDAP authentication.

Table 7-5 Support requirements for LDAP authentication

Item	Scope of support
LDAP server type	<p>Active Directory as provided in the OSs below is supported.</p> <ul style="list-style-type: none">• Windows Server 2008• Windows Server 2008 R2• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016 <p>If the LPAR manager firmware version is 02-45 less than earlier, you must set the LDAP authentication user to uidNumber in the Active Directory environment settings.</p> <p>For details about Active Directory settings, see the manual <i>Hitachi Compute Blade 2500 Management Module User Guide</i>. When you see the manual, note that the following:</p> <ul style="list-style-type: none">• Management module is appropriately read it in LPAR manager.• The user name and password, be in accordance with the LPAR manager and LDAP server each specification.• The allow group of log in to the management module, is not used in LPAR manager.
Number of LDAP servers	<p>Maximum of three LDAP servers.</p> <p>LDAP servers will be accessed in the order of LDAP server 1, LDAP server 2, and then LDAP server 3. Authentication will be performed by using the first server that is successfully accessed.</p>
User name and password to be	<ul style="list-style-type: none">• You can specify a user name or a password consisting of a character string of 1 to 31 characters.

Item	Scope of support
registered on the LDAP server	<ul style="list-style-type: none"> For user names, alphanumeric characters, periods (.), hyphens (-), and underscores (_) can be specified. The first character must be an alphabetic character. For passwords, alphanumeric characters and symbols (excluding space characters) can be specified. User names and passwords are case sensitive. <p>About also confirmed to be the specifications and limitations of the LDAP server.</p>
LDAP protocol	LDAP v3
TLS communication method	StartTLS
Binding to an LDAP server	Anonymous binding or simple authentication via TLS

Enabling LDAP authentication

This subsection describes how to enable LDAP authentication as the user authentication method. You can use the Web console or the HVM management command (HvmSh) to enable LDAP authentication.

You must also have the LPAR manager security permission if you want to perform this operations.

Enabling LDAP authentication by using the Web console

1. In the global tab of the web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR manager** tab. From the **Edit** button, execute **Edit authentication settings**.
The **Authentication Settings** dialog box appears.
4. Specify **Local authentication prior to LDAP authentication** for **User authentication method**, and then click the **Confirm** button.

Enabling LDAP authentication by using the HVM management command (HvmSh)

To use the HVM management command (HvmSh) to enable LDAP authentication, execute the `opr ExternalAuthentication` command.

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)

Setting LDAP information

This subsection describes how to set LDAP server information and directory retrieval information that are used for LDAP authentication. You can use the Web console or the HVM management command (HvmSh) to set LDAP information.

You must also have the LPAR manager security permission if you want to perform this operations.

Setting LDAP information by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR manager** tab. From the **Edit** button, execute **Edit LDAP settings**.
The **LDAP Settings** dialog box appears.
4. Specify required items, and then click the **Confirm** button.

Setting LDAP information by using the HVM management command (HvmSh)

To use the HVM management command (HvmSh) to set LDAP information, execute the following commands:

- LDAP configuration settings: `opr LdapConfig` command, `opr LdapPasswd` command
- Security settings on the destination for encrypted communication: `opr HvmIfSecureLevel` command
- Settings on whether to validate the certificate when encrypted communication is performed: `opr HvmIfSecureVerify` command
- Registration of the certificate of the communication destination or the certificate of the certificate authority: `opr HvmClientCertificateRegist` command

In addition, to use the HVM management command (HvmSh) to assign a role to a LDAP authentication user, execute the `opr LdapConfig` command.

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)

Authenticating a user by using RADIUS

This section describes RADIUS authentication, by using RADIUS.

The following table lists the versions that support RADIUS authentication.

Table 7-6 Versions that support RADIUS authentication

Item	Version
Management module firmware	A0150 or later
LPAR manager firmware	02-45 or later
HvmSh	9.20 or later

Support requirements for RADIUS authentication

This section describes the support requirements for RADIUS authentication.

Table 7-7 Support requirements for RADIUS authentication

Item	Scope of support
RADIUS server type	Free RADIUS and the following types of Network Policy Server are supported: <ul style="list-style-type: none">Windows Server 2008Windows Server 2008 R2Windows Server 2012Windows Server 2012 R2Windows Server 2016
Number of RADIUS servers	Maximum of three RADIUS servers. RADIUS servers will be accessed in the order of RADIUS server 1, RADIUS server 2, and then RADIUS server 3. Authentication will be performed by using the first server that is successfully accessed.
User name and password to be registered on the RADIUS server	<ul style="list-style-type: none">You can specify a user name or a password consisting of a character string of 1 to 31 characters.For user names, alphanumeric characters, periods (.), hyphens (-), and underscores (_) can be specified. The first character must be an alphabetic character.For passwords, alphanumeric characters and symbols (excluding space characters) can be specified.User names and passwords are case sensitive. About also confirmed to be the specifications and limitations of the RADIUS server.
Shared secret	The following encryption key is used when the RADIUS server is connected: <ul style="list-style-type: none">The number of characters that can be specified for the encryption key is 1 to 64.The characters that can be specified for the encryption key are alphanumeric characters and symbols (excluding spaces).
Authentication method	The following authentication methods are supported: <ul style="list-style-type: none">PAPCHAP

Item	Scope of support
	<ul style="list-style-type: none"> MS-CHAPv2

Enabling RADIUS authentication

This section explains how to enable RADIUS authentication as the user authentication method. To configure RADIUS authentication, use the Web console or the HVM management command (HvmSh).

You must also have the LPAR manager security permission if you want to perform this operations.

Enabling RAIDUS authentication by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR manager** tab. From the **Edit** button, execute **Edit authentication settings**.
The **Authentication Settings** dialog box appears.
4. In **User authentication method**, specify **Local authentication prior to RADIUS authentication**, and then click the **Confirm** button.

Enabling RADIUS authentication by using the HVM management command (HvmSh)

To enable RADIUS authentication by using the HVM management command (HvmSh), execute the `opr ExternalAuthentication` command.

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)

Setting RADIUS information

This subsection describes how to set RADIUS server information and the authentication method that are used for RADIUS authentication. This subsection also describes how to set the role to be assigned to the RADIUS authentication user.

You can use the Web console or the HVM management command (HvmSh) to set RADIUS information.

You must also have the LPAR manager security permission if you want to perform this operations.

Setting RADIUS information by using the Web console

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR manager** tab. From the **Edit** button, execute **Edit RADIUS settings**.
The **RADIUS Settings** dialog box appears.
4. Appropriately specify settings for the required items and click the **Confirm** button.

Setting RADIUS information by using the HVM management command (HvmSh)

To use the HVM management command (HvmSh) to set RADIUS information, execute the `opr RadiusConfig` command.

In addition, to use the HVM management command (HvmSh) to assign a role to a RADIUS authentication user, execute the `opr RadiusConfig` command:

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)
- [Verifying connection with the RADIUS server on page 7-24](#)

Verifying connection with the RADIUS server

Execute the communication test to check if the RADIUS server used for RADIUS authentication can be connected. To execute the communication test for the RADIUS server, use the Web console or the HVM management command (HvmSh).

Note that after setting RADIUS information, verify that connection with the RADIUS server can be correctly established.

You must also have the LPAR manager security permission if you want to perform this operations.

Verifying connection with RADIUS server by using the Web console

In advance, log in to the management module.

1. In the global tab of the Web console, select the **Resources** tab.
The navigation area displays the **Modules** tree view.
2. In the **Modules** tree view, select the icon of the target server blade.
The application area displays the **Server Blade *n*** view. The variable *n* represents a unique number that identifies the server blade.

3. In the **Server Blade *n*** view, select the **LPAR manager** tab. From the edit button, execute **RADIUS connectivity verification**.
The **RADIUS Connectivity Verification** dialog box is displayed.
4. Specify the required items, and then execute the communication test.
According to the result of the communication test, a message dialog box is displayed.

Verifying connection with RADIUS server by using the HVM management command (HvmSh)

To use the HVM management command (HvmSh) to verify the connection with the RADIUS server, execute the `opr RadiusConnectivityVerify` command.

Related topics

- [Logging in to LPAR manager on the Web console on page 7-8](#)

Managing LPAR manager and LPARs

This chapter describes the functionality for managing LPAR manager and LPARs, and how to set the functionality.

- ☐ [Setting the ports to be used for management path communication](#)
- ☐ [Displaying the LPAR manager screen and the guest screen](#)
- ☐ [LP communication settings](#)
- ☐ [Encrypting communication of the LPAR manager](#)
- ☐ [Initializing the LPAR manager configuration](#)
- ☐ [Backing up and restoring the LPAR manager configuration information](#)
- ☐ [Updating LPAR manager firmware](#)
- ☐ [Linking with management software](#)
- ☐ [N+M cold standby](#)
- ☐ [HA monitor and LPAR manager](#)
- ☐ [Use of USB devices with the server blade](#)
- ☐ [Setting the times handled by LPAR manager](#)
- ☐ [Setting NTP time synchronization for the LPAR manager system time](#)
- ☐ [Logical VGA snapshot](#)

- ☐ [Viewing the LPAR manager system logs](#)
- ☐ [Collecting audit logs](#)
- ☐ [Specifying the DNS server](#)

Setting the ports to be used for management path communication

This section describes the settings of the NICs and ports that are used by LPAR manager for communication for management paths.

Related topics

- [NIC to be used for management path communication on page 1-13](#)

What is the management path specification functionality?

You can select a maximum of two ports from among the ports of the NICs that are installed in a server blade, and specify them as ports to be used on management paths. By specifying ports on different NICs, you can configure port redundancies and enhance fault tolerance.

Supported server blade

This functionality is supported by all server blades.

Firmware combination

Note that the management path specification functionality is supported for the combinations of LPAR manager firmware version, management module firmware version, and server blade firmware version listed in the table below.

Table 8-1 Firmware versions

Server blade	Server blade firmware	Management module firmware	LPAR manager firmware
CB 520X B1	07-28 or later	A0120 or later	02-20 or later
CB 520X B2	09-17 or later	A0135 or later	02-27 or later
CB 520X B3	11-04 or later	A0165 or later	02-55 or later
CB 520H B3	08-29 or later	A0120 or later	02-20 or later
CB 520H B4	10-03 or later	A0160 or later	02-50 or later

Specifiable NICs for communication with management paths

You can specify the following NICs for communication with management paths:

- Onboard LAN on CB 520X B1/B2/B3, CB 520H B3/B4
- Broadcom 1Gb 4-port LAN mezzanine card
- 1000BASE-T 4-port LAN adapter
- 10GBASE-SR 2-port LAN adapter
- Emulex 10Gb 2-port converged network adapter

Scheduling mode of NICs to be used as management paths

In general, be sure to set the scheduling mode of the NICs to be used as management paths to shared mode.

If you specify a NIC whose scheduling mode is set to dedicated mode as a NIC to be used as a management path, LPAR manager changes the scheduling mode of the specified NIC to shared mode.

If the dedicated port functionality is enabled, scheduling mode of only the specified ports will be changed to shared mode.

Because of this change, LPAR manager behaves as follows:

- If the number of the controllers or ports on the NICs whose scheduling mode is set to shared mode exceeds the maximum (8 for controllers, 16 for ports), the scheduling mode of the NIC with the largest PCI bus number among the NICs whose scheduling mode has been set to shared mode is changed to dedicated mode.
- If a NIC whose scheduling mode was changed is assigned to an LPAR, the assignment is removed.
If NICs from which assignment to LPARs were removed exist, LPAR manager starts in safe mode. If necessary, review the changed configuration and remove safe mode.
- If the changes above occur, LPAR manager system log messages, and system event log (SEL) messages and information are output. Note that if the failure level of an output message is Warn, HCSM is notified via an alert.

Related topics

- [Safe mode on page 9-20](#)
- [LPAR manager system log messages on page 11-17](#)

Specifying the ports to be used for management path communication

Use the Web console to specify the ports to be used for communication between LPAR manager and management modules via management paths.

Before this operation, be sure to power off the target server blade.

Using the Web console to specify the ports for management path communication

1. From the global task bar of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.

3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. In the **Edit** menu, select **Edit system settings**.
The **System Settings** dialog box appears.
4. Click **Advanced Option**.
5. In **Specify management NIC**, select **Enable** and specify the NICs and ports to be used for management path communication.
If you specify NICs or ports for **Port0** and **Port1**, you can use the ports for management path communication in a redundant configuration.

Confirming the communication statuses of management paths

LPAR manager allows you confirm actual statuses of the active port and the standby port used for communication with management paths. You can use the Web console, the LPAR manager screen, or an HVM management command (HvmSh) to confirm the statuses of the ports.

To update the status of the standby port, diagnose the management path.

Using the Web console to confirm the statuses of communication ports

1. From the global task bar of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. Check **Management path**, **Port*n***, and **State**.
The variable *n* of **Port*n*** represents a unique number that identifies the port, and is displayed as a value of 0 or 1.
If the server blade is powered on, one of the following values is displayed:

Active

This port is used for management path communication.

Standby

This port does not have problems with communications, and is in the normal standby state.

Error

This port is in a network failure state.

Link down

This port is in the link-down state.

The management path is in a blocked state.

Unknown

LPAR manager is unable to communicate externally.

No port is specified for the path.

When the server blade is powered off, if there is a problem with the specification as a port for management path communication, a message is displayed.

Using the LPAR manager screen to confirm the statuses of communication ports

In the System Service State screen, check SVP Network Path State. For details about the System Service State screen, see [System Service State screen on page 10-58](#).

Using an HVM management command (HvmSh) to check the statuses of communication ports

Execute the `get ConfigAll` command to check the contents of the `MANAGEMENT_PATH` record.

Related topics

- [System Service State screen on page 10-58](#)

Diagnosis of the standby port of management paths

LPAR manager diagnoses the status of the standby port, which is used for communication with management paths. The Web console or an HVM management command (HvmSh) is available for the diagnosis. To update the status of the standby port periodically, enable the management path periodic diagnosis setting.

Using the Web console to manually diagnose the standby port of management paths

1. From the global task bar of the Web console, select the **Resources** tab. In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the target server blade. In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. In the **Edit** menu, select **Diagnose the management paths**. A confirmation dialog box appears. Take action according to the message in the dialog box.

Using the HVM management command (HvmSh) to manually diagnose the standby port of management paths

Execute the `get MgmtStandbyPortStatus` command.

Using the Web console to periodically diagnose the standby port of management paths

1. From the global task bar of the Web console, select the **Resources** tab. In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the target server blade. In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR manager** tab. In the **Edit** menu, select **Edit LP options**. The **LP option settings** dialog box appears.
4. In **Mgmt path periodic diagnosis setting**, select Enable. A confirmation dialog box appears. Take action according to the message in the dialog box.

Using the HVM management command (HvmSh) to periodically diagnose the standby port of management paths

Execute the `opr MgmtStandbyPortDiagnosis` command.

Switching the active port of the management path

The following describes how to switch the active port of the management path.

Using the HVM management command (HvmSh) to switch the active port of the management path

Execute the `opr MgmtPathSwitch` command.

Monitoring the link status of the active port of the management path

The following describes how to monitor the link status of the active port of the management path. If a link down is detected, switch the active port of the management path.

Using the HVM management command (HvmSh) to monitor the link status of the active port of the management path

Execute the `set MgmtPathSwitchLinkDown` command.

Displaying the LPAR manager screen and the guest screen

This section describes the LPAR manager screen for managing LPAR manager and LPARs, and the guest screen for setting up guest OSs.

OS console and virtual COM console for displaying screens

LPAR manager provides the OS console and the virtual COM console as consoles for displaying various screens.

Both the OS console and the virtual COM console are console windows running on the CLI console. Use the commercial terminal software Tera Term to execute the CLI console.

The following describes these consoles.

Features of the OS console

- The console that is connected to the management module and started from the terminal software is called the OS console.
- When the OS console starts, the LPAR manager screen appears.
You can use the LPAR manager screen to set and manage the functionality of LPAR manager and LPARs.
- The OS console can switch the display between the LPAR manager screen and the guest screen.
You can use the guest screen to set and manage the guest OS.
- The OS console and the virtual COM console cannot be used at the same time. If you connect to the same guest OS from different terminal software, operations from the OS console will be given higher priority.

Features of the virtual COM console

- The console that is displayed by connecting to LPAR manager running on a server blade from terminal software is called the virtual COM console.
- This console operates at a faster speed than the standard serial connection by the Serial over LAN (SOL) functionality of LPAR manager.
- When you start the virtual COM console, the guest screen appears.
However, you cannot display the LPAR manager screen.
- If you start multiple terminal softwares and connect each terminal software to LPAR manager by using the virtual COM console, you can perform operations on a maximum of 16 guest OSs. However, you cannot connect to the same guest OS at the same time.
- When LPAR manager starts, it assigns the TCP port number to be used for connecting to the guest screen via Telnet or SSH.
Although you can change this TCP port number in the System Configuration screen, we recommend that you use the initial value (serial number from 20801) assigned by LPAR manager.
When changing the TCP port number, first investigate the terminal and network environment to be used.

**Note:**

- We recommend that you use the remote desktop connection functionality of the OS to connect to the guest OS desktop window.
If you use the remote console to connect to the guest OS desktop window, the problems below occur because the connection emulates SVGA display.
 - The remote control window display and mouse operations are slow to respond.
 - If you use the mouse in a logical EFI window or in a text window that appears during the installation process of the guest OS, keyboard operations are slow to respond.
 - Error messages that are generated during Windows startup might not be displayed correctly.

Related topics

- [Logical Partition Configuration screen on page 10-8](#)
- Manual *Hitachi Compute Blade 2500 Series Management Module User Guide*

Using the OS console to display the LPAR manager screen

To open the LPAR manager screen, start the CLI console by using the Telnet or SSH communication protocol, and then enter the command that opens the LPAR manager screen.

The console that is connected to the management module by using the CLI console is called the OS console.

1. Start the CLI console by specifying Telnet or SSH as the communication protocol and specifying the management module IP address as the connection-destination host.
2. On the CLI console, execute the `change console -b server-blade-number` command.

The LPAR manager screen opens.

Notes on using the virtual COM console

Operations of the guest screen

- Although the virtual COM console can work with multiple guest OSs at once, the increase in output data might cause a degradation in the performance of consoles associated with other LPARs.
- When a paste operation to a guest screen involves a large number of characters, some of the characters might not be pasted.
You cannot paste 256 or more characters to the Windows command prompt, or 1,024 or more characters to the Linux prompt. In Linux, this

operation might cause the OS to hang or the screen to behave in unexpected ways.

In text editors such as vi, make sure the text to be pasted in a single paste operation is less than 10,000 characters.

- If boot processing stops when the guest OS is being booted, take actions according to the following instructions:

For Windows:

If boot processing stops with the UEFI window displayed, press the **Enter** key to resume the boot processing.

For Linux:

If boot processing stops at the grub command console, press the **Esc** key to resume the boot processing.

When the virtual COM console is running

- If you enable the virtual COM console, a load is placed on the entire LPAR manager processing even if the virtual COM console is not actually connected. To avoid this, make sure that you enable or disable the functionality when you use the virtual COM console.
- If you remain connected to the virtual COM console for an extended period of time, I/O processing of the console might unexpectedly stop. If this occurs, reconnect to the virtual COM console.
- If you repeatedly change the configuration of the virtual COM console in the Logical Partition screen while connected to the virtual COM console, the console screen becomes scrambled.
If this occurs, in the Edit (E) menu of Tera Term, execute Screen clear (S) to refresh the screen.
- If a communication failure occurs during a connection to a virtual COM console, reconnection to that virtual COM console might become impossible. In such a case, specify "N" for the port setting of the affected virtual COM console, and then return the setting to its previous value. After doing so, reconnection will become possible after a certain amount of time elapses (after a maximum of 17 minutes).

Related topics

- [Logical Partition Configuration screen on page 10-8](#)

Configuring the terminal software

We recommend that you use the commercial terminal software Tera Term to start the CLI console that displays the LPAR manager screen and the guest screen. The operations described in this manual assume that Tera Term is used for operating the LPAR manager screen and the guest screen.

Make sure that you set up the Tera Term environment in advance, as shown below.

Table 8-2 Tera Term environment settings

Item	Setting
Terminal size	80x50
Linefeed code	CR
Terminal type	VT100
Chinese character encoding set to be used for transmission	UTF-8
Meta key option	Enabled

Enabling the virtual COM console functionality

To use the virtual COM console, first enable the virtual COM console functionality for the target LPAR.

1. Start the OS console and then, from the **LP Menu** screen, open the **Logical Partition Configuration** screen.
2. Place the cursor on the VC column of the target LPAR row, and then press the **Enter** key.
The **LPARn Virtual Console** sub-screen appears.
3. Select **Y**.
Note that, after placing the cursor on the VC column in the above step, you can press the **F1** key and select a VC number.

Related topics

- [Logical Partition Configuration screen on page 10-8](#)

Using the virtual COM console to display the guest screen

Display the guest screen by using the virtual COM console.

Features when connecting to the virtual COM console

- Use Telnet or SSH to connect to the virtual COM console. Select either Telnet or SSH. You cannot use both at the same time.
- When connecting to the virtual COM console, user authentication can be performed.
 - For Telnet connection, you can select whether to perform user authentication.
 - For SSH connection, user authentication is required.
 - Telnet connection is enabled and user authentication is disabled by default.
- For SSH connection, an SSH host key is used.

- An SSH host key is automatically generated the first time LPAR manager starts.
 - You can also re-create an SSH host key.
 - The type of SSH host key that can be created is RSA and the length is fixed at 2048 bits.
1. Start the CLI console by specifying Telnet or SSH as the communication protocol, the LPAR manager IP address as the destination host, and specifying the TCP port number of the LPAR on which the target guest OS is to run.
The virtual COM console and the LPAR manager screen appear.

**Note:**

- If a LP IP address for IPv4 is not specified, you cannot disable Telnet authentication. Select Enable for Telnet authentication or select SSH for connection mode.
- If Telnet user authentication is disabled, Telnet connections cannot be established to LP IP addresses for IPv6.

**Tip:**

- If the virtual COM console does not display the guest screen, check the configuration of the serial console.

Related topics

- [Authenticating LPAR manager users on page 7-9](#)

LP communication settings

Specify the port number to be used for communication between LPAR manager and management module. This function is supported if the version of the management module firmware is version A0130 or later.

All LPAR managers in the server chassis use the same port number. You cannot use a different port number for an individual LPAR manager.

Before you change the setting, make sure that all server blades for which Logical partitioning is set to Enable.

Table 8-3 Firmware versions

Server blade	Server blade firmware	Management module firmware	LPAR manager firmware
CB 520X B1	07-34 or later	A0130 or later	02-25 or later
CB 520X B2	09-17 or later	A0135 or later	02-27 or later
CB 520X B3	11-04 or later	A0165 or later	02-55 or later
CB 520H B3	08-35 or later	A0130 or later	02-25 or later

Server blade	Server blade firmware	Management module firmware	LPAR manager firmware
CB 520H B4	10-03 or later	A0160 or later	02-50 or later



Note:

- To set port numbers, the firmware version of all the server blades whose Logical Partitioning is set to Enabled must be a version that supports this function. If the firmware version does not support this function, port numbers cannot be set.

Setting the port numbers for LPAR manager management and communication

1. In the **Resources** tab, select **LP communication settings** from the **Systems** tree view.
The various port numbers that are currently set are displayed.
2. Click the **Edit** button.
The **LP communication settings** dialog box is displayed.
3. Specify the port number to be used.
 - For **Port of management module**, specify a number in the range from 1024 to 32767.
 - For **Port of LP**, specify a number in the range from 1024 to 32767.

Encrypting communication of the LPAR manager

You can enhance security with encrypted communication information, when connecting to the virtual COM console and when connecting to LPAR manager by using the LP CLI from external management software. By enabling SSH for communication with the virtual COM console, you can perform secure communication with encrypted communication information.

Encrypting communication with the virtual COM console

When connecting to the virtual COM console, SSH can be used and communication can be encrypted. If SSH is enabled, an SSH host key is used for communication. An SSH host key is automatically generated the first time LPAR manager starts. You can also re-create an SSH host key.

1. Start the OS console and then, from the **LP Menu** screen, open the **System Configuration** screen.
2. Place the cursor on **Type** of the **System Configuration** screen, and then press the **Enter** key.
The **Virtual Console Connection Type** sub-screen appears.
3. Select **ssh**.
If you select **Telnet**, non-encrypted communication can be performed.

When configuration is complete, the configuration information about user authentication is saved.

Re-creating an SSH host key

Re-create the SSH host key that is used in SSH-encrypted communication.

1. Start the OS console and then, from the **LP Menu** screen, open the **System Configuration** screen.
2. Place the cursor on **Generate Host Key** of the System Configuration screen, and then press the **Enter** key.
The **Execute Generate Host Key?** sub-screen appears.
3. Select **Yes**.

Initializing the LPAR manager configuration

This section describes how to initialize the LPAR manager configuration from the Web console. Note that you can only initialize the LPAR manager configuration while the server blade is off.

When you initialize the LPAR manager configuration, all configuration information is deleted from LPAR manager. We recommend that you back up the configuration information before continuing with this process.

To initialize LPAR manager settings from the Web console:

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. From the **Action** pull-down menu, select **Initialize LP Settings**.
3. In the **Initialize LP Settings** dialog box, click **OK**.

Backing up and restoring the LPAR manager configuration information

This section describes how to back up the configuration of LPAR manager from the Web console, and how to restore the configuration from a backup.

Before backing up the LPAR manager configuration

When you set up LPAR manager and are just about to start operation, and before you perform any of the operations below, create an LPAR manager backup file and keep it somewhere safe.

Create a backup file before making any of the following changes to the hardware configuration:

- Adding or removing processors, and changing the hyper-threading configuration
- Adding or removing memory

- Changing the settings for planned operations in reduced-operation mode
- Adding or removing mezzanine cards or I/O adapters and changing card types
- Changing the SMP configuration of a server blade
- Adding or removing PCI expansion blades

Create a backup file after making the following changes to the configuration of LPARs or LPAR manager:

- Changing the LPAR manager system configuration
- Adding, deleting, or reconfiguring an LPAR
- Changing the boot order setting for an LPAR
- Changing the EFI driver settings for an LPAR

When a failure occurs in a system, you can recover the system quickly by restoring it from a backup. We recommend that you regularly back up LPAR manager configuration information in case you need to revert back to the last known good configuration.

Note that, by using the KeepConfig option, you are able to back up an LPAR manager configuration as of a point in time before device isolation, even after the device isolation. For details, see [Backing up the LPAR manager configuration as of a time before device isolation on page 8-16](#).

If a hardware failure occurs, the affected devices might be blocked or might operate in reduced-operation mode. These blocked devices or devices in reduced-operation mode will not be recognized the next time LPAR manager starts, and some of the configuration information for the devices will be removed from the configuration information or reset. In situations of this nature, you can replace the hardware and then restore the backup file.

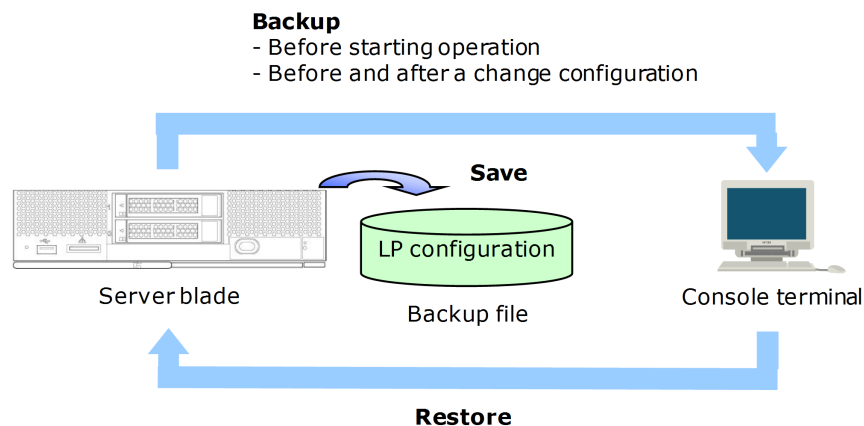


Figure 8-1 Saving and backing up the LPAR manager configuration information

The following table lists the means by which LPAR manager configuration information is saved, backed up, and restored.

Table 8-4 Saving the LPAR manager configuration

LPAR manager status	Means	Save	Backup	Restore
Inactive	Web/CLI console	--	Y	Y
	HCSM	N	N	N
	HVM Navigator	--	--	--
	LPAR manager screen	--	--	--
	HvmSh	--	--	--
Active	Web/CLI console	Y	Y	N
	HCSM	Y ¹	N	N
	HVM Navigator	Y	N	N
	LPAR manager screen	Y	N	N
	HvmSh	Y	--	--
Legend: Y: Can be performed N: Cannot be performed --: Not available Notes: 1. HCSM automatically saves the LPAR manager configuration when it is changed from HCSM.				

Backing up the LPAR manager configuration as of a time before device isolation

When device isolation occurs, the LPAR manager does not detect devices in startup of the LPAR manager. At that time, part of the LPAR manager configuration on devices is cleared or reset.

By using the KeepConfig option, the LPAR manager does not save the LPAR manager configuration in device isolation until exit of safe mode and holds LPAR manager configuration before device isolation.

You are able to set the KeepConfig option with HvmSh. For details, see the manual *HVM Management Command (HvmSh) Operation Guide*.

- When device isolation occurs with the KeepConfig option enabled, the LPAR manager outputs event logs and notifies HCSM of the event via an alert.
- When LPAR manager detects one of the following events comparing with the LPAR manager configuration, the LPAR manager determines that PCI devices are isolated.

- The number of physical processor cores has reduced.
- Available memory size has reduced.
- One or more of IO devices are not detected.
- When an event log is output and the LPAR manager starts in safe mode, back up the LPAR manager configuration. After that, check device isolation and then exit safe mode. Also, after you change hardware devices for maintenance, restore the LPAR manager configuration with a backup file.



Note:

- When you use the KeepConfig option, install one of the following versions of management module firmware.

Server blade	Management module firmware
CB 520X B1	A0120 or later
CB 520X B2	A0135 or later
CB 520X B3	A0165 or later
CB 520H B3	A0120 or later
CB 520H B4	A0160 or later

- When you perform one of the following operations with the KeepConfig option enabled, the LPAR manager detects reduction of the number of PCI devices and then starts in safe mode. In this case, exit safe mode.
 - Removing PCI devices or coordinate the number of PCI devices by software operation
 - Performing N+M cold standby between the active and the standby blades with different hardware configurations

Related topics

- [Safe mode on page 9-20](#)

Backing up the LPAR manager configuration

This section describes how to back up the configuration of LPAR manager from the Web console.

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. From the **Action** pull-down menu, select **Back up LP settings**.
3. In the **Back up LP settings** dialog box, click **Save**.

Save the files by using the procedure associated with the operating system you are using.

The file names are as follows:

`hvm-pX-VVRR-YYYYMMDDhhmmss.backup`

(*X* is the partition (server blade) number and *VVRR* is the version of LPAR manager assigned to the server blade).

Restoring the LPAR manager configuration

When restoring the LPAR manager configuration from the Web console, make sure that the backup file you use satisfies the following requirements:

- The backup file was created for the same instance of LPAR manager
- The current firmware version of LPAR manager is the same as when the file was backed up

If the file you use does not satisfy these requirements, LPAR manager might not work correctly. The following describes how to restore the LPAR manager configuration. Note that you can only restore the LPAR manager configuration if the server blade is turned off.

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. From the **Action** pull-down menu, select **Restore LP settings**.
3. In the **Restore LP settings** dialog box, click **Browse** and select the file you want to restore.
Open the file by using the procedure associated with the operating system you are using.
4. Click **Confirm**, and then click **OK** to start the restore process.

Updating LPAR manager firmware

Version numbers of LPAR manager firmware are in the format *VV-RR*. A revision upgrade entails a change to the *RR* component of the firmware version. For example, a revision upgrade might involve upgrading from version 02-00 to 02-01.



Note:

- Although you can use the downgraded version of the LPAR manager firmware, the LPAR manager configuration information might not be inherited.

To downgrade the LPAR manager firmware version, perform the operations described in [Restoring the LPAR manager configuration on page 8-18](#) first, and then those described in [Performing a version upgrade of LPAR manager firmware on page 8-20](#).

When downgrading the LPAR manager firmware version to the previously used LPAR manager firmware version, restore the LPAR manager configuration information that was backed up while that LPAR manager firmware was being used.

- Before you update the LPAR manager firmware, check whether the Emulex 10Gb NICs below are used. If they are used, you might have to update the Emulex 10Gb NIC firmware.

- Onboard LAN
- Emulex 10Gb 2-port converged network adapter

For details about the relationship between LPAR manager firmware versions and Emulex 10Gb NIC firmware versions, see [Limitations on using Emulex 10Gb NICs on page 1-30](#) in [Notes on logical NICs on page 1-30](#).

Relationship between server blades and LPAR manager firmware

The following shows the relationship between server blades and LPAR manager firmware:

- On the management module, you can install a maximum of four banks of LPAR manager firmware with different versions.
- You need to assign an LPAR manager firmware bank to the server blades running in LP mode.
- You can assign one LPAR manager firmware bank to multiple server blades.
- You can install new LPAR manager firmware and assign it to a server blade even if LPAR manager is running. When LPAR manager restarts, the LPAR manager firmware is updated to the new version.

To check the information about the LPAR manager firmware, use the Web console. The following table shows information items related to the LPAR manager firmware and the Web console window where each information item can be checked.

Table 8-5 Information items related to the LPAR manager firmware and the corresponding window in Web console

Item	Description	Confirmation method on the Web console
Upper limit on the available versions	The highest version of the LPAR manager firmware supported by the server blade	Resources tab > Systems > LP License
Current firmware version	The version of the LPAR manager firmware that is currently in use.	Resources tab > Systems > Firmware management > Server blade tab
Assigning LPAR manager firmware	Linking a server blade to an LPAR manager firmware bank	Resources tab > Systems > Firmware management > Server blade tab
Installed version	The version of the LPAR firmware installed on the management module	Resources tab > Systems > Firmware management > LPAR Manager tab

Related topics

- [Updating LPAR manager firmware on page 8-21](#)

Performing a version upgrade of LPAR manager firmware

The following table describes the scenarios in which you might need to perform a version upgrade of LPAR manager firmware:

Table 8-6 Triggers a revision upgrade for the LPAR manager firmware

Item	Details and tasks
Scenario 1	To install LPAR manager firmware in a bank that is not assigned to a server blade, perform the following operations: <ul style="list-style-type: none">Installing LPAR manager firmwareUpdating LPAR manager firmware
Scenario 2	To install LPAR manager firmware in a bank that is assigned to a server blade, perform the following operation: <ul style="list-style-type: none">Installing LPAR manager firmware
Scenario 3	To use LPAR manager firmware that is already installed in a firmware bank, perform the following operation: <ul style="list-style-type: none">Updating LPAR manager firmware

Installing LPAR manager firmware

For obtaining LPAR manager firmware, contact <contact information>.

The following describes how to install LPAR manager firmware.

- From the **Systems** tree view in the **Resources** tab, select **Firmware**.
- Select a firmware bank on the **LPAR Manager** tab, and click **Install firmware**.
The **Install LP Firmware** dialog box appears.
- Click **Browse**, specify the LPAR manager firmware file, and then click **Confirm**.
- The procedure from this point onward differs depending on the status of the firmware bank you selected.
 - If "-----" is displayed for **Status** for the selected firmware bank, click **OK** to complete the installation process.
 - If the value of **Status** is "Assigned (enable firmware overwrite)", select the server blades whose configuration information you want to back up, and then click the **Backup** button.
- Click **Save**.

Save the files by using the procedure associated with the operating system you are using. The file names are as follows:

`hvm-pX-VVRR-YYYYMMDDhmmss.backup`

(*X* is the partition (server blade) number and *VVRR* is the version of LPAR manager assigned to the server blade).

The system downloads a number of backup files equivalent to the number of server blades you selected as backup targets.

- In the **Install LP Firmware** dialog box, click **OK**.

**Tip:**

- "Backup LP settings", "Executed", and "Unexecuted" only appear if you are installing firmware in a firmware bank whose status is "Assigned (enable to overwrite firmware)".
-

Updating LPAR manager firmware

The following describes how to update the LPAR manager firmware.

1. From the **Systems** tree view in the **Resources** tab, select **Firmware**.
2. On the **Server blade** tab, select a server blade and click **Assign LP firmware**.
The **Assign LP firmware** dialog box appears.
3. Select **LP firmware version**, and click **Next**.
4. Back up the configuration information by clicking **Backup** and then **Save**.
You can skip this step if you created a backup when you installed the LPAR manager firmware.
5. Click **Confirm**, and then click **OK**.

Uninstalling LPAR manager firmware

You can only uninstall LPAR manager firmware from a firmware bank that is not assigned to a server blade.

1. From the **Systems** tree view in the **Resources** tab, select **Firmware**.
2. In the **LPAR Manager** tab, select a firmware bank and click **Install firmware**.
3. In the **Install LP Firmware** dialog box, click **OK**.

Linking with management software

This section describes linkage with various types of management software.

Linkage with HCSM

Hitachi Compute Systems Manager (HCSM) is software that facilitates the operation of servers in large-scale environments.

HCSM allows the system administrator to manage hardware resources, monitor system activity, perform N+M cold standby, implement power management, and operate hardware.

Related topics

- Manual *Hitachi Command Suite Compute Systems Manager User Guide*

Linkage with HVM Navigator

HVM Navigator is a GUI-based tool to support the configuration and operation of LPARs. It supports functionality such as the monitoring functionality, which displays the usage of processors and NICs in graphs, and the LPAR migration functionality, which migrates an LPAR from the server blade on which the LPAR is running to another server blade.

If you use HVM Navigator, you must disable the user authentication of the LP CLI, or log in as a user with the LPAR manager security permission.

When HVM Navigator is used, there are restrictions on guest OSs. For the restrictions, see [Differences in supported items depending on the guest OSs on page B-22](#).

Related topics

- Manual *Hitachi Compute Blade HVM Navigator User's Guide - Getting Started*
- Manual *Hitachi Compute Blade HVM Navigator Installation Manual*
- Manual *Hitachi Compute Blade HVM Navigator User's Guide - LPAR Configuration*
- Manual *Hitachi Compute Blade HVM Navigator User's Guide - Monitoring*
- Manual *Hitachi Compute Blade HVM Navigator User's Guide - Viewer*
- Manual *Hitachi Compute Blade HVM Navigator User's Guide - Migration*
- Manual *Hitachi Compute Blade HVM Navigator User's Guide - Operation Quick Reference*
- Manual *Hitachi Compute Blade LPAR Migration Guide*

N+M cold standby

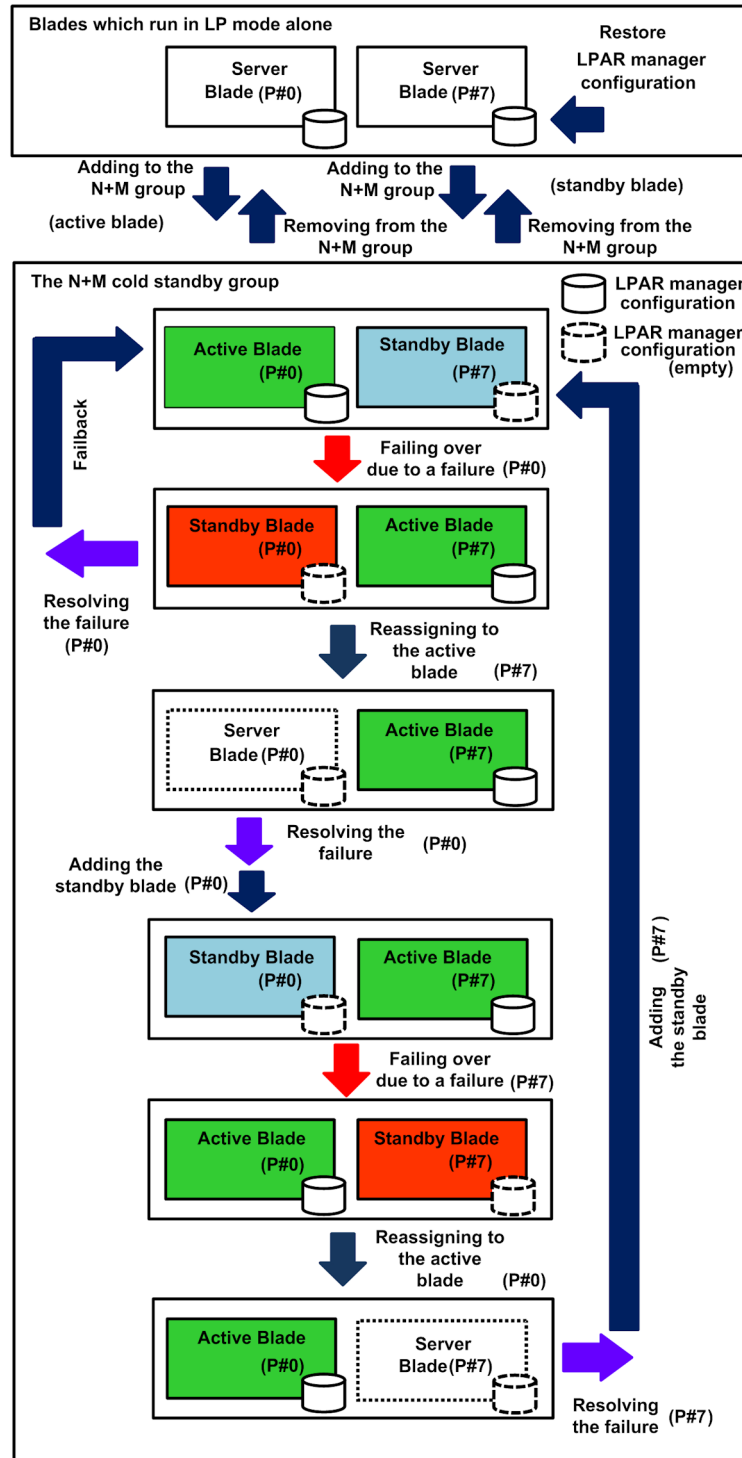
N+M cold standby is to start the standby blade automatically when an active blade fails. Management server, such as HCSM, receives the failure notification, analyzes the failure, and switches the active blade to the standby one.

For details, see the manual *Hitachi Compute Blade 2500 Series Management Module User Guide*.

How to use the N+M cold standby from the viewpoint of the LPAR manager configuration

1. Make sure that all server blades that are targeted for N+M cold standby group assignment can start in LP mode alone, and make a note of the LP IP address and the VNIC System Number. Then, select Yes for Pre-State Auto Activation on the LP Options screen and save the LPAR manager configuration. After that, backup the LPAR manager configuration.
If you have any plan to use the server blades in LP mode alone in the step 7, perform them (this step) to all of the server blades.

2. After completing the adding active and standby blades to the N+M cold standby group, start LPAR manager on the active blade and boot the guest OS. After that, you can use the functionality of LPAR manager.
3. If a failover occurs due to a failure on the active blade or the N+M failover test, LPAR manager automatically starts on the active blade (standby blade before the failover) and the guest OS that was operating until just before the failover also automatically starts. After that, you can use the functionality of LPAR manager. The LPAR manager configuration of the standby blade (active blade before the failover) is cleared (undefined) in the process of the failover.
4. The failed standby blade is repaired (or replaced) by maintenance personnel. You are not required to perform the maintenance work. Do not restore the LPAR manager configuration of the repaired (or replaced) standby blade to keep it cleared.
5. For the N+M failback, you are not required to perform operations related to the LPAR manager configuration. Do not restore the LPAR manager configuration of the standby blade after the N+M failback to keep it cleared.
6. You reassign the blade as active, the blade is automatically removed from the N+M cold standby group. After the removed server blade is repaired (or replaced), add the server blade to the N+M standby group again. Do not restore the LPAR manager configuration to keep it cleared.
7. If you want to start a server blade in LP mode alone and the server blade has failed over at least once, you need to restore the LPAR manager configuration because the LPAR manager configuration of the server blade is cleared. Perform the following procedure to restore the LPAR manager configuration. If you perform the procedure in a wrong way, the WWN or MAC address of the LPAR will be duplicated in another LPAR.
 - a. On the Web console, check that the LP IP Address and VNIC System No. of the server blade that was removed from the N+M cold standby group are blank. A server blade whose LP IP Address and VNIC System No. are not blank was a standby blade to which the failover had never been performed, or an active blade.
 - b. On the Web console, specify the LP IP Address and VNIC System No. that you made a note in the step 1 for the blank LP IP Address and VNIC System No., and then start LPAR manager without restoring the LPAR manager configuration. Do not restore the LPAR manager configuration in this step.
 - c. Check that LPAR manager is started, and then shut down LPAR manager. Do not go to the next step until you check that LPAR manager is normally started.
 - d. Restore the LPAR manager configuration that was backed up for the server blade in the step 1.



This figure explains the situation that there are two server blades, partition no. 0 (P#0) and partition no. 7 (P#7).

Figure 8-2 Transition of LPAR manager configuration in N+M cold standby configuration

Related topics

- [Using N+M cold standby \(LUID mode\) to start LPARs on page 6-22](#)

- Manual *Hitachi Compute Blade 2500 Series Management Module User Guide*

HA monitor and LPAR manager

You can create a cluster system based on HA monitor (Linux) between an LPAR and a physical server.

HA monitor uses a partition ID to uniquely identify platform hardware. Partition IDs are derived from the physical partition name. However, the HA monitor that support LPARs uses partition IDs derived from the logical partition name. This logical partition name must match the value of the LPAR Name field in the LPAR manager control screen.

The following table shows examples of the recommended NIC assignment using HA monitor.

Table 8-7 Type of connected LANs and HA monitor environments

Connected LAN	HA monitor environment	
	Same server blade	Same server chassis but different server blade, or different server chassis
Operation LAN	Virtual NIC	Shared NIC and VF NIC
LAN for monitoring	Virtual NIC	Shared NIC and VF NIC
LAN for reset	Shared NIC and VF NIC	

Use of USB devices with the server blade

You can use USB devices connected to the front USB port, USB devices connected via the KVM connector, and the remote console with the server blade.

For CB 520X B1/B2/B3, you can assign USB devices connected via the KVM connector and the remote console to an LPAR in exclusively shared mode, and USB devices connected to the front USB port to an LPAR in dedicated mode.

For CB 520H B3/B4, you can assign USB devices connected to the front USB port, USB devices connected via the KVM connector, and the remote console to an LPAR in exclusively shared mode.

Attach and Detach operations of USB devices in exclusively shared mode

USB devices in exclusively shared mode are connected and disconnected from LPARs by the Attach and Detach operations. The Attach operation is equivalent to plugging in a USB device and the Detach operation is equivalent

to unplugging a USB device. For this reason, you must perform a safe hardware removal operation for Windows or an unmount operation for Linux on a guest OS before performing a Detach operation. You can attach USB devices in exclusively shared mode to one LPAR at a time. An LPAR to which a USB device is not attached recognizes the USB device as disconnected.

Related topics

- [PCI Device Assignment screen on page 10-30](#)
- [LP Options screen on page 10-74](#)
- Manual *Hitachi Compute Blade 2500 Series Getting Started Guide*

Setting the times handled by LPAR manager

This section describes the setting of the times handled by LPAR manager.

Times handled by LPAR manager

LPAR manager creates each time by using information about the differences between times. In addition, based on the LPAR manager system time, LPAR manager creates a logical timer for each LPAR. A guest OS on an LPAR uses this logical timer to manage the OS system time.

LPAR manager handles times shown in the following figure and table.

Table 8-8 Times handled by LPAR manager

Time	Description
System unit time (Physical RTC time)	A battery-powered clock (local time) in the server blade. The LPAR manager system time is based on this time.
LPAR manager system time	Used as the LPAR manager time to be displayed on the LPAR manager screen. This is calculated by adding the elapsed time obtained from the timer counter to the physical RTC time at startup of LPAR manager.
Logical RTC time	The base clock for the OS system time. This is calculated by using the difference from the LPAR manager system time.
OS system time	Used as the time of the guest OS. This is calculated by adding the logical RTC time at startup of the OS, the elapsed time obtained from the timer counter and timer interrupt, and the time zone.
SEL time	Used as the time stamp of the logical SEL. This is calculated by using the difference from the LPAR manager system time.

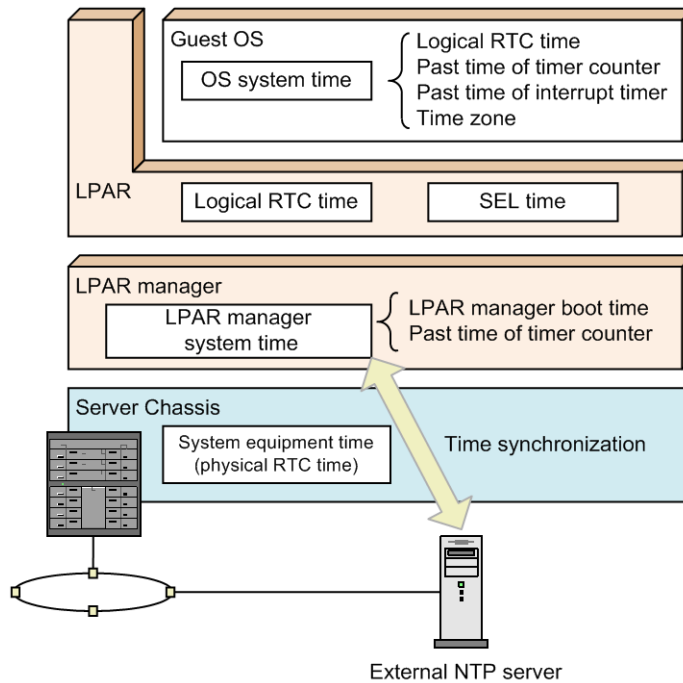


Figure 8-3 Times handled by LPAR manager



Note:

- NTP time synchronization that takes place at regular intervals (15 minutes) stops if the difference between the correct time and the time to be corrected exceeds 60 seconds. If this phenomenon occurs, in the LP System Logs screen, find a message that includes "An abnormal time difference was detected", and then take action described in the message.

The following table shows the precision of the timers, and how or when to adjust time.

Table 8-9 Accuracy and change of timers

Item	Time	Accuracy	How and when time is adjusted
System unit	Physical RTC time ¹	±4 seconds per day	<ul style="list-style-type: none"> • UEFI setup menu • Date and Time screen² • Enabling NTP time synchronization • Booting LPAR manager while NTP system time synchronization is enabled • Periodic NTP time synchronization once every 24 hours • Saving the LPAR manager configuration

Item	Time	Accuracy	How and when time is adjusted
			<ul style="list-style-type: none"> Shutting down LPAR manager
LPAR manager	LPAR manager system time	± 4 seconds per day	<ul style="list-style-type: none"> Date and Time screen² Enabling NTP time synchronization Booting LPAR manager while NTP system time synchronization is enabled Periodic NTP time synchronization once every 15 minutes
LPAR	Logical RTC time ¹	± 1 second per day	<ul style="list-style-type: none"> Guest OS command Date and Time screen² Periodic NTP time synchronization once every 15 minutes
	SEL time	± 1 second per day	<ul style="list-style-type: none"> Date and Time screen² Periodic NTP time synchronization once every 15 minutes
Guest OS	OS system time ³	± 2 seconds per day	Guest OS command
<p>Notes:</p> <ol style="list-style-type: none"> LPAR manager provides Save Time Config functionality that automatically saves and updates the physical and logical RTC time. This functionality eliminates the time lag that is introduced when you restart the guest OS or LPAR manager. We recommend that you enable Save Time Config on the LP Options screen. When the LPAR is deactivated, you can adjust the logical RTC time. If you adjusted the system equipment time or a difference is generated between the system equipment time and the LPAR manager system time due to time correction through the external NTP server, we strongly recommend that you adjust the logical RTC time by the Adjust LPAR Time before booting the guest OS. If you do not use the recommended kernel parameters with LPAR manager, issues might occur such as the OS system time differing significantly from the actual time, or the system failing to boot. To ensure that the OS system time remains accurate, we recommend that you synchronize the OS system time with an NTP server. 			

Related topics

- [LP Options screen on page 10-74](#)

Setting NTP time synchronization for the LPAR manager system time

This section describes how to set the time zone for the LPAR manager system, and how to configure LPAR manager to use an NTP server to coordinate time.

Setting the time zone for the LPAR manager system:

1. Display the **Date and Time** screen of the LPAR manager screen.
2. On the **Date and Time** screen, press **F7** (Change System Time Zone) to display a sub-screen in which you can set the time zone.
Set the time zone, and press the **Enter** key.
3. In the **Date and Time** screen, align your cursor with **TimeSync** and press the **Enter** key. The **Select NTP Server** sub-screen appears.
4. In the **Select NTP Server** sub-screen, select **SVP**, and then press **Enter**.
5. On the **System Service State** screen, make sure NTP is set to **SYNC**.

Configuring auto-save for time information:

1. Display the **LP Options** screen.
2. In the **LP Options** screen, align the cursor with **Save Time Config** and press the **Enter** key. The **Save Time Configuration Setting** sub-screen appears.
3. On the **Save Time Configuration Setting** sub-screen, select **Enable**, and then press **Enter**.

Saving the configuration in the LPAR manager screen:

1. Display the **LP Menu** screen.
2. In the **LP Menu** screen, press **F9** (Save Configuration).

Related topics

- [LPAR manager Menu screen on page 10-5](#)

Logical VGA snapshot

You can view and acquire the images that the guest OS on each LPAR outputs to the display device.

The logical VGA snapshot functionality lets you acquire images from a web server provided by LPAR manager. You can use a Web browser on an external console to access this web server and acquire stored snapshot images (still images) output by each LPAR to the display device. Note that you can use the HVM management command (HvmSh) to disable communication using HTTP. If you change this setting, restart LPAR manager. For details about the

command, see the manual *HVM Management Command (HvmSh) Operation Guide*.

LPAR manager uses a built-in certificate signed with SHA-1 in http communications.

We do not recommend that you use the certificate owing to insecurity. We recommend that you use the server certificate for LPAR manager, instead.

For details about the server certificates for LPAR manager, see [Server certificate issued by LPAR manager on page 9-6](#). For details about the command, see the manual *HVM Management Command (HvmSh) Operation Guide*.

The logical VGA snapshot functionality has three components:

Table 8-10 Components that configure the logical VGA snapshot functionality

Component	Description
Logical VGA device	A virtual VGA device to which the guest OS writes image data.
Snapshot image storage web server	A web server built into LPAR manager. This server collects image data from virtual VGA devices in response to requests for snapshot images received from a Web browser.
External console	A console on which a Web browser is used to display snapshot images.

Related topics

- Manual *Hitachi Compute Blade Logical VGA Snapshot*
- Manual *HVM Management Command (HvmSh) Operation Guide*

Viewing the LPAR manager system logs

The LPAR manager information of operations and errors, you will be able to get from LPAR manager system logs, you can view the LPAR manager system log. You can use the Web console, or the LPAR manager screen to view the LPAR manager system logs.

Using the Web console to view the LPAR manager system logs

1. From the global task bar of the Web console, select the **Resources** tab. In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the target server blade. In the application area, the **Server Blade n Information** view is displayed. The variable n represents a unique number that identifies the server blade.
3. In the **Server Blade n Information** view, select the **LPAR Manager** tab. In the **Edit** menu, select **Show LP system logs**.

The **LP system logs** dialog box appears, and view to LPAR manager system logs.

Using the LPAR manager screen to view the LPAR manager system logs

1. Start the OS console and then, **LP Menu** screen.
2. Move to the **LP system logs** screen. In the **LP system logs** screen, align the cursor with the title of LPAR manager system log and press the **Enter** key.

Related topics

- [LP System Logs screen on page 10-89](#)

Collecting audit logs

You can use collected audit logs to detect and investigate unauthorized operations using LPAR manager. Audit logs record the operation history for LPAR manager, and are transferred to an external syslog server.

The versions that support audit logs are as follows:

Table 8-11 Versions that support audit logs

Item	Version
Management module firmware	A0145 or later ¹
LPAR manager firmware	02-40 or later
HvmSh	9.00 or later
Notes: 1. To set the collection target to Authentication and modification , the management module firmware version must be A0165 or later.	

Support requirements for collecting audit logs system

The following system requirements apply to the communication or the syslog server to which audit logs are transferred:

Table 8-12 Support requirements for audit log transfer

Item	Scope of support
Syslog server type	Syslog servers that support the RFC5424 format
Number of syslog servers	Maximum of two syslog servers. The same auditing log will be sent to all registered syslog servers.
Communication protocol	<ul style="list-style-type: none">• UDP

Item	Scope of support
	<ul style="list-style-type: none"> TLS v1.0-v1.2
Collection target	<p>Select Authentication or Authentication and modification.</p> <ul style="list-style-type: none"> Authentication (LPAR manager firmware version 02-40 or later) Logs for user authentication will be collected. Authentication and modification (LPAR manager firmware version 02-55 or later) In addition to the logs for user authentication, the logs for user operations to change the settings or status of LPAR manager or of an LPAR will be collected.

Format of audit logs

The table below shows the information and messages output to audit logs.

Table 8-13 Output items for audit logs

Item	Description
Priority	<p>The value according to the severity of each audit event is output to the format of <code><value></code>.</p> <ul style="list-style-type: none"> For an operation failure, <code><13></code> is output. This means <code>facility=user, severity=notice</code>. For other audit events, <code><14></code> is displayed. This means <code>facility=user, severity=info</code>.
Syslog version	"1" is always output.
Date and time	The date and time when the processing request was received is output to the format of <code>YYYY-MM-DDThh:mm:ss.sTZD</code> .
Host information	<p>The LP IP address is output.</p> <ul style="list-style-type: none"> If an IPv4 address is set, the IPv4 address takes priority over the IPv6 address, and the IPv4 address is output. If only an IPv6 address is specified, the IPv6 static address is output.
Application information	"LP" is output.
Process ID	"-" is always output.
Message ID	An audit log ID ¹ defined by LPAR manager is output.
Structure data section	"-" is always output.
Message	<p>The log information for the performed operation is output.</p> <p>For details, see Table 8-14 Content of messages in audit logs on page 8-33.</p>
Notes:	

Item	Description
1.	The value varies depending on the event. For details, see Audit log messages on page 11-34 .

The messages output to audit logs are composed of the information items below. Each information item in a message is separated by a comma (,).

Table 8-14 Content of messages in audit logs

Item	Description
Common identifier	"CELFSS" is always output.
Common specifications revision number	"2.0" is always output.
Serial message number	The serial number (1 to 9999999999) of the audit log message is output. <ul style="list-style-type: none"> 1 is assigned to the log information collected immediately after LPAR manager starts. The serial number counter is reset to 1 when LPAR manager is restarted or shutdown.
Message ID	An audit log ID ¹ defined by LPAR manager is output.
Date and time	The date and time when the processing request was received is output in the formation of YYYY-MM-DDThh:mm:ss.sTZD.
Component name and process name	"LP" is output.
Host name	The LP IP address is output. <ul style="list-style-type: none"> If an IPv4 address is set, the IPv4 address takes priority over the IPv6 address, and the IPv4 address is output. If only an IPv6 address is specified, the IPv6 static address is output.
Audit event type	The type of the audit event, such as viewing of information or change of settings, is output. <ul style="list-style-type: none"> Authentication: User authentication StartStop: Starting, restarting, and stopping LPAR manager or LPARs ConfigurationAccess: Configuration changes to LPAR manager or LPARs (including configuration changes made along with status changes) Maintenance: Operations other than the above
Result of the audit event	One of the following values is output. <ul style="list-style-type: none"> Success: The operation finished successfully. Failed: The operation failed.
Result subject identification information for the audit event	The LPAR manager account name is output in the format of uid=xxx. <ul style="list-style-type: none"> If the LPAR manager account name consists of 32 or more characters, the first 31 characters are output.

Item	Description
	<ul style="list-style-type: none"> If the LPAR manager account name contains a prohibited character, the character is replaced with an asterisk (*). <p>Nothing is output when an attempt to login fails or when operations are performed on LPAR manager by using HVM Navigator or HvmSh while the user authentication status is invalid. When performing operations on LPAR manager by using the Web console, HCSM, or LPAR manager screen, <code>uid=ManagementModuleUser</code> is output.</p>
Model name and serial number of the hardware	The serial number of the primary server blade is output.
Hardware component identification information	The type of the server chassis is output.
Location identification information	Information about the slot where the primary server blade is installed is output.
Fully qualified domain name	(No value is output.)
Redundancy identification information	(No value is output.)
Agent information	(No value is output.)
Request source host	<ul style="list-style-type: none"> If the collection target is Authentication, no information is output. If the collection target is Authentication and modification, the IP address of the management module or management server from which operations were performed will be output in the format <code>from=xxx</code>.
Request source port number	(No value is output.)
Request destination host name	(No value is output.)
Request destination port number	(No value is output.)
Batch operation identifier	(No value is output.)
Log type information	(No value is output.)
Application identification information	<ul style="list-style-type: none"> If the collection target is Authentication, no information is output. If the collection target is Authentication and modification, the session number of the session to which the user is logged in will be output in the format <code>session=xxx</code>. (This information is output for users who successfully logged in.)

Item	Description
Message	<p>The details of the audit event¹ are output by being enclosed in double quotation marks (").</p> <p>If the message text exceeds 255 characters, the text after the 250th letter will be omitted and replaced with the following characters in the given order: a space, three periods (.), and a double quotation mark (").</p>
<p>Notes:</p> <ol style="list-style-type: none"> The value varies depending on the event. For details, see Audit log messages on page 11-34. 	

Enabling the collection of audit logs

This subsection describes how to configure settings so that the audit logs for LPAR manager can be collected. You can use the management module or HVM management command to enable or disable the collection of audit logs.

You must also have the LPAR manager security permission if you want to perform this operations.

Enabling the collection of audit logs by using the Web console

Enable the collection of audit logs. Audit logs are output to the specified syslog server. As a result, you also need to specify the output destination syslog server and the transfer protocol.

- In the global tab of the web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
- In the **Modules** tree view, select the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
- In the **Server Blade *n* Information** view, select the **LPAR manager** tab. From the **Edit** button, execute **Edit syslog transfer settings**.
The **Syslog Transfer Settings** dialog box appears.
- Set the following items:
 - Syslog transfer function: Enable**
 - Target to log: Authentication** or **Authentication and modification**
 - Syslog server1, Syslog server2:** Set the IP address (IPv4 or IPv6) and host name for the syslog server.
 - Port number:** Set the port number used to connect to the syslog server in the range from 1 to 65535.
You need to change this setting only when a port number other than the default port number (6514) must be used.

- **Transfer protocol:** Set the transfer protocol (**TLS** or **UDP**) used for communications with the syslog server.
 - **TLS version:** Set the TLS version used for communications with the syslog server.
 - **Server certificate verification:** Specify whether LPAR manager is used to verify the certificate of the syslog server.
5. Click the **Confirm** button.

Enabling the collection of audit logs by using the HVM management command (HvmSh)

To use the HVM management command (HvmSh) to enable the collection of audit logs, execute the `opr AuditLogConfig` command.

To register the certificate of the communication destination or the certificate of the certificate authority, execute the `opr HvmClientCertificateRegist` command.

Specifying the DNS server

This section describes how to specify the DNS server that is accessed to resolve names including the name of an external server to be accessed. The following list of program versions support DNS servers.

Table 8-15 Firmware that supports DNS servers

Item	Version
Management module firmware	A0145 or later
LPAR manager firmware	02-40 or later
HvmSh command	9.00 or later

Specifying the DNS server by using the Web console

To do this, you must be logged in to the management module.

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR manager** tab. From the **Edit** button, execute **Edit DNS settings**.
The **DNS Settings** dialog box appears.
4. Specify the IP address of the DNS server, and then click the **Confirm** button.

You can specify the IPv4 or IPv6 address.

Setting DNS server by using the HVM management command (HvmSh)

To use the HVM management command (HvmSh) to setting DNS server, execute the `opr SystemConfigDNS` command.

Maintaining LPAR manager and LPARs

This chapter describes the functionality for maintaining LPAR manager and LPARs.

- ☐ [Migration between basic and LPAR manager environments](#)
- ☐ [Upgrading LPAR manager licenses](#)
- ☐ [LPAR manager security](#)
- ☐ [Collecting a memory dump of a guest OS](#)
- ☐ [Collecting LPAR manager failure information from the Web console](#)
- ☐ [Collecting LPAR manager dumps](#)
- ☐ [LPAR Migration](#)
- ☐ [Safe mode](#)
- ☐ [Collecting SYS2 dump files](#)

Migration between basic and LPAR manager environments

This section describes migration from a basic environment (Basic mode) to an LPAR manager environment (LP mode), and vice-versa.

Settings and items to be confirmed during migration from Basic mode to LP mode

The following table describes the settings and items to be confirmed during migration from Basic mode to LP mode.

Table 9-1 Settings during migration from Basic mode to LP mode

Item	Setting or confirmation item	
	Prior to migration	After migration
Guest OS	Remove IP address (Windows only)	Set IP address (Windows only)
	--	Install drivers
	--	Configure teaming/bonding
Server blade	Configure UEFI ¹	--
	Set LP mode ¹	--
	--	LPAR manager settings
Storage	--	Configure WWPN/WWNN
Notes:		
1. For details, see the manual <i>Hitachi Compute Blade 2500 Series Getting Started Guide</i> , or the manual <i>Hitachi Compute Blade 2500 Series UEFI Setup Guide</i> .		

Settings and items to be confirmed during migration from LP mode to Basic mode

The following table describes the settings and items to be confirmed during migration from LP mode to Basic mode.

Table 9-2 Settings during migration from LP mode to Basic mode

Item	Setting or confirmation item	
	Prior to migration	After migration
Guest OS	Remove IP address (Windows only)	Set IP address (Windows only)
	--	Install drivers
	--	Configure teaming/bonding
Server blade	Configure UEFI ¹	--

Item	Setting or confirmation item	
	Prior to migration	After migration
	Set Basic mode ¹	--
Storage	--	Configure WWPN/WWNN
Notes:		
1. For details, see the manual <i>Hitachi Compute Blade 2500 Series Getting Started Guide</i> , or the manual <i>Hitachi Compute Blade 2500 Series UEFI Setup Guide</i> .		

Notes on migration between Basic mode and LP mode

- In a Windows environment in which the NIC is assigned a static IP address, if you perform migration between Basic mode and LP mode, an IP address remains assigned to the old MAC address. As a result, a conflict error occurs when you attempt to assign the IP address again. For this reason, you need to remove the IP address before starting the migration process.
- The NIC types and MAC addresses in LP mode differ from those in Basic mode. Consequently, you need to install drivers when migrating the system for the first time. You also need to change the configuration of the middleware used to identify MAC addresses. For details about how to do so, see the documentation for the middleware you are using.
- The WWPN and WWNN of the HBA differ between the LPAR manager and basic environments. For this reason, you need to change the SAN security configuration on the storage side. For details about how to change the SAN security configuration, see the documentation for the storage product.

Upgrading LPAR manager licenses

From the Web console, change the LPAR manager model to Advanced or Enterprise.

To upgrade your LPAR manager license, you need to request an LPAR manager license key and apply it to LPAR manager in the Web console.

The server blade must be off before you can register an LPAR manager license key.

Requesting an LPAR manager license key

The following describes how to request a license key for LPAR manager.

Procedure for requesting an LPAR manager license key

For obtaining LPAR manager License Keys, contact <contact information>.

Registering LPAR manager license keys directly

This section describes how to register a license key for LPAR manager by entering it directly from the Web console.

To register a license key by registering it directly from the Web console:

1. From the **Systems** tree view in the **Resources** tab, select **LP license**.
2. Select the applicable server blade, and then click **Register LP License Key**.
3. In the **Change LP model** dialog box, select the **Direct input** radio button in the **License key** area, enter the license key in the text box, and then click **Confirm**.
4. Check the details of the license key, and then click **OK**.

Registering LPAR manager license keys by loading a license key file

The following describes how to register an LPAR manager license key by loading a license key file from the Web console.

To register an LPAR manager license by loading a license key file from the Web console:

1. From the **Systems** tree view in the **Resources** tab, select **LP license**.
2. Select the applicable server blade, and then click **Register LP License Key**.
3. In the **Change LP model** dialog box, select the **File name** radio button in the **License key** area, and click **Browse**.
4. Specify the LPAR manager license key file, and click **Confirm**.
5. Check the details of the license key, and then click **OK**.

Notes on temporary LPAR manager licenses

- LPAR manager system log messages and HCSM alert messages are output when an expiration date for a temporary LPAR manager license is near or has passed.
For details about the HCSM alert messages, see the manual *Hitachi Compute Blade 2500 Series Management Module User Guide*.
- If the license expires while LPAR manager is operating, the following operations are suppressed:
 - Operations to activate LPARs
 - OS startup after reactivating LPARs
 - OS startup after restarting OSs
 - Operations that include the operation to activate LPARs (Boot order configuration and boot device acquisition)
- If the expiration date has already passed when LPAR manager starts, LPAR manager will operate as the Essential model.

- If the license has expired, register a string of 49 characters (beginning with "0" and followed by the temporary LPAR manager license key of 48 characters) as the LPAR manager license key, so that the server blade can be updated to one with a permanent Essential license.
- When a temporary Enterprise license is additionally registered for the server blade for which a permanent Advanced license is registered, the permanent Advanced license is overwritten. Register the permanent Advanced license key again to return the server blade to the permanent Advanced license.
To register a new license, confirm in advance that a registered license key already exists.
- Depending on the type of a license key that is registered, some of the functions might become unavailable due to downgrades of the LPAR manager model (see "Functional differences depending on LPAR manager licenses"). In such a case, the LPAR settings for these functions are changed to the default.
Therefore, backup the LPAR manager configuration information before registering a license key, and then restore the LPAR manager configuration information after the license is registered.
- The time settings of the management module and LPAR manager must be synchronized. If the time settings do not match, LPAR manager might recognize an expiration date earlier than the actual expiration date.

LPAR manager security

Transport Layer Security (TLS) and certificates provide the basis of LPAR manager security.

Certificates have two roles:

- Authenticating ownership of the certificate
- Encrypting communication



Note: To perform operations related to LPAR manager security, you need the LPAR manager security permission.

Related topics

- [LPAR manager security permission on page 7-6](#)
- *Manual HVM Management Command (HvmSh) Operation Guide*

Using certificates in LPAR manager

LPAR manager can use a server certificate to authenticate itself, and can authenticate the systems with which it communicates (hereafter other systems) based on their certificates.

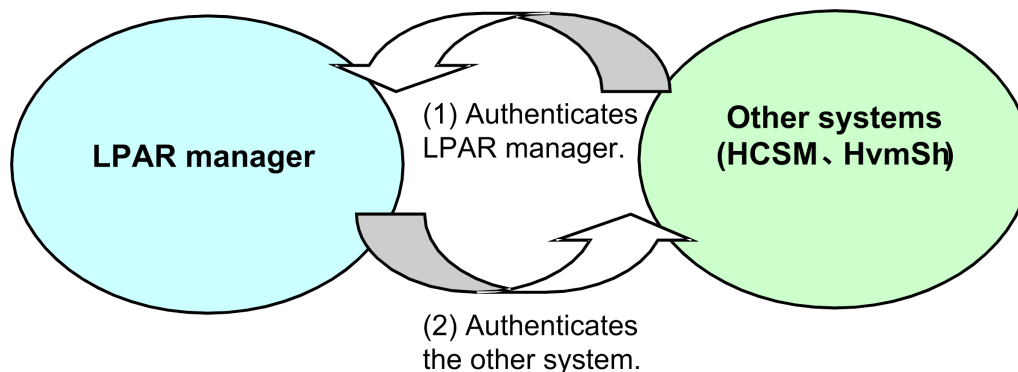


Figure 9-1 LPAR manager authentication

Server certificate issued by LPAR manager

When another system uses TLS to connect to LPAR manager, LPAR manager presents its server certificate to the other system. The other system can then authenticate LPAR manager by validating this server certificate.

LPAR manager server certificates

LPAR manager can use a self-signed certificate as its server certificate, or a certificate signed by a certificate authority (CA). If other systems will authenticate LPAR manager using its server certificate, register the server certificate on the other system. For details about how to register certificates, see the documentation for the other system. Note that there might be a delay of approximately 30 seconds before the server certificate takes effect. During this period, the other system might be unable to communicate with LPAR manager.

Systems that can use LPAR manager server certificates

The following systems can use LPAR manager server certificates:

- HCSM
- HvmSh

Server certificate parameters

The following table describes the parameters of LPAR manager server certificates.

Table 9-3 Server certificate parameters

Item	Description
Public key algorithm, bit-length	RSA (2,048 bits)
Signature algorithm	SHA-2, etc. ⁷
Format of certificates that can be imported	PEM / DER
Certificate format in downloading	DER
Format of CSRs that can be created	PEM / DER

Item	Description
Information about the subject that can be included in the certificate and CSR	Common name (CN): Maximum of 60 characters ^{1, 2}
	Country (C): Maximum of two characters ³
	State or province (ST): Maximum of 60 characters ⁴
	Locality (L): Maximum of 60 characters ⁴
	Organization (O): Maximum of 60 characters ⁴
	Organizational unit (OU): Maximum of 60 characters ⁴
	Email address: Maximum of 60 characters ⁵
	DN qualifier: Maximum of 60 characters ⁴
	Last name: Maximum of 60 characters ⁴
	First name: Maximum of 60 characters ⁴
	Initials: Maximum of 30 characters ⁴
	Unstructured name: Maximum of 60 characters ^{4, 6}
	Challenge password: Maximum of 30 characters ^{4, 6}
Notes: <ol style="list-style-type: none"> 1. This must be entered in the certificates. 2. Can contain alphanumeric characters, hyphens (-), and commas (,). 3. Can contain upper case alphabetic characters. 4. Can contain alphanumeric characters, hyphens (-), periods (.), plus signs (+), single quotation marks ('), parentheses (()), forward slashes (/), colons (:), equals signs (=), question marks (?), and spaces. 5. You can enter ASCII characters that can be displayed. 6. This can be entered only when creating a CSR. 7. You can check the signature algorithm by using the <code>get HvmServerCertificate</code> command of the HvmSh command. 	

Creating signed server certificates

You can create a simple authentication system that uses the self-signed certificate that is created when LPAR manager starts the first time. However,

you can create a more secure authentication system that uses signed server certificates.

Creating signed server certificates by using the Web console

To do this, you must be logged in to the management module.

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. From the Edit button, execute **Show certificate settings**.
The **Certificate Settings** dialog box appears.
4. From the Certificate drop-down list box, select **Create CSR**.
 - The common name (CN) field in the CSR must uniquely identify the instance of LPAR manager.
 - When a CSR is created, a private key that corresponds to the CSR is created in LPAR manager. You cannot create only a private key.
 - The private key and server certificate that were just created are not used until you register the signed certificate in a subsequent step. Until you register the certificate, the previous private key and server certificate remain in effect.
5. Obtain a signed server certificate by submitting the CSR to a certificate authority.
6. From the Certificate drop-down list box, select **Import LP certificate**.
You can register the signed server certificate on the LPAR manager that created the CSR. You cannot use the signed server certificate on other LPAR manager.

Creating signed server certificates by using an HVM management command (HvmSh)

1. To create a CSR, use the `opr HvmCSR` command.
 - The common name (CN) field in the CSR must uniquely identify the instance of LPAR manager.
 - When a CSR is created, a private key that corresponds to the CSR is created in LPAR manager. You cannot create only a private key.
 - The private key and server certificate that were just created are not used until you register the signed certificate in a subsequent step. Until you register the certificate, the previous private key and server certificate remain in effect.

After creating the CSR, save the LPAR manager configuration information by executing the `opr HvmSecureCmmConfigSave` command or the `opr SaveConfig` command.

2. Obtain a signed server certificate by submitting the CSR to a certificate authority.

3. To register the signed certificate with LPAR manager, use the `opr HvmCACertificateRegist` command.

You can register the signed server certificate on the LPAR manager that created the CSR. You cannot use the signed server certificate on other LPAR manager.

After registering the signed server certificate, save the LPAR manager configuration information by executing the `opr HvmSecureCmmConfigSave` command or the `opr SaveConfig` command.

Authenticating other systems

When LPAR manager uses TLS to connect to another system, it can authenticate the other system by verifying its security certificate.

To authenticate another system, you need to register with LPAR manager the certificate of the other system or the certificate of the authority that signed the certificate, and enable the certificate verification functionality.

Authenticating other systems by using the Web console

To do this, you must be logged in to the management module.

1. In the global tab of the Web console, select the **Resources** tab.
In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the icon of the target server blade.
In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. From the Edit button, execute **Show certificate settings**.
The **Certificate Settings** dialog box appears.
4. From the Certificate drop-down list box, select **Import certificate**.

Authenticating other systems by using the HVM management command (HvmSh)

To register the certificate, use the `opr HvmClientCertificateRegist` command.

To enable certificate verification, use the `opr HvmIfSecureVerify` command respectively.

To enable certificate verification of a syslog server, use the `opr AuditLogConfig` command.

After registering the certificate, save the LPAR manager configuration information by executing the `opr HvmSecureCmmConfigSave` command or the `opr SaveConfig` command.

Systems LPAR manager can authenticate

LPAR manager can authenticate the following systems:

- HCSM (alert notification)
- LDAP server (LDAP authentication)
- syslog server (audit log)

Related topics

- [Authenticating LPAR manager users on page 7-9](#)
- [Collecting audit logs on page 8-31](#)
- Manual *Hitachi Compute Blade 2500 Series Management Module User Guide*

About security on LPAR manager features and tools that used management network

This section describes the security measures of LPAR manager features and tools that used the management network.

The following shows the major LPAR manager features and tools that used the management network:

- HCSM
- HVM Navigator
- Virtual COM Console
- Logical VGA Snapshot
- HvmSh
- LDAP authentication
- RADIUS authentication
- Audit log

Security strength

You can enhance the security strength, LPAR manager supports communication method in the following:

- Communication in cleartext is prohibited.
- For encrypted communication, only encryption algorithms with high security strength are used.

LPAR manager features and tools that used management network and security strength

In LPAR manager, you can change the security strength of the LPAR manager features and tools listed in the table below. The following table describes the protocols and encryption methods used by LPAR manager functionality under each security strength setting.

The following table describes the protocols that can be used with LPAR manager.

Table 9-4 LPAR manager features and tools that used management network and security strength

Feature or tool	Options	Available protocols	
		plaintext	encryption
HCSM (LPAR migration)	Default	TCP	TLS v1.0-v1.2
	High	-	TLS v1.2
HCSM (Alert transmission)	Default	-	<ul style="list-style-type: none">• SSL v3.0¹• TLS v1.0-v1.2
	High	-	TLS v1.2
HVM Navigator	Default	TCP	-
	High	-	TLS v1.2
HvmSh	Default	<ul style="list-style-type: none">• UDP• TCP	TLS v1.0-v1.2
	High	-	TLS v1.2
Virtual COM Console	Telnet	Telnet	-
	SSH	-	SSH v2
Logical VGA Snapshot	Default	-	-
	High	-	<ul style="list-style-type: none">• SSL v3.0¹• TLS v1.0-v1.2
LDAP authentication	TLS1.0	-	TLS v1.0-v1.2
	TLS1.2	-	TLS v1.2
RADIUS authentication	-	UDP	-
Audit log	UDP	UDP	-
	TLS1.0	-	TLS v1.0-v1.2
	TLS1.2	-	TLS v1.2
Management module communication	-	Encryption is executed by TLS v1.2 (same as "High" level) or AES-128.	
Legend: -: Not applicable Notes: 1. LPAR manager firmware versions 02-20 or later do not allow using SSL v3.0. For the firmware of those versions, select TLS v1.0 or later in HCSM or web browser optional setting.			



Note:

- To use HVM Navigator via a plain text connection, set the HCSM and HvmSh using the management network to "Default".

- If you set HCSM and HvmSh using the management network to "High", also specify the setting so that HVM Navigator uses TLS.

Setting the security strength

You can set the security strength by using the Web console and the HVM management command (HvmSh). It can take approximately 30 seconds for changes to the security strength to take effect. During this period, the other system might be unable to communicate with LPAR manager.

Encryption algorithms supported by LPAR manager

The tables below list the encryption algorithms supported by LPAR manager.

- SSL/TLS

Table 9-5 Cipher suite and security strength

Cipher suite	Security strength	
	Default	High
TLS_RSA_WITH_AES_128_CBC_SHA	Y	N
TLS_RSA_WITH_AES_128_CBC_SHA256	Y	Y
TLS_RSA_WITH_AES_256_CBC_SHA256	Y	Y
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	Y	N
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Y	N
TLS_DHE_DSS_AES_128_CBC_SHA1	Y ¹	N
TLS_DHE_DSS_AES_256_CBC_SHA1	Y ¹	N
TLS_DHE_DSS_AES_128_CBC_SHA256	Y ¹	N
TLS_DHE_DSS_AES_256_CBC_SHA256	Y ¹	N
TLS_RSA_AES_256_CBC_SHA1	Y ¹	N
Legend: Y: Supported N: Not supported Notes: 1. This cipher suite is used for communications with the syslog server only if "TLS v1.0-v1.2" is specified for the communication protocol for audit logs.		

Table 9-6 Security strength of server certificates (public-key algorithm)

Server certificate (public-key algorithm)	Security strength	
	Default	High
RSA-2048 verification	Y	Y

Server certificate (public-key algorithm)	Security strength	
	Default	High
RSA-2048 creation	Y	Y
Legend: Y: Supported		

Table 9-7 Security strength of server certificates (signature algorithm)

Server certificate (signature algorithm)	Security strength	
	Default	High
SHA-256 verification	Y	Y
SHA-256 creation	Y	Y
Legend: Y: Supported		

- SSH v2

Table 9-8 Security strength for SSH v2

Item	Security strength
Encryption method	3des-cbc
	aes128-cbc
	aes192-cbc
	aes256-cbc
	aes128-ctr
	aes192-ctr
	aes256-ctr
Message authentication	hmac-sha1
	hmac-sha1-96
	hmac-sha2-256
	hmac-sha2-512
Key exchange	diffie-hellman-group14-sha1
	diffie-hellman-group-exchange-sha1
	diffie-hellman-group-exchange-sha256
Host key	RSA 2048

Collecting a memory dump of a guest OS

Guest memory dump collection

The functionality that allows you to collect a memory dump even if the nature of a failure occurred on a logical server prevents the guest OS from collecting OS memory data (a memory dump) is called a guest memory dump.

When you execute the guest memory dump collection command, a memory dump of the specified guest OS (LPAR) is collected by LPAR manager and transferred to an external FTP server. This command is part of the HVM management command (HvmSh).

Specifications of guest memory dump collection command

The following table describes the specifications of the guest memory dump collection command.

Table 9-9 Guest memory dump collection command

Item	Description
Target of dump collection	The command can collect LPAR memory dumps (only when the guest OS is Linux)
Dump size (scope of dump collection)	Of the memory areas allocated to the target LPAR, the command collects data from the following three memory areas that are used by the OS (you cannot specify a memory range in the LPAR): <ul style="list-style-type: none">DOS region: 00_0000_0000 to 00_0009_FFFFLow Memory: 00_0010_0000 to 00_7FFF_FFFFHigh Memory: 01_0000_0000 to [MMCFG] - 1 This is the same memory range as Niko2Dump in Basic mode.
User operations	On the LPAR manager management server, execute the guest memory dump collection command, which is an HVM management command.
Output destination	The memory dump is output to the external FTP server specified for the guest memory dump collection command. The memory dump also can be output to the server that executed the guest memory dump collection command.
Dump data transfer method	Dump data between LPAR manager and an external FTP server is transferred as a file by using FTP. The management path is used for the transfer.
Format of dump collection data	Conforms to Niko2Dump format
Format of dump output files	Dump output files are binary format files based on the format of the dump collection data.
File names of dump output files	<code>gmdP#L#-YYMMDD-hhmmss-<i>nnn</i>.dat</code> <i>P#</i> : Partition number <i>L#</i> : LPAR number

Item		Description
		<p><i>YYMMDD</i>: Collection date (YY: Year, MM: Month, DD: Day)</p> <p><i>hhmmss</i>: Collection time (24 hour clock. hh: hour, mm: minutes, ss: seconds)</p> <p><i>nnn</i>: Serial number (relevant when data spans more than one file. The serial number can contain any number of digits and is not padded with 0s).</p> <p>The collection date and time are based on the LPAR manager system time.</p>
Information input by user		<p>When executing the command to initiate the guest memory dump, enter the following information:</p> <ul style="list-style-type: none"> • LPAR manager IP address • LPAR number of the LPAR for which a guest memory dump is to be collected • IP address of the external FTP server • User ID for the external FTP server • Password for the external FTP server • Path to which the dump file is to be output on the external FTP server (a directory path under FTP) <p>Note that if the user ID or password contains a symbol, dump collection might fail.</p>
Command functionality	Start operation	<p>Starts the memory dump.</p> <p>To avoid a situation in which the memory data changes while the dump is being collected, all logical processors of the LPAR stop automatically when the dump process starts.</p> <p>Note that the logical processors remain stopped after the dump process has finished.</p>
	Stop operation	<p>Stops the memory dump.</p> <p>Note that the logical processors that automatically stopped when you started the memory dump do not restart automatically.</p>
	Progress indication	<p>Displays the progress of the memory dump collection process. The displayed information is as follows:</p> <ul style="list-style-type: none"> • Total volume, transferred volume, percent transferred (transferred volume/total volume)
Maximum concurrent collection		<p>One LPAR per instance of LPAR manager.</p> <p>LPAR manager ignores further requests for dump collection once collection is in progress, even if the request pertains to another LPAR in the same LPAR manager.</p>
Collection conditions		<p>The following condition must be met to collect a guest memory dump:</p> <ul style="list-style-type: none"> • - The target LPAR is activated.
Guest software operation		<p>A guest memory dump can be collected regardless of the operating status of the guest software. For example, if a failure that occurs while the guest software is running prevents the</p>

Item	Description
	software from continuing processing, you can still collect a memory dump.

Executing the guest memory dump collection command

Before using the guest memory dump collection command, you need to know how to use the HVM management command. For a basic overview of how to use this command, see the manual *HVM Management Command (HvmSh) Operation Guide*. For details about how to use commands related to the guest memory dump functionality in LPAR manager management, see Starting Guest Memory Dump, Stopping Guest Memory Dump, and Acquiring Guest Memory Dump Progress under LPAR manager Interface Reference in the manual *HVM Management Command (HvmSh) Operation Guide*.

Notes on using the guest memory dump collection command

Note the following when using the guest memory dump collection command:

- All logical processors of the LPAR stop when you initiate the dump process, and related logical servers do not automatically resume processing when the dump process has finished. For this reason, you should only acquire a memory dump if the nature of the failure means that the logical server cannot continue processing (for example, when the failure is in the logical server itself).
- After collecting a guest memory dump of an LPAR, to start operations of the LPAR, reactivate or deactivate the LPAR, activate it, and then restart the guest OS.
- If you deactivate or reactivate the target LPAR or perform LPAR reassignment operation while collecting a guest memory dump, the operation takes priority and the guest memory data is not retained. This means that the guest memory dump can no longer be collected, and the collection process is canceled. Do not deactivate or reactivate the target LPAR and do not perform LPAR reassignment operation while collecting a guest memory dump.
- After initiating a memory dump, you can continue to use LPARs other than the one for which the memory dump is being collected. However, the network performance of LPARs that use shared NICs in the network segment to which the LPAR manager management NIC belongs might be affected.
- If you perform a Force Recovery operation on the System Service State screen, which is one of the LPAR manager screens, while a guest memory dump is being collected, the dump collection process is canceled.
- If the processing that automatically stops the logical processors of the LPAR fails before guest memory dump collection, the dump collection process is canceled. At this point, the LPAR is forcibly deactivated. If deactivating the LPAR fails, the LPAR is blocked. If this occurs, contact your reseller or maintenance personnel.

- If an unrecoverable failure occurs in LPAR manager while a guest memory dump is being collected, the dump collection process is canceled. If this occurs, contact your reseller or maintenance personnel.
- If a failure occurs in LPAR manager Assist while a guest memory dump is being collected, the dump collection process might be canceled. If this occurs, contact your reseller or maintenance personnel.
- If a network communication failure occurs between LPAR manager and the FTP server while a guest memory dump is being collected, the dump collection process is canceled. In this case, check the network configuration between LPAR manager and the FTP server. If you are unable to resolve the problem, make sure that the FTP software on the external FTP server is operating correctly. If you are still unable to resolve the problem, contact your reseller or maintenance personnel.
- If you perform a guest memory dump collection and a Dump operation from the Front Panel screen to collect a guest OS dump on the same LPAR at the same time, the guest memory dump collection process stops the logical processors of the LPAR. Because this stops all processing by the guest OS, the Dump operation initiated from the Front Panel screen fails. The guest memory dump will be collected in the usual way. You can avoid this issue by following the procedure below:
 - a. If you notice that the guest OS is behaving abnormally and decide to collect dump information, first perform a Dump operation on the Front Panel screen to collect a guest OS dump.
 - b. If collection of the guest OS dump fails, use the guest memory collection command to collect a guest memory dump.
- The transfer data to an FTP server is supported only an IP address in IPv4 format.

Collecting LPAR manager failure information from the Web console

This section describes how to collect failure information from LPAR manager. You need to collect failure information when a fault occurs in the equipment you are using.

This process results in the collection of an LPAR manager dump that you can use to diagnose the failure. Under normal operation, it is not necessary to collect LPAR manager dumps.

To collect an LPAR manager dump from the Web console:

1. From the **Modules** tree view in the **Resources** tab, select the target server blade.
2. On the **LPAR** tab, click **Collect LP dump log** in the bottom right **Action** box, and then click **OK**.
When the processing is complete, the LPAR manager dump data is downloaded as a file.

**Note:**

- Although you can download the LPAR manager dump log as a file, you cannot save it in the management module.

To retrieve the LPAR manager dump from the Web console:

1. In the **General Tasks** panel, click **Dump Log**.
2. Click **Download** to save the dump log.
The dump file is downloaded.

Collecting LPAR manager dumps

This section describes the collection commands for LPAR manager dumps.

Overview of LPAR manager dump collection

LPAR manager dumps are collected by LPAR manager dump collection commands. These commands are part of the HVM management command (HvmSh).

There are two LPAR manager dump collection commands:

- The `HvmDumpToSvp` command, which transfers the dump data to the management module
This command has the same functionality as the **Take LP Dump** option on the LP Options screen.
- The `TakeHvmDump` command, which transfers the dump data to the external FTP server

This command transfers the collected LPAR manager dump data to the specified FTP server where it is saved as a file.

Related topics

- [LP Options screen on page 10-74](#)

Specifications of LPAR manager dump collection commands

The following table describes the specifications of the LPAR manager dump collection commands.

Table 9-10 LPAR manager dump collection commands

Item	Description
Target of dump collection	LPAR manager
Dump size	Maximum 16 MB (the size of two dump files compressed by GZIP)

Item	Description
User operations	The user executes the LPAR manager dump collection command on the LPAR manager management server.
Output destination	An external FTP server specified in the LPAR manager dump collection command (can be the server on which the command is executed)
Dump data transfer method	Dump data is transferred from LPAR manager to the external FTP server over the management LAN. A GZIP compressed dump data file is created in LPAR manager and transferred to the external FTP server using the FTP protocol.
Format of dump collection data	Same as existing LPAR manager dump format
Format of dump output files	GZIP format Dump data is output to two GZIP-compressed files with the existing 128-byte dump header appended to the compressed data.
File names of dump output files	<p>First dump file: <code>hvmddump-yyyymmdd-hhmmss-01</code></p> <p>Second dump file: <code>hvmddump-yyyymmdd-hhmmss-02</code></p> <p><i>yyyymmdd</i>: Collection date (yyyy Year, mm: Month, dd: Day)</p> <p><i>hhmmss</i>: Collection time (hh: hour, mm: minutes, ss: seconds)</p> <p>Note that the first and second files have the same collection date and time.</p>
Information input by user	<p>When executing the command to collect an LPAR manager dump, enter the following information:</p> <ul style="list-style-type: none"> • LPAR manager IP address • IP address of the external FTP server • User ID for the external FTP server • Password for the external FTP server • Path to which the dump file is to be output on the external FTP server (a directory path under FTP) <p>Note that if the user ID or password contains a symbol, dump collection might fail.</p>
Maximum concurrent collection	1 (if LPAR manager receives another request to collect dump data while a memory dump is in progress, the request is ignored)
Collection conditions	Aside from the circumstances described in the notes below, an LPAR manager dump can be collected at any time.

Executing the LPAR manager dump collection commands

Before using the LPAR manager dump collection command, you need a basic understanding of using LPAR manager for management. For a basic overview, see the manual *HVM Management Command (HvmSh) Operation Guide*. For details about how to use LPAR manager dump collection, see "Collecting LPAR manager dump data" in "LPAR manager Interface Individual Specifications" in the manual *HVM Management Command (HvmSh) Operation Guide*.

Notes on using the LPAR manager dump collection commands

Note the following when using LPAR manager dump collection commands:

- While an LPAR manager dump is being collected by the LPAR manager dump collection commands, you cannot initiate another LPAR manager dump through the LPAR manager screens or other means.
- If collection of an LPAR manager dump initiated by an on-screen operation or similar is in progress, you cannot use the LPAR manager dump collection commands to collect an LPAR manager dump.
- If an unrecoverable failure occurs in the LPAR manager that initiated LPAR manager dump collection, the dump collection process is canceled. If this occurs, contact your reseller or maintenance personnel.
- If a network communication failure occurs between LPAR manager and the FTP server while an LPAR manager dump is being collected, the dump collection process is canceled. In this case, check the network configuration between LPAR manager and the FTP server. If you are unable to resolve the problem, make sure that the FTP software on the external FTP server is operating correctly. If you are still unable to resolve the problem, contact your reseller or maintenance personnel.
- The transfer data to an FTP server is supported only an IP address in IPv4 format.

LPAR Migration

The LPAR migration functionality migrates an LPAR from the server blade on which it is currently running to another server blade.

For details about system requirements and notes, see the manual *Hitachi Compute Blade LPAR Migration Guide*.

For details about how to perform LPAR migration, see the manual *Hitachi Command Suite Compute Systems Manager User Guide* or the manual *Hitachi Compute Blade HVM Navigator User's Guide - Migration*.

Safe mode

When the LPAR manager fulfills the following conditions, the LPAR manager starts in safe mode that temporarily disables LPAR activation and saving configuration.

When the LPAR manager starts in safe mode, LPAR manager log messages and system logs (SEL) are output. Take measures according to their log messages.

Note that, when the LPAR manager starts in safe mode, the LPAR migration functionality is also disabled.

The conditions under which the LPAR manager starts in safe mode, and the operations that are disabled in safe mode are as follows.

Condition	Operation		Supported version
	LPAR activation	Saving configuration	
A NIC which is in dedicated mode and is assigned to an LPAR has been changed to shared mode since the NIC has been specified as an LPAR manager management NIC.	Disabled	Disabled	02-20 or higher
A NIC which is in shared mode and is assigned to LPARs has been changed to dedicated mode since some NICs which are in dedicated mode and are not assigned to any LPARs have been specified as LPAR manager management NICs and the number of NIC ports of NICs in shared mode exceeds the maximum number of NIC ports in shared mode.	Disabled	Disabled	02-20 or higher
The KeepConfig option is enabled and the LPAR manager cannot detect the physical processors, memory, or PCI devices that have been recorded in the LPAR manager configuration.	Enabled	Disabled	02-56 or higher

Checking whether LPAR manager is running in safe mode

You can use the Web console, the LPAR manager screen, or an HVM management command (HvmSh) to check whether LPAR manager is running in safe mode.

Using the Web console to confirm the safe mode status

1. From the global task bar of the Web console, select the **Resources** tab. In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the target server blade. In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. Check **LP condition** and **Condition detail**.
If LPAR manager is running in safe mode, "The LP is running in safe mode." is displayed.

Using the LPAR manager screen to confirm the safe mode status

In the LP Options screen, check the System Control - Safe Mode.

Using an HVM management command (HvmSh) to confirm the safe mode status

Execute the `get ConfigAll` command and check the contents of the `HVM_CONFIGURATION` record.

Related topics

- [System Service State screen on page 10-58](#)

Exiting safe mode

If LPAR manager is running in safe mode, you can use the Web console, the LPAR manager screen, or an HVM management command (HvmSh) to exit safe mode.

Using the Web console to exit safe mode

1. From the global task bar of the Web console, select the **Resources** tab. In the navigation area, the **Modules** tree view is displayed.
2. In the **Modules** tree view, select the target server blade. In the application area, the **Server Blade *n* Information** view is displayed. The variable *n* represents a unique number that identifies the server blade.
3. In the **Server Blade *n* Information** view, select the **LPAR Manager** tab. Click the **Exit safe mode** button. A confirmation dialog box appears. Respond appropriately to the message in the dialog box.

Using the LPAR manager screen to exit safe mode

In the System Control of the LP Options screen, exit safe mode.

Using an HVM management command (HvmSh) to exit safe mode

Execute the `set HvmOptions` command.

Related topics

- [LP Options screen on page 10-74](#)

Collecting SYS2 dump files

The SYS2 Dump is the function to collect detailed failure information when a failure occurs in the LPAR manager communication component and service control component (SYS2).

This function is disabled by default. Do not enable this function unless specifically instructed to do so.

Use an HVM management command to collect SYS2 dump files.

For details, see the manual *HVM Management Command (HvmSh) Operation Guide*.



Note:

- If a failure occurs in SYS2 when this function is enabled, the time length in which communications of shared NICs are suspended will be longer by up to one minute than when this function is disabled (default).
-

LPAR manager Screen

This chapter describes the configuration and items displayed on the LPAR manager screen. In addition, the configuration and items displayed on the sub-screens that open from the LPAR manager screen are also described.

- ☐ [Operations and roles of the keys used to manipulate the LPAR manager screen](#)
- ☐ [Names and usages of the LPAR manager screen](#)
- ☐ [LPAR manager Menu screen](#)
- ☐ [Logical Partition Configuration screen](#)
- ☐ [Logical Processor Configuration screen](#)
- ☐ [Physical Processor Configuration screen](#)
- ☐ [PCI Device Information screen](#)
- ☐ [PCI Device Assignment screen](#)
- ☐ [Virtual NIC Assignment screen](#)
- ☐ [Shared FC Assignment screen](#)
- ☐ [Allocated FC Information screen](#)
- ☐ [System Configuration screen](#)
- ☐ [System Service State screen](#)

- ☐ [Date and Time screen](#)
- ☐ [LP Options screen](#)
- ☐ [LPAR Usage screen](#)
- ☐ [Front Panel screen](#)
- ☐ [LP System Logs screen](#)
- ☐ [Firmware Version Information screen](#)
- ☐ [LPAR manager sub-screens](#)

Operations and roles of the keys used to manipulate the LPAR manager screen

To manipulate the LPAR manager screen, use the keyboard to enter information. The LPAR manager screen consists of screens and sub-screens. This section describes the keys that are common across the LPAR manager screens, and their functionality. Keys specific to a screen and their functionality are described in the topics section of the applicable screen.

Table 10-1 Operation keys on the LPAR manager screen

Key	Operation and role
The up, down, left, or right cursor key	Moves the cursor in the direction of the pressed key.
Tab	Moves the cursor from the current screen item to the next one.
Enter	Executes an item with the specified value. On a sub-screen, closes the sub-screen.
Esc	<ul style="list-style-type: none">For screens other than the LPAR manager Menu screen, returns to the LPAR manager Menu screen from the current screen.For a sub-screen, stops operation on the sub-screen, and closes it. Note that no operation is performed on the LPAR manager Menu screen.
PageUp, PageDown	These keys can be used on a screen that requires vertical movement, or on a sub-screen on which a value is selected. <ul style="list-style-type: none">Scrolls the screen upward or downward.On a sub-screen in which a value must be selected, select the maximum or minimum value.
F11, F12	On a screen that requires horizontal movement, scrolls the screen to the right or left.
Alt + t	Redraws the screen.
Alt + r	Shuts down LPAR manager, and turns off the server blade.
Ctrl + l	Switches the guest screen to the LPAR manager screen. The initial value for the input key is set to l (lower case "l").
Ctrl + b	Returns to the console screen where the LPAR manager screen was launched.

Names and usages of the LPAR manager screen

Screen names and usages

This section describes usage of the LPAR manager screens that open from the LPAR manager main screen (the LPAR manager Menu screen). The following

table describes the names and usages of the LPAR manager Menu screen and LPAR manager screens.

Table 10-2 Names and usages of LPAR manager screen

Screen name	Usage	Reference
LPAR manager Menu	Main screen of the LPAR manager screen. From this screen, you can move to the LPAR manager screen that suits your purpose.	LPAR manager Menu screen on page 10-5
Logical Partition Configuration	Sets the number of processors and memory size. In addition, you can switch to an LPAR guest screen, activate (turn on the power), or deactivate (turn off the power).	Logical Partition Configuration screen on page 10-8
Logical Processor Configuration	Sets physical processors for the logical processors of an LPAR.	Logical Processor Configuration screen on page 10-20
Physical Processor Configuration	You can view the configuration or the status of a physical processor, add or remove a processor group.	Physical Processor Configuration screen on page 10-23
PCI Device Information	Displays the PCI device information.	PCI Device Information screen on page 10-26
PCI Device Assignment	Assigns a PCI device to an LPAR.	PCI Device Assignment screen on page 10-30
Virtual NIC Assignment	Assigns a logical NIC to an LPAR.	Virtual NIC Assignment screen on page 10-34
Shared FC Assignment	Assigns a shared FC to an LPAR.	Shared FC Assignment screen on page 10-42
Allocated FC Information	Displays the configuration information (WWN) of the fibre channel adapter attached to the system unit.	Allocated FC Information screen on page 10-45
System Configuration	Sets the configuration of LPAR manager.	System Configuration screen on page 10-47
System Service State	Displays the LPAR manager service status.	System Service State screen on page 10-58
Date and Time	Sets the time, time zone, and other information.	Date and Time screen on page 10-63
LP Options	Sets optional functionality of LPAR.	LP Options screen on page 10-74
LPAR Usage	Displays the usage status of LPAR manager or each LPAR.	LPAR Usage screen on page 10-81
Front Panel	Obtains the memory dump of the guest OS or guest screen data.	Front Panel screen on page 10-86
LP System Logs	Displays events generated in LPAR manager.	LP System Logs screen on page 10-89

Screen name	Usage	Reference
Firmware Version Information	Displays the firmware version of a component.	Firmware Version Information screen on page 10-91

Items common to the LPAR manager screen

This subsection describes the display items common to the LPAR manager screen.

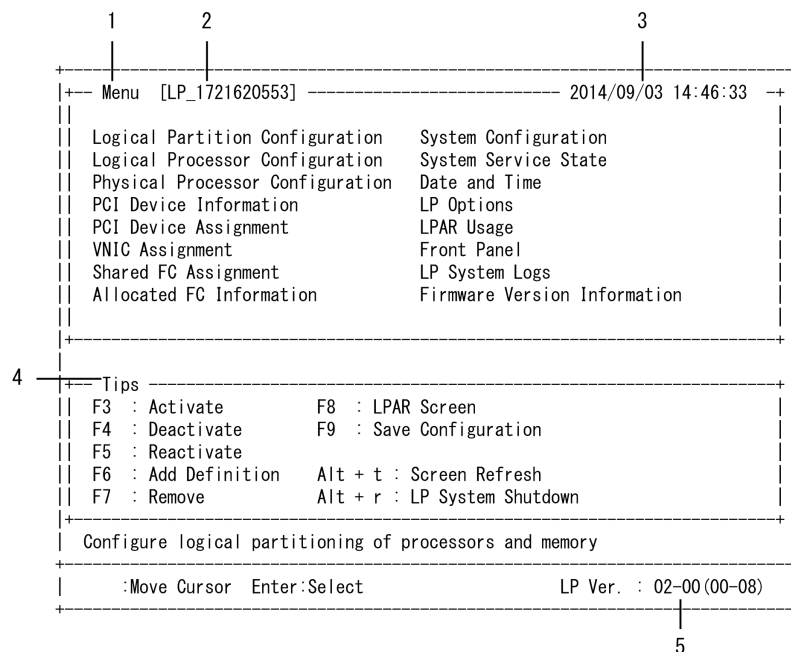


Table 10-3 Items common to the LPAR manager screen

No.	Item	Description	Initial value	Supported version
1	Error Event Detected	Indicates that an error-level LPAR manager system log was detected. In the LP System Logs screen, check the contents of the LPAR manager system log. This item disappears by pressing Esc in the screen that displays this item, or by opening the LP System Logs screen.	--	02-0x or later
2	Safe Mode	Indicates that LPAR manager is running in safe mode. For details, see Safe mode on page 9-20	--	02-20 or later

LPAR manager Menu screen

The following figure shows the LPAR manager Menu screen.



The LPAR manager Menu screen is the starting point of each LPAR manager screen operation. In addition, the following operations can be performed:

- Turning on the power of an LPAR (activating an LPAR)
- Turning off the power of an LPAR (deactivating an LPAR)
- Restarting an LPAR (reactivating an LPAR)
- Adding an LPAR
- Deleting an LPAR
- Displaying the guest screen
- Saving the configuration information

The following table describes the items on the LPAR manager Menu screen.

Table 10-4 Items on the LPAR manager Menu screen and the their descriptions

No.	Item	Description	Initial value
1	Menu	Placing the cursor on the desired screen title, and pressing Enter switches the display to the selected screen.	--
2	LPAR manager identifier	Displays the ID of the LPAR manager configured on the System Configuration screen.	--
3	System time	The LPAR manager system time set on the Date and Time screen. The time is not continuously updated. It is updated when an operation is performed on the screen, or when screen refresh is required within LPAR manager. Use this as an approximate time.	--
4	Tips	Displays the function keys that can be used on the LPAR manager Menu screen.	--

No.	Item	Description	Initial value
		<p>F3</p> <p>Activates a deactivated LPAR.</p> <p>On the displayed Activate LPAR sub-screen, select the LPAR you want to activate.</p> <p>LPARs you failed to migrate cannot be activated.</p> <p>F4</p> <p>Deactivates an activated LPAR.¹</p> <p>On the displayed Deactivate LPAR sub-screen, select the LPAR you want to deactivate.</p> <p>F5</p> <p>Reactivates an activated LPAR.²</p> <p>On the displayed Reactivate LPAR sub-screen, select the LPAR you want to reactivate.</p> <p>LPARs you failed to migrate cannot be reactivated.</p> <p>F6</p> <p>Adds an LPAR.</p> <p>On the displayed Add LPAR sub-screen, select the LPAR you want to add.</p> <p>LPARs you failed to migrate cannot be added.</p> <p>F7</p> <p>Removes an LPAR.</p> <p>On the displayed Remove LPAR sub-screen, select the LPAR you want to remove. If you remove an LPAR, all resources allocated to that LPAR are unallocated.</p> <p>You cannot perform this operation for LPARs you failed to migrate, or are not deactivated.</p> <p>F8³</p> <p>Transitions to the guest screen from the LPAR manager screen.</p> <p>On the displayed Call LPAR Guest Screen sub-screen, select the LPAR on the guest screen.</p> <p>Only activated LPARs can be transitioned to the guest screen.</p> <p>F9</p> <p>Saves the configuration information.</p> <p>Alt + t</p> <p>Redraws the LPAR manager screen.</p>	
5	LPAR manager firmware version	Displays the LPAR manager's firmware version and firmware internal version.	--
<p>Notes:</p> <p>1. ○ If a guest OS is running, shut down the guest OS or host OS instead of deactivating it.</p> <p>Deactivating an LPAR turns its power off. If you deactivate an LPAR when a guest OS is running and the LPAR is accessing data, the disk might be damaged.</p>			

No.	Item	Description	Initial value
	<ul style="list-style-type: none"> If the OS hangs up at the end of shutdown of a guest OS, deactivate the LPAR. The disc is not connected at this time, and is therefore not damaged. 		
2.	<ul style="list-style-type: none"> If a guest OS is running, restart the guest OS instead of reactivating it. Reactivating an LPAR restarts it. If you reactivate an LPAR when a guest OS is running and the LPAR is accessing data, the disk might be damaged. If the OS hangs up in the middle of the restarting the guest OS, reactivate LPAR. The disc is not connected at this time, and is therefore not damaged. 		
3.	To switch from the LPAR manager screen to the guest screen, you must set up the serial console environment for the guest OS in advance.		

Related topics

- [System Configuration screen on page 10-47](#)
- [Date and Time screen on page 10-63](#)

Logical Partition Configuration screen

The following figure shows the Logical Partition Configuration screen.

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
	Logical Partition (LPAR) Configuration																
1	#	Name	Sta	Scd	Pro	Grp	Srv	Mem	VN	PN	MN	ID	AA	AC	PC	VC	PB
	1	LPAR1	Dea	D	1	0	100	1024	0	A	A	Y	*	N	*	N	64UEFI
	2	LPAR2	Dea	S	1	0	100	1024	0	A	A	Y	*	N	N	N	64UEFI
	3																
	4																
	5																
	6																
	7																
	8																
	9																
	10																
	[PageUp]:Page Up / [PageDown]:Page Down																
	Logical Information								Physical Information								
					Pro	Shr	Ded	Mem	VN					User Memory	: 62464		21
18	Assign Total				2	1	1	2048	0					Processors	: 24 (24)		22
19	Act Total				0	0	0	0	0					Shared	: 0		
20	Remain							62464						Dedicate	: 0		
	Logical partition name																
	F1:VCAssign F2:MemAllocDsp F3:Act F4:Deact F5:React F6:Add F7:Remove																
	F8:LPARScreen F9:SaveConfig F11:Left F12:Right Esc:Menu																
23																	


```

24      25
+-----+-----+
|| Logical Partition (LPAR) Configuration |-----+
|| # Name      Sta  NUMA  PRTE |
|| 1 LPAR1     Act   Y    N   |
|| 2 LPAR2     Dea   N    N   |
|| 3           |
|| 4           |
|| 5           |
|| 6           |
|| 7           |
|| 8           |
|| 9           |
|| 10          |
||                                     [PageUp]:Page Up / [PageDown]:Page Down
+-----+-----+
|| Logical Information |-----+ Physical Information |-----+
||                   Pro  Shr  Ded      Mem VN || User Memory : 11008
|| Assign Total      4    2    2      4096  2 || Processors  : 16(16)
|| Act Total         0    0    0         0  0 || Shared      : 0
|| Remain            |      |      | 11008 || Dedicate    : 0
+-----+-----+
|F1:VCAssign F2:MemAllocDsp F3:Act F4:Deact F5:React F6:Add F7:Remove
|F8:LPARScreen F9:SaveConfig F11:Left F12:Right
|Esc:Menu

```

On the Logical Partition Configuration screen, the following operations can be performed in the environment of an LPAR:

The following table describes the items on the Logical Partition Configuration screen.

Table 10-5 Items on the Logical Partition Configuration screen and their descriptions

No.	Item	Description	Initial value
1	#	Displays the LPAR number.	--
2	Name	<p>Sets the LPAR name.</p> <p>Move the cursor to the Name column of the LPAR, and then press Enter. On the displayed Logical Partition Name sub-screen, type the name of the LPAR.</p> <ul style="list-style-type: none"> A maximum of 31 characters can be set as an LPAR name. '0' o '9', 'a' to 'z', 'A' to 'Z', '-', and '_' can be used. However, only 'a' to 'z' and 'A' to 'Z' can be used as the first character of the LPAR name. An LPAR name cannot be duplicated with another LPAR name. <p>If a name with more than eight characters is set, the ninth and any subsequent characters are omitted on the LPAR manager screen.</p>	NO_NAME
3	Sta	<p>Displays the LPAR status.</p> <p>Move the cursor to the Sta column of the LPAR row to activate, and then press Enter. On the displayed The power status sub-screen, you can select Activate, Deactivate¹, or Reactivate² state.</p> <p>Act (Activated) The LPAR is turned on.</p> <p>Dea (Deactivated) The LPAR is turned off.</p> <p>Fai (Failure) The LPAR cannot be used due to an unrecoverable failure.</p>	Dea
4	Scd	<p>Sets the scheduling mode.</p> <p>Move the cursor to the Scd column of the LPAR row, and then press Enter. On the displayed Logical Processors Scheduling mode Assignment sub-screen, you can set the scheduling mode.³</p> <p>S Shared mode</p> <p>D Dedicated mode</p>	D
5	Pro	<p>Sets the number of logical processors.⁴</p> <p>Move the cursor to the Pro column of the LPAR row, and then press Enter. On the displayed The number of Logical Processors sub-screen, type the number of processors.</p> <p>This functionality can be performed only for deactivated LPARs.</p>	1
6	Grp	Sets the processor group number. ⁵	0

No.	Item	Description	Initial value
		Move the cursor to the Grp column of the LPAR row, and then press Enter . On the displayed Group Number Assignment sub-screen, select the processor group number. For details about how to add or set the processor group number, see the Physical Processor Configuration screen.	
7	Srv	Sets the relative allocation (service ratio) of the time (service time) an LPAR uses a physical processor. You can set a value from 1 to 999 for the service ratio. Move the cursor to the Srv column of the LPAR row, and then press Enter . On the displayed The service ratio sub-screen, enter the service ratio. Set the service ratio so that the service time becomes equal to or greater than the number of processors assigned to LPAR x 250 ms. When the system is highly loaded, the processing performance might be significantly degraded. You can set the service ratio to LPAR of shared mode. You cannot set it to LPARs in dedicated mode.	100
8	Mem	Sets the memory size in multiples of 256 MB. If NUMA is disabled for the LPAR Move the cursor to the Mem column of the LPAR row, and then press Enter . On the displayed The memory size (in MB) sub-screen, you can set the memory size. Use the arrow keys to increase or decrease the memory capacity. If NUMA is enabled for the LPAR Move the cursor to the Mem column of the LPAR row, and then press Enter . On the displayed NUMA Mem Allocation sub-screen, you can specify the setting. Use the arrow keys to increase or decrease the memory capacity. You can change the memory capacity only for deactivated LPARs. If you press the F1 key on the display-destination subscreen, you can specify the memory capacity in units of GB.	1024
9	VN	Displays the total number of logical NICs assigned to an LPAR.	0
10	PN	The following are items displayed on the processor node: A: Indicates that the node is selected automatically when an LPAR is activated. Number: Indicates that only the displayed node is assigned. M: Indicates that multiple nodes are assigned.	A
11	MN	The following are display and setting items on the memory node: A: Indicates that the node is selected automatically when the LPAR is activated. Number:	A

No.	Item	Description	Initial value
		<p>Indicates that the displayed node number will be assigned to the LPAR when the LPAR is in Deactivate status.</p> <p>Indicates that the displayed node number is assigned to the LPAR when the LPAR is in Activate status.</p> <p>M:</p> <p>Indicates that multiple nodes are assigned to the LPAR.</p> <p>NM:</p> <p>Indicates that the NUMA setting of the LPAR is enabled.</p> <p>You can specify the setting on the Setting 'A' or NUMA Memory Node Number sub-screen, which is displayed by pressing Enter.</p> <p>6</p>	
12	ID	<p>Enables or disables the functionality that detects the idle state of the logical processor.</p> <p>Move the cursor to the ID column of the LPAR row, and then press Enter. On the displayed Processor Idle Detection sub-screen, select Yes or No.</p> <p>Y (the default value)</p> <p>Enables the idle detection functionality.</p> <p>N</p> <p>Disables the idle detection functionality.</p> <p>Set this item to Y to use CPU resources efficiently.</p>	Y
13	AA	<p>When LPAR manager is launched, LPAR is activated automatically. ⁷</p> <p>Move the cursor to the AA column of the LPAR row, and then press Enter. On the displayed The auto activation order sub-screen, you can specify the setting.</p> <p>1 to 99: Activated automatically. Activated in ascending order.</p> <p>*: Not activated automatically.</p>	*
14	AC	<p>Enables or disables the functionality to clear the logical SEL automatically.</p> <p>Move the cursor to the AC column of the LPAR row, and then press Enter. On the displayed Auto Clear sub-screen, select Yes or No. This functionality can be performed only for deactivated LPARs.</p> <p>Y</p> <p>Enables the auto-clear functionality.</p> <p>N</p> <p>Disables the auto-clear functionality.</p>	N
15	PC	<p>Enables or disables the processor capping functionality.</p> <p>Move the cursor to the PC column of the LPAR row, and then press Enter. On the displayed Processor Capping sub-screen, select Yes or No. Note that you cannot specify this setting for LPARs in dedicated mode.</p> <p>Y</p> <p>Enables the processor capping functionality. (Capping fluctuates within the service range specified for Srv.)</p>	*

No.	Item	Description	Initial value
		<p>N</p> <p>Deactivates the processor capping functionality.</p> <p>*</p> <p>The processor capping functionality is deactivated.</p>	
16	VC	<p>Enables or disables the virtual COM console functionality⁸, or specifies the VC number.</p> <p>Move the cursor to the VC column of the LPAR row, and then press Enter. On the displayed LPAR_n Virtual Console sub-screen, you can specify the setting. The maximum number of concurrent connections for the virtual COM console is 16. On the Allocated LPAR Information to VC/TCP Port sub-screen displayed by pressing F1, you can select the VC number or display the assignment status of the VC number and the TCP port.</p> <p>Y</p> <p>Enables the virtual COM console.</p> <p>N</p> <p>Deactivates the virtual COM console.</p> <p>1 to 16</p> <p>Sets the VC number of the virtual COM console.</p>	N
17	PB	<p>Sets the pre-boot firmware.</p> <p>Move the cursor to the PB column of the LPAR row, and then press Enter. On the displayed Pre-boot F/W sub-screen, you can specify the setting. This functionality can be performed only for deactivated LPARs.</p> <p>Use this item by setting the value to 64UEFI.</p> <p>64UEFI</p> <p>Starts the logical EFI by activating an LPAR.</p> <p>BIOS</p> <p>Starts the logical BIOS by activating an LPAR.</p>	64UEFI
18	Assign Total	<p>Displays the total resources allocated to an LPAR.</p> <p>Pro</p> <p>Displays the total number of logical processors.</p> <p>Shr</p> <p>Displays the total number of logical processors in shared mode.</p> <p>Ded</p> <p>Displays the total number of logical processors in dedicated mode.</p> <p>Mem</p> <p>Displays the total amount of memory in megabytes.</p> <p>VN</p> <p>Displays the total number of logical NICs.</p>	--
19	Act Total	<p>Displays the total amount of each resource used by an LPAR (activated).</p> <p>Pro</p>	--

No.	Item	Description	Initial value
		<p>Displays the total number of logical processors.</p> <p>Shr Displays the total number of logical processors in shared mode.</p> <p>Ded Displays the total number of logical processors in dedicated mode.</p> <p>Mem Displays the total amount of memory in megabytes.</p> <p>VN Displays the total number of logical NICs.</p>	
20	Remain	<p>Displays the remaining memory that can be used by LPAR (total-amount-of-memory-that-can-be-allocated-to-LPAR - total-amount-of-memory-used-by-LPAR) in megabytes.</p> <p>Memory isolated due to detection of a memory failure is not included in this number.</p>	--
21	User Memory	<p>Displays the total amount of memory that can be allocated to an LPAR in megabytes.</p> <p>Displays the memory capacity installed in the server blade minus the amount of memory used by LPAR manager.</p> <p>Memory that is isolated due to detection of a memory failure is not included in this number.</p>	--
22	Processors	<p>Displays the total number of physical processors in "<i>n (m)</i>" format.</p> <p><i>n</i> Displays the total number of physical processors running normally.</p> <p><i>m</i> Displays the total number of physical processors installed in the server blade.</p> <p>Also displays the total number of physical processors for each mode.</p> <p>Shared Displays the total number of physical processors in shared mode.</p> <p>Dedicate Displays the total number of physical processors in dedicated mode.</p> <p>0 is displayed when there is no LPAR in Activate status in shared or dedicated mode.</p> <p>If hyper-threading is enabled, the number of threads is displayed. If hyper-threading is disabled, the number of processor cores is displayed.</p>	--
23	Function Key	<p>Displays the function keys that can be used on the Logical Partition Configuration screen.</p> <p>F1</p>	--

No.	Item	Description	Initial value
		<p>Use this key to select the VC number, and to display the assignment status of the VC number and the TCP port. You can change the memory capacity only for deactivated LPARs.</p> <p>F2</p> <p>Displays the memory allocation status on the Memory Allocation Display sub-screen.</p> <p>F3</p> <p>On the displayed Activate LPAR sub-screen, select the LPAR you want to activate. LPARs you failed to migrate cannot be activated.</p> <p>F4</p> <p>On the displayed Deactivate LPAR sub-screen, select the LPAR you want to deactivate. ¹</p> <p>F5</p> <p>On the displayed Reactivate LPAR sub-screen, select the LPAR you want to reactivate. ² LPARs you failed to migrate cannot be reactivated.</p> <p>F6</p> <p>Adds an LPAR. On the displayed Add LPAR sub-screen, select the LPAR you want to add.</p> <p>LPARs you failed to migrate cannot be added.</p> <p>F7</p> <p>Removes an LPAR. On the displayed Remove LPAR sub-screen, select the LPAR you want to remove.</p> <p>If you remove an LPAR, all resources allocated to the LPAR also fall in the unallocated state.</p> <p>LPARs you failed to migrate cannot be removed.</p> <p>F8</p> <p>Switches the LPAR manager screen to the guest screen. Select the LPAR on the guest screen you want to move on the displayed Call LPAR Guest Screen sub-screen.</p> <p>This functionality can be performed only for activated LPARs.</p> <p>F9</p> <p>Saves the configuration information.</p> <p>F11</p> <p>Scrolls the screen to the left.</p> <p>F12</p> <p>Scrolls the screen to the right.</p>	
24	NUMA	<p>Enables or disables the guest NUMA.</p> <p>[LPAR manager firmware version: Earlier than 02-40]</p> <p>Y</p> <p>Enables NUMA for the LPAR.</p> <p>N</p> <p>Disables NUMA for the LPAR.</p>	N

No.	Item	Description	Initial value
		<p>[LPAR manager firmware version: 02-40 or later]</p> <p>Y(PB)</p> <p>Enables NUMA for the LPAR. The method to set logical processors⁹ is set to bind physical processors.</p> <p>Y(NB)</p> <p>Enables NUMA for the LPAR. The method to set logical processors⁹ is set to bind physical NUMA nodes.</p> <p>N</p> <p>Disables NUMA for the LPAR.</p> <p>Move the cursor to the NUMA column of the LPAR row, and then press Enter. On the displayed Setting NUMA sub-screen, you can specify the setting. This functionality can be performed only for deactivated LPARs.</p>	
25	PRTE	<p>[LPAR manager firmware version: 02-25 or later]</p> <p>Enables or disables the PRTE function for the LPAR.</p> <p>Y</p> <p>Enables the PRTE function for the LPAR.</p> <p>N</p> <p>Disables the PRTE function for the LPAR.</p> <p>Move the cursor to the PRTE column on the LPAR row, and then press Enter. On the displayed Setting PRTE sub-screen, you can specify the setting. Note that you can specify the setting for only an LPAR in Deactivate status.</p>	N
<p>Notes:</p> <ol style="list-style-type: none"> <ul style="list-style-type: none"> When the guest OS is running, shut down the guest OS or host OS instead of deactivating it. Deactivating an LPAR turns its power off. If you deactivate an LPAR when a guest OS is running and the LPAR is accessing data, the disk might be damaged. If the OS hangs up at the end of shutdown of a guest OS, deactivate the LPAR. The disc is not connected at this time, and is therefore not damaged. <ul style="list-style-type: none"> If a guest OS is running, restart the guest OS instead of reactivating it. Reactivating an LPAR restarts it. If you reactivate an LPAR when a guest OS is running and the LPAR is accessing data, the disk might be damaged. If the OS hangs up in the middle of restarting the guest OS, reactivate the LPAR. The disc is not connected at this time, and is therefore not damaged. If either of the following conditions is met, a screen message is displayed, and the process terminates with an error: <ul style="list-style-type: none"> When shared mode is switched to dedicated mode dynamically, and there is no physical processor that can be used for assigning all logical processors in dedicated mode in the group set for an LPAR. When shared mode is switched to dedicated mode dynamically, and physical processors that do not belong to the group set in an LPAR are included in physical processor assignment of the Logical Processor Configuration screen. The following shows the recommended value for the number of logical processors to be assigned to LPARs in shared mode: <ul style="list-style-type: none"> Number of logical processors for one LPAR \leq Number of physical processors Total number of logical processors for all LPARs \leq Number of physical processors x 4 			

No.	Item	Description	Initial value
		<ul style="list-style-type: none">To use Windows for the guest OS of an LPAR to which more than 64 logical processors are assigned, enable NUMA for the LPAR.To run an LPAR to which more than 64 logical processors are assigned, disable the PRTE functionality for the LPAR.If all of the following conditions are met, the guest OS might not run correctly on the LPAR:<ul style="list-style-type: none">The guest OS is Linux.Hyper threading is enabled.NUMA is enabled for the LPAR.The total number of NUMA nodes is 5 or more. <p>To avoid this problem, assign an even number of logical processors to each NUMA node.</p> <ul style="list-style-type: none">If all of the following conditions are met, do not assign the logical processors more than half the number of physical processors belonging to one socket.<ul style="list-style-type: none">A 4-blade SMP configuration is made, or the forcible multiple-queue scheduling is enabled. The forcible multiple-queue scheduling can be specified by the HVM management command (HvmSh) option. The forcible multiple-queue scheduling is disabled by default.Processor in shared mode are allocated to the LPARThe guest OS is RHEL7. <p>The number of processors belonging to one socket is determined depending on the types of installed processors and the hyper-threading setting of the server blade. The following table provides an example.</p>	
Table 10-6 Example of Intel E7-8890v4 (24-core)			
Installed processor		Hyper-threading	Half the number of physical processors belonging to one socket
E7-8890v4 (24-core)		Valid	48/2 = 24
		Invalid	24/2 = 12

5.

You can change the processor group number when an LPAR is deactivated or an LPAR is activated in shared mode. If either of the following conditions is met, a screen message appears, and the process terminates with an error:

- The scheduling mode of an LPAR is in dedicated mode and activated.
- There are no physical processor in shared mode in the change destination group.

6.

In an environment where an LPAR with memory node specified and an LPAR without memory node specified co-exist, if you activate an LPAR without memory node specified first, you might fail to activate the LPAR with memory node specified.

Because of this, when you create at least one LPAR with memory node specified, specify the memory node for all LPARs.

If you want to create a mixed LPAR configuration, always activate an LPAR with memory node specified first, and then activate the LPAR without memory node specified.

7.

- LPARs you want to activate automatically must be deactivated.
- When LPAR manager starts, LPAR manager activates an LPAR that has the smallest value for the automatic activation functionality first, in ascending order. If the same value is set for AA, perform auto-activation from the smallest LPAR number.
- If auto-activation of an LPAR fails for any reason, such as allocation memory not being reserved, no further auto-activation is performed.

No.	Item	Description	Initial value
	o	For 15 seconds before starting auto-activation, cancellation of auto-activation can be accepted. If you want to cancel auto-activation, press Ctrl + c at this time. Note that once auto-activation starts, you cannot cancel it.	
	o	When the LPAR manager reboots without shutting down, the setting of Auto Activation Order is ignored. LPARs are automatically activated according to the setting of Pre-State Auto Activation in the LP options screen.	
8.	o	When you enable the virtual COM console functionality and connect to the guest screen via Telnet or SSH, you can continue using the guest screen connection by pressing F8 on the LPAR manager screen. In this case, the guest screen displayed through the LPAR manager screen has precedence.	
	o	If the guest screen is not displayed while connecting to the virtual COM console, review the serial console configuration.	
	o	To connect to the guest screen, set the TCP port assigned to each LPAR, and then connect to the LPAR manager IP address via Telnet or SSH. You can check the TCP port to be set for connection in the Comment section, or on the LPAR1 Virtual Console(TCP Port=Unassigned) sub-screen. To view the Comment section, move the cursor to the VC column of the LPAR row. To open the sub-screen, move the cursor to the VC column of the LPAR row, and then press Enter .	


```

+- Logical Partition(LPAR) Configuration -+-
|| # Name   Sta  Scd  Pro  Grp  Srv   Mem  VN  PN  MN  ID  AA  AC  PC  VC  PB  || | |
|| 1 LPAR1   Dea   D    1    0  100   1024  0  A  A  Y  *  N  *  N  64UEFI ||
|| 2 LPAR2   Dea   S    1    0  100   1024  0  A  A  Y  *  N  N  N  64UEFI ||
|| 3                                                ||
|| 4                                                ||
|| 5                                                ||
|| 6                                                ||
|| 7                +-+ LPAR1 Virtual Console +-+ ||
|| 8                | (TCP Port=Unassigned) | ||
|| 9                |                         | ||
|| 10               |  Yes  | ||
||                  |  No  | ||
||                  +-+-----+ p / [PageDown]:Page Down ||
+- Logical Information -+- Physical Information -+-
||               Pro  S| Virtual Console Disable | User Memory : 62464 ||
|| Assign Total    2  |-----+ Processors : 24 (24) ||
|| Act Total      0  0  0  0  0  0  || Shared : 0 ||
|| Remain         62464  || Dedicate : 0 ||
+- Virtual Console (TCP Port=Unassigned) -+-
|F1:VCAssign F2:MemAllocDsp F3:Act F4:Deact F5:React F6:Add F7:Remove
|F8:LPARScreen F9:SaveConfig F11:Left F12:Right Esc:Menu

```


- To connect to the guest screen, set the TCP port assigned to each LPAR, and then connect to the LPAR manager IP address via Telnet or SSH. You can check the TCP port to be set for connection in the Comment section, or on the LPAR1 Virtual Console sub-screen. To view the Comment section, move the cursor to the VC column of the LPAR row. To open the sub-screen, move the cursor to the VC column of the LPAR row, and then press **Enter**.

No.	Item	Description	Initial value
	<div><div><div><div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div></div></div></div>		

If you press the **F1** key on the LPAR1 Virtual Console sub-screen, assignment status of the VC numbers and TCP ports is displayed on the Allocated LPAR Information to VC/TCP Port sub-screen.

	<pre> +-----+ Logical Partition(LP) LPAR1 Virtual Console -----+-----+ # Name Sta Scd VC TCP Port 1 LPAR1 Dea D N 20801 2 LPAR2 Dea S N Unassigned 3 1 20801 4 2 20802 5 3 20803 6 4 20804 7 5 20805 8 6 20806 9 7 20807 10 8 20808 9 20809 / [PageDown]:Page Down +-----+-----+ Logical Info 10 20810 Physical Information -----+-----+ Pro 11 20811 ser Memory : 62464 Assign Total 12 20812 rocessors : 24 (24) Act Total 13 20813 Shared : 0 Remain 14 20814 Dedicate : 0 +-----+-----+ Virtual Console(TCP P) 15 20815 16 20816 +-----+ </pre>			
	<pre> +-----+ Allocated LPAR Information to VC/TCP Port -----+-----+ VC TCP LPAR VC TCP LPAR 1 20801 -- 9 20809 -- 2 20802 -- 10 20810 -- 3 20803 -- 11 20811 -- 4 20804 -- 12 20812 -- 5 20805 -- 13 20813 -- 6 20806 -- 14 20814 -- 7 20807 -- 15 20815 -- 8 20808 -- 16 20816 -- +-----+-----+ </pre>			
	<pre> [F1:VCAssign F2:MemAlloc] F1:Allocated VC Information Add F7:Remove [F8:LPARScreen F9:SaveC] Esc:Menu </pre>			

- Use the HvmSh command for the "set logical processors" setting. For details, see the manual *HVM Management Command (HvmSh) Operation Guide*.

The following table lists the LPAR status for the items on the Logical Partition Configuration screen.

Table 10-7 LPAR status for the items on the Logical Partition Configuration screen

Item	LPAR status			Remarks
	Activated	Deactivated	Failure	
Name	N	Y	N	--
Sta	Y	Y	N	--
Scd	Y	Y	N	--
Pro	N	Y	N	--
Grp	C (shared mode only)	Y	N	--
Srv	C (shared mode only)	C (shared mode only)	N	--
Mem	N	Y	N	--
VN	N	N	N	Display only
PN	N	N	N	Display only
MN	N	C	N	Only if NUMA is enabled for the UEFI
ID	Y	Y	N	--
AA	N	Y	N	--
AC	N	Y	N	--
PC	C (shared mode only)	C (shared mode only)	N	--
VC	Y	Y	N	--
PB	N	Y	N	--
NUMA	N	C	N	Only if NUMA is enabled for the UEFI
PRTE	N	Y	N	--
Legend: Y: Can be changed N: Cannot be changed C: Can be changed with conditions				

Related topics

- [Physical Processor Configuration screen on page 10-23](#)
- [Memory Allocation Display sub-screen on page 10-93](#)

Logical Processor Configuration screen

The following figure shows the Logical Processor Configuration screen.

Table 10-8 Items on the Logical Processor Configuration screen and their descriptions

No.	Item	Description	Initial value
1	#	Displays the LPAR number.	--
2	Name	Displays the LPAR name.	NO_NAME
3	Sta	Displays the LPAR status. Act (Activated) The LPAR is turned on. Dea (Deactivated) The LPAR is turned off. Fai (Failure) The LPAR cannot be used due to an unrecoverable failure.	Dea
4	Scd	Displays the scheduling mode. S: Shared mode D: Dedicated mode	D
5	Pro	Displays the number of logical processors.	1
6	Grp	Displays the processor group number.	0
7	Logical Processor Number	Displays the logical processor number. Move the cursor to the logical processor number column of the LPAR row, and then press Enter . On the displayed Setting 'A' or Physical Processor Number sub-screen, you can set the physical processor to assign.	--
8	Logical Processor Assignment	Move the cursor to the item whose settings are to be changed, and then assign physical processors for the logical processors of each LPAR. * Indicates that no physical processor is assigned. A Indicates that a physical processor is automatically selected and assigned when an LPAR is activated in the shared mode and in the dedicated mode. Number Indicates that a physical processor with a displayed number is assigned when the status of the LPAR in the dedicated mode is Act(Activated), and that, if the status is other than Act(Activated), the function to assign a physical processor with a displayed number (function to specify a physical processor number) next time the LPAR is activated in the dedicated mode is enabled.	A
9	Function Key	Displays the function keys that can be used on the Logical Processor Configuration screen. F11 Scrolls the screen to the left. F12 Scrolls the screen to the right.	--

The following table lists the LPAR status for the items on the Logical Processor Configuration screen.

Table 10-9 LPAR status for the items on the Logical Processor Configuration screen

Item	LPAR status			Remarks
	Activated	Deactivated	Failure	
Name	N	N	N	Display only
Sta	N	N	N	Display only
Scd	N	N	N	Display only
Pro	N	N	N	Display only
Grp	N	N	N	Display only
Logical Processor Number	N	N	N	Display only
Logical Processor Assignment	C (shared mode only)	Y	N	--
Legend: Y: Can be changed N: Cannot be changed C: Can be changed with conditions				

Physical Processor Configuration screen

The following figure shows the Physical Processor Configuration screen.

	Physical Processor Configuration																
1	Processor#	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	Blade#	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	Socket#	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
4	Core#	0	0	1	1	2	2	3	3	0	0	1	1	2	2	3	3
5	Thread#	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
6	State	ACT	ACT	ACT	ACT	ACT	ACT	ACT	ACT	ACT	ACT	ACT	ACT	ACT	ACT	ACT	ACT
7	Status	HIG	HIG	HIG	HIG	HIG	HIG	HIG	HIG	HIG	HIG	HIG	HIG	HIG	HIG	HIG	HIG
8	Group#	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	Schedule	D	D	S	S	S	S	S	S	S	S	S	S	S	S	S	S
10	Freq(GHz)	3.0	2.9	2.9	2.9	3.0	2.9	2.9	2.9	2.9	2.9	2.9	2.9	2.8	2.9	2.9	2.9
11	Node#	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
	Processor Group Configuration																
12	Group#	0															
13	Name	NO_NAME															
14	Total Core	8															
15	Shr Core	7															
16	Ded Core	1															
17	F1:Add F2:Remove F11:Left F12:Right Esc:Menu																

On the Physical Processor Configuration screen, the following operations can be performed for a processor group.

- Changing the processor group number
- Changing the processor group name
- Adding a processor group
- Deleting a processor group



Note:

If an unrecoverable failure occurs in a physical processor, the following symptoms might occur:

- The logical NIC becomes temporally unavailable, communication with management modules and with external networks is disconnected.
- In dedicated mode, a failure occurs in the LPAR that uses the failed physical processor in dedicated mode. Other LPARs are not affected.
- In shared mode, if an unrecoverable failure occurs, a failure occurs in the LPAR that uses the physical processor in shared mode. In addition, other LPARs in shared mode might be slowed down. If this happens, deactivate the slowed down LPAR, and then reactivate it. By doing so, it can be recovered.

The following table describes the items on the Physical Processor Configuration screen.

Table 10-10 Items on the Physical Processor Configuration screen and their descriptions

No.	Item	Description	Initial value
1	Processor#	Displays the physical processor number.	--
2	Blade#	Displays the server blade number.	--
3	Socket#	Displays the socket number.	--
4	Core#	Displays the processor core number.	--
5	Thread#	Displays the thread number.	--
6	State	Displays the processor core status. ACT (Activate): Processor core in a normal state of operation	--
7	Status	Displays the physical processor status. HIG The physical processor is ready to operate at the maximum speed. When a physical processor is idle, or the turbo mode functionality or power capping functionality is set for it, the processor might not operate at maximum speed. MXX The physical processor is ready to operate at medium speed. M01 is the fastest, and M02, M03 ... are increasingly slower. LOW The processor is ready to operate at the lowest speed. FAI	--

No.	Item	Description	Initial value
		<p>The physical processor is in the FAULT state.</p> <p>ERR</p> <p>The physical processor is in the ERROR state.</p> <p>OFF</p> <p>The physical processor is in the OFFLINE state.</p>	
8	Group#	Sets the processor group number.	0
9	Schedule	<p>S</p> <p>Indicates that the physical processor can be used by the LPAR in shared mode.</p> <p>D</p> <p>Indicates that the physical processor is used by the LPAR in dedicated mode.</p>	D
10	Freq (GHz)	<p>Displays the current operating frequency of the physical processor.</p> <p>When a physical processor is idle, or the turbo mode functionality or power capping functionality is set for it, the processor might not operate at maximum speed.</p>	--
11	Node#	<p>Displays the physical processor node number.</p> <p>If the NUMA setting of the EFI is disabled, '-' is displayed.</p>	--
12	Group#	<p>Displays the processor group number.</p> <p>Move the cursor to the Processor column of the Group row, and then press Enter. On the displayed Group Number Assignment sub-screen, you can set the processor group number. You can set the following values for the processor group number.</p> <ul style="list-style-type: none"> • Essential: 4 • Advanced: 30 • Enterprise: 60 <p>You can change the processor group number of a processor core in the Activate or Warning state at any time. If either of the following conditions is met, a screen message appears, and LPAR manager terminates with an error:</p> <ul style="list-style-type: none"> • An LPAR in dedicated mode is activated on the target processor core. • An LPAR in shared mode is activated on the target core (in the change-target group). If you change the group number of the target core, there will be no physical processor in shared mode in the change-target group. 	0
13	Name	<p>Sets the processor group name.</p> <p>Move the cursor to the Processor column of the Name row, and then press Enter. On the displayed Group Name sub-screen, you can set the processor group name.</p> <p>A maximum of 31 characters can be set for a processor group name. You cannot use the same name for different processor groups.</p> <p>If the processor group name has more than seven characters, "~" is shown as the seventh character, and the characters after that are omitted.</p>	NO_NAME

No.	Item	Description	Initial value
		'0' to '9', 'a' to 'z', 'A' to 'Z', '-', and '_' can be used, but for the first character, only 'a' to 'z', and 'A' to 'Z' can be used.	
14	Total Core	Displays the total number of processor cores.	--
15	Shr Core	Displays the number of processor cores in shared mode.	--
16	Ded Core	Displays the number of processor cores in dedicated mode.	--
17	Function Key	<p>Displays the function keys that can be used on the Physical Processor Configuration screen.</p> <p>F1</p> <p>Adds a processor group.</p> <p>On the displayed Add Group sub-screen, select the number of the processor group you want to add.</p> <p>F2</p> <p>Deletes a processor group.</p> <p>On the displayed Remove Group sub-screen, select the number of the processor group you want to delete.</p> <p>Processor group 0, which is the default processor group, cannot be deleted.</p> <p>F11</p> <p>Scrolls the screen to the left.</p> <p>F12</p> <p>Scrolls the screen to the right.</p>	--

PCI Device Information screen

The PCI Device Information screen is described below.

PCI Device Information					
#	Vendor	Device Name	Slot#	LPAR#	SNIC#
0	Intel Corp.	USB Controller	UK13	M	-
1	Renesas Corp.	USB Controller	U13	-	-
2	Broadcom Corp.	GbE Controller 4Port	E131	S	1
3	Intel Corp.	10GbE Controller 2Port	13A	-	-
4	Hjtachi, Ltd.	Fibre Channel 8Gbps 2Port(S)	13B	S	-
[PageUp]:Page Up / [PageDown]:Page Down					
F2:MappingInfo			Esc:Menu		

On the PCI Device Information screen, the following operations can be performed.

- Checking mapping information of the physical PCI device and the PCI device on an LPAR

The following table describes the items on the PCI Device Information screen.

Table 10-11 Items on the PCI Device Information screen and their descriptions

No.	Item	Description	Initial value
1	#	Displays the number added by LPAR manager to identify PCI devices.	--
2	Vendor	Displays the vendor name (maximum of 15 characters).	--
3	Device Name	Displays the device name (maximum of 31 characters). If the dedicated port functionality is enabled, the port number is displayed at the end of the device name.	--
4	Slot#	Displays the number of the slot where the applicable PCI device is installed. For CB 520XB1/B2/B3: <ul style="list-style-type: none"> ◦ USB controller that controls front USB port: Ux ◦ USB controller that controls KVM port and remote console: UKx ◦ Onboard NIC: Gx ◦ Mezzanine card slot: Ex1 to Ex4 ◦ I/O adapter slot: 01A to 14B For CB 520HB3/B4: <ul style="list-style-type: none"> ◦ USB controller that controls front USB port, KVM port and remote console: Ux ◦ Onboard NIC: Gx ◦ Mezzanine card slot: Ex1 to Ex2 ◦ I/O adapter slot: 01A to 14B x: Server blade number "! " is displayed on the right of the slot number when the PCI device is not recognized for the reason that the PCI device is removed through the hot-plug operation or powered off due to a failure causing the blockade of the PCI device.	--
5	LPAR#	Displays the number of the LPAR to which the applicable PCI device is assigned, or the assignment status. Number Indicates that the device is exclusively assigned to an LPAR indicated by the number. M Indicates that the device is assigned to multiple LPARs. S Indicates that the device is assigned in shared mode. - Indicates that the device is not assigned.	--

No.	Item	Description	Initial value
		<p>Network Interface Card (NIC) For VF NICs, "v" is displayed at the end.</p> <p>F Fibre Channel (FC)</p> <p>S SCSI controller, RAID controller</p>	
5	Schd	<p>Displays the scheduling mode of the physical PCI device.</p> <p>D Dedicated mode</p> <p>S Shared mode</p> <p>E Exclusively shared mode</p> <p>-- Virtual NIC</p>	--
6	ID	<p>When the scheduling mode of the physical PCI device is shared mode, displays the ID used by the LPAR.</p> <p>Number vfcID 1a to 8d Network segment identifier of shared NIC For VF NICs, "v" is displayed at the end. (The displayed information might vary depending on the number of controllers for the NIC to be installed or depending on the number of ports.) Va to Vd Network segment identifier of a virtual NIC</p>	--
7	Slot	<p>Host PciConfig: Displays the location to install a physical PCI device. For a virtual NIC, "----" is displayed. "err" or "!" next to the slot display indicates that the physical PCI device is blocked or hot removed.</p> <p>LPAR PciConfig: Displays the location to install a logical PCI device. For a virtual NIC, "----" is displayed. "!" next to the slot display indicates that the physical PCI device is hot removed.</p>	--
8	Seg.Bus.Dev.Fnc	<p>Host PciConfig: Displays the PCI configuration address for the physical PCI device and virtual NIC.</p> <p>LPAR PciConfig: Displays the PCI configuration address of the logical PCI device that can be seen on an LPAR.</p>	--

No.	Item	Description	Initial value
		An asterisk (*) at the end of the PCI configuration address indicates that the physical PCI information and logical PCI information are different.	

PCI Device Assignment screen

The following figure shows the PCI Device Assignment screen.

```

+-----+
|+ PCI Device Assignment +-----+
+-----+
4 ||      PCI Device#:  0  1  2  3  4  5  6  7  8  9 10 11  ||
5 ||      Type:        U  N  N  F  ||
6 ||      Schd:        E  S  S+ S+  ||
1 ||  # Name      Sta  ||
  ||  1 LPAR1    Act  #R  -  -  -  ||
  ||  2 LPAR2    Act  A  -  -  -  ||
2 ||  3          ||
3 ||  4          ||
7 ||  5          ||
  ||  6          ||
  ||  7          ||
  ||  8          ||
  ||  9          ||
  || 10          ||
  ||                                     [PageUp]:Page Up / [PageDown]:Page Down
+-----+
8 ||+ Selected PCI Device Information+-----+
  || # Vendor      Device Name      Slot#  Bus# Dev# Func# ||
  || 0 Intel Corp.  USB Controller    U1     0  1a  0  ||
+-----+
9 ||+ F5:Attach/Detach F6:Set/Reset F10:Update Schd F11:Left F12:Right Esc:Menu |
+-----+

```

On the PCI Device Assignment screen, the following operations can be performed for a PCI device:

- Changing the scheduling mode of a PCI device
- Assigning a PCI device to an LPAR
- Switching the LPAR to which the PCI device in exclusively shared mode is attached
- Changing the USB Auto Attach setting for a specified LPAR

The following table describes the items on the PCI Device Assignment screen.

Table 10-13 Items on the PCI Device Assignment screen and their descriptions

No.	Item	Description	Initial value
1	#	Displays the LPAR number.	--
2	Name	Displays the LPAR name.	NO_NAME
3	Sta	Displays the LPAR status. Act (Activated) The LPAR is turned on.	Dea

No.	Item	Description	Initial value
		<p>Dea (Deactivated) The LPAR is turned off.</p> <p>Fai (Failure) The LPAR cannot be used due to an unrecoverable failure.</p>	
4	PCI Device#	Displays the number added by LPAR manager to identify PCI devices.	--
5	Type	<p>Displays the PCI device type.</p> <p>U USB controller</p> <p>N NIC (Network interface Card) For VF NICs, "v" is displayed at the end.</p> <p>F FC (Fibre Channel)</p>	--
6	Schd	<p>Sets the scheduling mode.</p> <p>To change the scheduling mode, you must deactivate all LPARs. Move the cursor to the PCI device number column of the Schd row, and then press Enter. On the displayed PCI Device Scheduling mode Assignment sub-screen, you can select the scheduling mode.</p> <p>D Assigns the device to an LPAR in dedicated mode.</p> <p>E Assigns the device to an LPAR in exclusively shared mode.</p> <p>S Assigns the device to an LPAR in shared mode.</p> <p>A plus sign (+) is displayed to the right of Schd for a PCI device for which you can change the scheduling mode.</p> <p>You can change the scheduling mode of a PCI device for NICs and FCs that support shared mode.</p>	--
7	PCI Device Assignment	<p>Sets the PCI device assignment.</p> <p>Move the cursor to the PCI device number column of the LPAR row, and then press Enter. On the displayed PCI Device Number Assignment sub-screen, you can specify the setting.</p> <p>An LPAR to which you want to assign a PCI device in dedicated mode or exclusively shared mode must be deactivated.</p> <p>* Not assigned</p> <p>A Assigned (unused) When the LPAR to which the PCI device is assigned is deactivated, when the PCI device in dedicated mode is used by another LPAR, or when the PCI device in exclusively shared mode is not attached to the LPAR</p> <p>R</p>	--

No.	Item	Description	Initial value
		<p>Assigned (in use)</p> <p>When the LPAR to which the PCI device is assigned is activated and the PCI device in dedicated mode is used by the LPAR, or when the PCI device in exclusively shared mode is attached to the LPAR</p> <p>-</p> <p>Cannot be assigned</p> <p>If the USB Auto Attach setting is enabled for the target LPAR, a hash mark (#) is displayed to the left of the assignment status (either "A" or "R").</p> <p>If a PCI device in dedicated mode is assigned ("A" is set) to multiple LPARs, only the LPAR that is activated first can use the PCI device. If a USB device in exclusively shared mode is not attached to any LPARs, and when the USB Auto Allocation to LPAR is enabled, the USB device is automatically attached to the LPAR that is activated first among LPARs for which "A" is set. On the other hand, when the USB Auto Allocation to LPAR is disabled, the USB device is automatically attached only in the case that an LPAR for which the USB Auto Attach setting is enabled is activated. A USB device in exclusively shared mode can be attached to an activated LPAR for which "A" or "A#" is set.</p> <p>"!" is displayed on the right of the slot number when the PCI device is not recognized for the reason that the PCI device is removed through the hot-plug operation or powered off due to a failure causing the blockade of the PCI device.</p>	
8	Selected PCI Device Information	<p>Displays information of the PCI device selected by the cursor.</p> <p>#</p> <p>Displays the number added by LPAR manager to identify PCI devices.</p> <p>Vendor</p> <p>Displays the vendor name (maximum of 15 characters).</p> <p>Device Name</p> <p>Displays the device name (maximum of 31 characters).</p> <p>Slot#</p> <p>Displays the slot number.</p> <p>Bus#</p> <p>Displays the bus number of the PCI configuration space.</p> <p>Dev#</p> <p>Displays the device number of the PCI configuration space.</p> <p>Func#</p> <p>Displays the function number of the PCI configuration space.</p> <p>"!" is displayed on the right of the slot number when the PCI device is not recognized for the reason that the PCI device is removed through the hot-plug operation or powered off due to a failure causing the blockade of the PCI device.</p>	--
9	Function Key	<p>Displays the function keys that can be used on the PCI Device Assignment screen.</p> <p>F5</p>	--

No.	Item	Description	Initial value
		<p>Moves the cursor to the PCI Device Assignment column of the target PCI device, then press the key.</p> <p>Then, Device Attach / Detach sub-screen appears, select the target LPAR to which you want to attach the USB device.</p> <p>F6</p> <p>Changes USB Auto Attach setting for the specified LPAR. ¹</p> <p>When the LPAR is activated or reactivated while the USB device in exclusively shared mode is not attached to any LPARs, the USB device is automatically attached to only the LPAR for which the USB Auto Attach setting is enabled.</p> <p>You can change USB Auto Attach setting for activated or deactivated LPARs.</p> <p>If you move the cursor to "A" or "R" of the assignment status of the USB device, and then press the key, you can switch the USB Auto Attach setting for the LPAR. This operation does not perform any Attach and Detach operation.</p> <p>If you want to enable the USB Auto Attach setting for the target LPAR, change "A" or "R" to "#A" or "#R". At this time, the USB Auto Attach setting is disabled for all other LPARs.</p> <p>If you want to disable the USB Auto Attach setting for the target LPAR, change "#A" or "#R" to "A" or "R".</p> <p>If the assignment status of the USB device is not "#A", such USB devices are not automatically attached. If there is no LPAR with "#A", USB devices are not automatically attached to any LPARs.</p> <p>F10</p> <p>When the scheduling mode of a PCI device is changed, the changes are applied to LPAR manager. You can make changes on the displayed sub-screen for checking settings.</p> <p>It takes time to apply the changes on Schd to LPAR manager. Therefore, other changes or transitions to another screen are suppressed to prevent other changes from being made until the change process completes.</p> <p>If you want to make changes other than Schd, or move to another screen, press F10 (Update PCI Dev Schd), and then select Yes to complete applying changes, or No to cancel the changes.</p> <p>F11</p> <p>Scrolls the screen to the left.</p> <p>F12</p> <p>Scrolls the screen to the right.</p>	
<p>Notes:</p> <ol style="list-style-type: none"> <ul style="list-style-type: none"> To use this functionality, you must disable USB Auto Allocation to LPAR on the LP Options screen. If you activate an LPAR of which USB device allocation status is "#A", the status display is changed to "#R". At that time, if the functionality is already attached to another LPAR, it is not detached or attached automatically. If you change the USB device not to assign to an LPAR ("*" of the assignment status), no USB device is automatically attached to the LPAR. 			

The following table lists the LPAR status for the items on the PCI Device Assignment screen.

Table 10-14 LPAR status for the items on the PCI device Assignment screen

Item	LPAR status			Remarks
	Activated	Deactivated	Failure	
Name	N	N	N	Display only
Sta	N	N	N	Display only
PCI Device#	N	N	N	Display only
Type	N	N	N	Display only
Schd	N	Y	N	--
PCI Device Assignment	N	C (dedicated mode and exclusively shared mode)	N	--
Legend: Y: Can be changed N: Cannot be changed C: Can be changed with conditions				

Related topics

- [LP Options screen on page 10-74](#)

Virtual NIC Assignment screen

The following figure shows the Virtual NIC Assignment screen.

```

+----- Virtual NIC Assignment -----+
||
5 ||
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 || # Name      Sta #VNIC  0   1   2   3   4   5   6   7   8   9
  || 1 LPAR1     Dea 2     1a  1b  *   *   *   *   *   *   *   *
  || 2 LPAR2     Dea 0     *   *   *   *   *   *   *   *   *
  || 3           ||
  || 4           ||
  || 5           ||
6 || 6
  || 7
  || 8
  || 9
  || 10
  ||
  || [PageUp]:Page Up / [PageDown]:Page Down
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
7 || VNIC Information-----+
  || No: 0  MAC Address: 00.00.87.62.c7.00  Shared NIC#: 1  Tag: Undef  Prm: T
  || Inter-LPAR Packet Filtering: Disable
  || VLANID:
  ||
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
8 || F2:Disp  F5:Set Prom. Mode  F6:Change MAC Addr  F7:Select VLAN
  || F8:Packet Filter  F11:Left  F12:Right
  || Esc:Menu
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

On the Virtual NIC Assignment screen, the following operations can be performed:

- Changing the assignment to an LPAR of the shared NIC and virtual NIC
- Displaying the list of VLAN ID assignments and promiscuous mode settings
- Changing the promiscuous mode
- Changing the MAC address
- Change the VLAN mode.
- Changing the inter-LPAR communication packet filtering for shared and virtual NICs

The following table describes the items on the Virtual NIC Assignment screen.

Table 10-15 Items on the Virtual NIC Assignment screen and their descriptions

No.	Item	Description	Initial value
1	#	Displays the LPAR number.	--
2	Name	Displays the LPAR name.	NO_NAME
3	Sta	Displays the LPAR status. Act (Activated) The LPAR is turned on. Dea (Deactivated) The LPAR is turned off. Fai (Failure) The LPAR cannot be used due to an unrecoverable failure.	Dea
4	#VNIC	Displays the total number of logical NICs.	0
5	Virtual NIC Number	Displays the logical NIC number. Move the cursor to the virtual NIC number column of the LPAR row, and then press Enter . On the displayed Physical NIC / Port Number setting sub-screen, select the network segment to change. To change the logical NIC assignment, you must deactivate the applicable LPAR. ¹	--
6	VNIC Assignment	Sets the logical processor assignment for each LPAR. * Indicates the device is not assigned. 1a to 8d Set the network segment identifier of shared NIC. For VF NICs, "v" is displayed at the end. (The displayed information might vary depending on the number of controllers for the NIC to be installed or depending on the number of ports.) Va to Vd Set the network segment identifier of a virtual NIC.	*

No.	Item	Description	Initial value
		"!" is displayed on the right of the slot number when the PCI device is not recognized for the reason that the PCI device is removed through the hot-plug operation or powered off due to a failure causing the blockade of the PCI device.	
7	VNIC Information	<p>Displays the logical NIC information selected by the cursor.</p> <p>No.</p> <p>Displays the logical NIC number.</p> <p>MAC Address</p> <p>Displays the MAC address.</p> <p>Shared NIC#</p> <p>Displays the shared NIC number.</p> <p>Tag</p> <p>Displays the VLAN mode.</p> <ul style="list-style-type: none"> ○ Undef: Neither the guest OS nor LPAR manager uses VLAN tags. ○ Tag: Only the guest OS adds or removes VLAN tags. ○ Untag: Only LPAR manager adds or removes VLAN tags. <p>Prm</p> <p>Displays whether to permit promiscuous mode.</p> <ul style="list-style-type: none"> ○ R: Prohibits the promiscuous mode. Only the frames that match the MAC address are received. ○ T: Permits the promiscuous mode. All packets can be received. (The actual behavior depends on the settings of the guest OS.) <p>VLANID</p> <p>Displays the VLAN ID. Note that VLAN ID: 4093 cannot be used because it is reserved by the system.</p> <ul style="list-style-type: none"> ○ Tagged: A maximum of 16 IDs in the range from 1 to 4094, or All (all IDs) For VF NIC, only All (all IDs) can be set. ○ Untagged: One ID in the range from 1 to 4094 <p>Inter-LPAR Packet Filtering</p> <p>Displays the inter-LPAR communication packet filtering.</p> <ul style="list-style-type: none"> ○ Disable: Inter-LPAR communication packets are transferred via the network segment in the LPAR manager. The packets are not transferred to external network. For VF NIC, only Disable is displayed. ○ Enable: Inter-LPAR communication packets are transferred via external network. The 	<p>Tag: Undef (shared NIC/virtual NIC/VFNIC (10GBASE-SR 2port LAN adapter))</p> <p>Tag: Tag (VF NIC (Emulex 10Gb 2-port converged network adapter/Onboard LAN))</p> <p>Prm: T (shared NIC/virtual NIC)</p> <p>Prm: R (VF NIC)</p> <p>Inter-LPAR Packet Filtering: Disable</p> <p>TXRATE: 10000 Mbps</p> <p>Other than above: -</p>

No.	Item	Description	Initial value
		<p>packets are not transferred to the network segment in the LPAR manager.</p> <ul style="list-style-type: none"> Disable (ALL): Inter-LPAR communication packets are transferred to the network segment in the LPAR manager and external network. <p>Inter-LPAR Packet Filtering is set into the network segment(1a to 8d), not to Logical NIC(#0~#15).</p> <p>TXRATE</p> <p>Sets the transmission band restrictions for a VF NIC.</p>	
8	Function Key	<p>Displays the function keys that can be used on the Virtual NIC Assignment screen.</p> <p>F2</p> <p>Displays the list of VLAN ID assignments.</p> <p>If a cursor points to a position where no network segment identifier is defined, nothing is displayed by clicking this key.</p> <p>To view the list of VLAN ID assignments/promiscuous mode settings defined for another network segment identifier, press Esc to close the current display, move the cursor to the appropriate position, and then press F2 (Disp) again. ²</p> <p>F5</p> <p>Sets whether to permit promiscuous mode.</p> <p>On the displayed Promiscuous Mode Setting sub-screen, select whether to permit promiscuous mode. ³</p> <p>F6</p> <p>Changes the MAC address. ^{4, 5}</p> <p>On the displayed Change of MAC Address sub-screen, enter the MAC address.</p> <p>You can change the MAC address only for deactivated LPARs.</p> <p>F7</p> <p>Sets the VLAN mode.</p> <p>On the displayed Select VLAN mode sub-screen, you can set the VLAN mode. ⁶</p> <p>F8</p> <p>Sets the inter-LPAR communication packet filtering.</p> <p>On the displayed Inter-LPAR Packet Filtering sub-screen, you can set the inter-LPAR communication packet filtering. ⁷</p> <p>F9</p> <p>Sets the transmission band restrictions for VF NIC.</p>	--

No.	Item	Description	Initial value
		<p>On the displayed Set TXRATE of VF (in Mbps) sub-screen, you can set a value from 100 Mbps to 10,000 Mbps in increments of 100 Mbps.</p> <p>When you press F1, you can type text in increments of 100 Mbps.</p> <p>F11</p> <p>Scrolls the screen to the left.</p> <p>F12</p> <p>Scrolls the screen to the right.</p>	
<p>Notes:</p> <ol style="list-style-type: none"> <ul style="list-style-type: none"> Logically, you can assign VF NICs over the maximum number of shares per port. However, the total number of VF NICs that can be used after the LPAR is activated is equal to the maximum number of shares per port. If the total number of VF NICs of an LPAR to activate exceeds the maximum number of shares per port, the message "The VF is already assigned the maximum assignable times to LPARs." appears when the LPAR is activated, and the activation fails. The following figure is a display example of a list of VLAN ID assignments and promiscuous mode settings. Describes the list of VLAN ID assignments and promiscuous mode settings. Explains promiscuous mode settings. We do not recommend to changing MAC addresses. Just in case, make sure the same MAC address does not exist on a network when changing a MAC address. If the same MAC address exists, a severe failure in the network might result. You can set the value from 00:00:00:00:00:00 to FF:FF:FF:FF:FF:FF, but values reserved by LPAR manager cannot be set. In addition, do not set multicast addresses and broadcast addresses. The following describes how to set the VLAN mode on the Select VLAN mode sub-screen. <ol style="list-style-type: none"> On the displayed Select VLAN mode sub-screen, set the VLAN mode. If you select Tagged or Untagged for the VLAN mode, enter the VLAN ID on the displayed VLAN ID Setting sub-screen. When Tagged is selected for the VLAN mode, and the number of settings for VLAN IDs is less than 16, the VLAN ID count is less than 16.Do you continue? sub-screen also appears. To continue setting VLAN IDS, click Yes. To finish VLAN ID setting, click No, and then press Enter. If you select Yes, enter VLAN IDs on the displayed VLAN ID Setting (a limit input : 1 to 4094 or 'All') (cont.) sub-screen. The following figure is an example when VLAN mode = Tag, VLANID = 1,2,3,4,5,6 are set for the shared NIC (1a) of LPAR1, Virtual NIC Number 0. Example of describes the list of VLAN ID assignments and promiscuous mode settings. Describes the inter-LPAR communication packet filtering. 			

```

+-- Virtual NIC Assignment -----+
||
||
|| Virtual NIC Number
|| # Name      Sta #VNIC  0    1    2    3    4    5    6    7
|| 1 LPAR1     Dea   2    1av 1bv  *   *   *   *   *   *
|| 2 LPAR2     Dea   0    *   *   *   *   *   *   *
|| 3
|| 4
|| 5
|| 6 +-----+
|| 7 | VLAN ID Allocation / Prom. Mode Setting Display
|| 8 | Segment:1av TXRATE ASSIGN 10000Mbps ACT 0Mbps
|| 9
|| 10 |
|| 11 |
|| 12 | LPAR# VNIC# Prm Mode VLAN ID TXRATE ACT
|| 13 | 10 1 0 R Undef 10000 N
|| 14 |
|| 15 | Down
|| 16
+-----+
+--VNIC Information-----+
|| No: 0 MAC Address: 00.00.87.e2.d2.00 Shared NIC#: 1 Tag: Undef Prm: R
|| Inter-LPAR Packet Filtering: Disable
|| VLANID: TXRATE: 10000 Mbps
+-----+
|| F2:Disp F5:Set Prom. Mode F6:Change MAC Addr F7:Select VLAN
|| F8:Packet Filter F9:Set TXRATE F11:Left F12:Right Esc:Menu

```

Figure 10-1 Describes the list of VLAN ID assignments and promiscuous mode settings

The following table describes the list of VLAN ID assignments and promiscuous mode settings.

No.	Item	Description
1	Segment	Displays the network segment identifier.
2	LPAR#	Displays LPAR numbers downward in ascending order.
3	VNIC#	Displays Virtual NIC numbers downward in ascending order.
4	Prm	Displays the promiscuous mode.
5	Mode	Displays the VLAN mode.
6	VLAN ID	Displays VLAN IDs downward in ascending order. If the number of defined VLAN IDs is nine or more, the IDs are displayed in two rows. If a VLAN ID is defined as ALL, only 'ALL' is displayed.
7	TXRATE ASSIGN	For VF NICs, displays the total number of transmission band restrictions assigned to an LPAR.
8	ACT	For VF NICs, displays the total number of transmission band restrictions used by an LPAR (activated).
9	TXRATE	Displays the transmission band restrictions for LPARs.
10	ACT	For VF NICs, displays the LPAR status. Y (Activated) The LPAR is turned on. N (Deactivated) The LPAR is turned off.

Note that if you press **F2** (Disp) when the VLAN ID is not defined for the network segment identifier set by using the cursor, the "VLAN ID is not set." message appears.

```

+----- Virtual NIC Assignment -----+
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
```

Figure 10-2 Example of describes the list of VLAN ID assignments and promiscuous mode settings



Note:

For a VF NIC assigned to an activated LPAR, do not change VLAN settings.

Table 10-16 Explains promiscuous mode settings

Promiscuous mode setting		Frames acceptance
Guest OS	LPAR manager screen	
Disable	Restricted/Through	Only frames of which destination is the LPAR (MAC address) are received by the guest OS on the LPAR.
Enable	Restricted	Only frames of which destination is the LPAR (MAC address) are received by the guest OS on the LPAR. For a VF NIC, only Restricted can be selected.
	Through	All packets in the same network segment are received.

Table 10-17 Describes the inter-LPAR communication packet filtering

Inter-LPAR communication packet filtering	Inter-LPAR communication packet		External-communication packet	Usage
	To the network segment in the LPAR manager	To external network		
Disable	Transferred	Not transferred	Transferred	Use this filter to perform inter-LPAR communication only via the network segment in the LPAR manager. For VF NIC, only Disable can be selected.
Enable	Not transferred	Transferred	Transferred	Use this filter to enhance isolation and security of each LPAR. It matches the case when each LPAR has a respective owner.
Disable (ALL)	Transferred	Transferred	Transferred	Use this filter to perform connection monitoring of Intel(R) PROSet in Windows, or inter-LPAR communication using a redundant network configuration, such as bounding for Linux.

The following table lists the LPAR status for the items on the Virtual NIC Assignment screen.

Table 10-18 LPAR status for the items on the Virtual NIC Assignment screen

Item		LPAR status			Remarks
		Activated	Deactivated	Failure	
Name		N	N	N	Display only
Sta		N	N	N	Display only
#VNIC		N	N	N	Display only
Virtual NIC Number		N	N	N	Display only
VNIC Assignment		N	Y	N	--
VNIC Information (shared NIC/ virtual NIC)	MAC Address	N	Y	N	--
	Tag	Y	Y	N	--
	Prm	Y	Y	N	--
	VLANID	Y	Y	N	--
	Inter-LPAR Packet Filtering	Y	Y	N	--

Table 10-19 Items on the Shared FC Assignment screen and their descriptions

No.	Item	Description	Initial value
1	#	Displays the LPAR number.	--
2	Name	Displays the LPAR name.	NO_NAME
3	Sta	Displays the LPAR status. Act (Activated) The LPAR is turned on. Dea (Deactivated) The LPAR is turned off. Fai (Failure) The LPAR cannot be used due to an unrecoverable failure.	Dea
4	Shared FC#	Displays the shared FC number.	--
5	Slot#	Displays the PCI slot number.	--
6	Port#	Displays the port number of the shared FC.	--
7	PortStatus	Displays the status of the shared FC port. ¹ A (Available) Can be used normally. D (LinkDown) Cannot be used because a cable is not connected. C (ConfigCheck) Cannot be used due to a configuration problem. E (ErrorCheck) Cannot be used because of an unrecoverable failure.	--
8	Shared FC Assignment	Sets shared FC port assignment of each LPAR. Move the cursor to the shared FC number of the LPAR row, and then press Enter . On the displayed Shared FC vfcWWNId Assignment sub-screen, you can select vfcID to set shared FC port assignment. To change the shared FC assignment, you must deactivate the applicable LPAR. You can set a value from 1 to 15 (for 8Gb fibre channel adapters) or 1 to 30 (for 16Gb fibre channel adapters) as the vfcID for each shared FC port. However, you cannot define the same vfcID for multiple LPARs. "!" is displayed on the right of the slot number when the PCI device is not recognized for the reason that the PCI device is removed through the hot-plug operation or powered off due to a failure causing the blockade of the PCI device.	*
9	Selected Virtual FC Port WWN Information	Displays the information on the shared FC port selected by using the cursor. ³ LPAR#	--

No.	Item	Description	Initial value
		<p>Displays the LPAR number to which the applicable shared FC is assigned.</p> <p>WWPN</p> <p>Displays WWPN of the applicable shared FC.</p> <p>WWNN</p> <p>Displays WWNN of the applicable shared FC.</p> <p>Bus#</p> <p>Displays the bus number of the applicable shared FC.</p> <p>Dev#</p> <p>Displays the device number of the applicable shared FC.</p> <p>Func#</p> <p>Displays the function number of the applicable shared FC.</p> <p>vfcID#</p> <p>Displays vfcID set for the applicable shared FC.</p>	
10	Function Key	<p>Displays the function keys that can be used on this screen.</p> <p>F11</p> <p>Scrolls the screen to the left.</p> <p>F12</p> <p>Scrolls the screen to the right.</p>	--
<p>Notes:</p> <ol style="list-style-type: none"> The following shows the cases in which PortStatus is different from "A (Available): Can be used normally": <ul style="list-style-type: none"> When PortStatus is "D (LinkDown): Cannot be used because a cable is not connected" <ul style="list-style-type: none"> Make sure the FC cable connected to the fibre channel adapter is inserted securely. Make sure the fibre channel switch where the fibre channel adapter is connected is turned on, and operating properly. Check if the same symptom occurs after replacing the FC cable (perform this if possible). When PortStatus is "C (ConfigCheck): Cannot be used due to a configuration problem" <ul style="list-style-type: none"> When the connector is connected to a fibre channel switch that does not support N_Port ID Virtualization (NPIV), check if the connection with the fibre channel switch is loop connection. (This applies when NPIV of the port for the connection destination fibre channel switch is deactivated.) If the storage is connected directly, make sure the connection is loop connection. When PortStatus is "E (ErrorCheck): Cannot be used because of an unrecoverable failure" <p>Contact your reseller or maintenance personnel.</p> The following figure shows an example when vfcID = 2 and shared FC # = 0 are set for LPAR1: 			

No.	Item	Description	Initial value
		<pre> +- Shared FC Assignment -----+ Shared FC#: 0 1 2 3 4 5 6 7 8 9 Slot#: 13B 13B Port#: 0 1 PortStatus: D A # Name Sta 1 LPAR1 Dea 2 * 2 LPAR2 Dea * * 3 4 5 6 7 8 9 10 [PageUp]:Page Up / [PageDown]:Page Down +- Selected Virtual FC Port WWN Information -----+ # LPAR# WWPN WWNN Bus# Dev# Func# vfcID# 0 1 2389000087fe7088 2389000087fe7089 10 0 0 1 F11:Left F12:Right Esc:Menu </pre>	
3.	<p>Call WWN that is used for the shared FC vfcWWN. vfcWWN is generated automatically according to the vfcID value assigned on the Shared FC Assignment screen. The generated vfcWWN is displayed within the Selected Virtual FC Port WWN Information area on the Shared FC Assignment screen.</p> <p>Also, WWN information of dedicated/shared FCs implemented in LPAR manager are listed on the Allocated FC Information screen.</p>		

The following table shows the LPAR status for the items on the Shared FC Assignment screen.

Table 10-20 LPAR status for the items on the Shared FC Assignment screen

Item	LPAR status			Remarks
	Activated	Deactivated	Failed	
Name	N	N	N	Display only
Sta	N	N	N	Display only
Slot#	N	N	N	Display only
Port#	N	N	N	Display only
PortStatus	N	N	N	Display only
Shared FC Assignment	N	Y	N	--
Selected Virtual FC Port WWN Information	N	N	N	Display only
Legend: Y: Can be changed N: Cannot be changed				

Allocated FC Information screen

The following figure shows the Allocated FC Information screen.

2	3	4	5	6	7	10	8, 9	11
Allocated	FC Information				WWN			
Lpar#	Slot#	Port#	SchMd	vfcID	WWPN	Vfc Seed	Info. 16334	<< 1/ 2>>
1	13B	0	S	1	2389000087fe7088	2389000087fe7089		
--	13B	0	S	2	2389000087fe7090	2389000087fe7091		
--	13B	0	S	3	2389000087fe7098	2389000087fe7099		
--	13B	0	S	4	2389000087fe70a0	2389000087fe70a1		
--	13B	0	S	5	2389000087fe70a8	2389000087fe70a9		
--	13B	0	S	6	2389000087fe70b0	2389000087fe70b1		
--	13B	0	S	7	2389000087fe70b8	2389000087fe70b9		
--	13B	0	S	8	2389000087fe70c0	2389000087fe70c1		
--	13B	0	S	9	2389000087fe70c8	2389000087fe70c9		
--	13B	0	S	10	2389000087fe70d0	2389000087fe70d1		
--	13B	0	S	11	2389000087fe70d8	2389000087fe70d9		
--	13B	0	S	12	2389000087fe70e0	2389000087fe70e1		
--	13B	0	S	13	2389000087fe70e8	2389000087fe70e9		
--	13B	0	S	14	2389000087fe70f0	2389000087fe70f1		
--	13B	0	S	15	2389000087fe70f8	2389000087fe70f9		
--	13B	1	S	1	2389000087fe708a	2389000087fe708b		
[PageUp]:Page Up / [PageDown]:Page Down								
Esc:Menu								

On the Allocated FC Information screen, the following operation can be performed:

- Checking the configuration information of the fibre channel adapter

The following table describes the items on the Allocated FC Information screen.

Table 10-21 Items on the Allocated FC Information screen and their descriptions

No.	Item	Description	Initial value
1	Select Display	Select displaying World Wide Name. This item appears only in a configuration that supports LPAR migration. Move the cursor onto WWN and press Enter, then Select Display sub-screen appears. Then, select WWN. WWN Displays the World Wide Name of the FC. WWN(Migration) Displays the World Wide Name of the FC to be temporarily used for LPAR migration in concurrent maintenance mode.	WWN
2	Lpar#	Displays the LPAR number to which FC is assigned. If no FC is assigned, "--" is displayed.	--
3	Slot#	Displays the number of the physical slot where the FC is inserted.	--
4	Port#	Displays the port number of the FC.	--
5	SchMd	Displays the scheduling mode of the FC. D Assigned to an LPAR in dedicated mode. S	D

No.	Item	Description	Initial value
		Assigned to an LPAR in shared mode.	
6	vfcID	Displays the set vfcID when the assigned FC is in shared mode. If it is not a shared FC, "-" is displayed.	--
7	WWPN	Displays the World Wide Port Name of the FC. Displays "?" for non-Hitachi fibre channel adapters and NICs for which the FCoE functionality is enabled.	--
8	WWNN	Displays the World Wide Node Name of the FC. Displays "?" for non-Hitachi fibre channel adapters and NICs for which the FCoE functionality is enabled.	--
9	WWPN(Migration)	Displays the World Wide Name of the FC to be temporarily used for LPAR migration in concurrent maintenance mode. This item is displayed when WWN(Migration) is selected in item 1. Displays "?" for non-Hitachi fibre channel adapters and NICs for which the FCoE functionality is enabled. Displays "-" for an unsupported fibre channel adapter.	--
10	Vfc Seed Info.	Displays Vfc seed information used for generating WWN.	--
11	Pages	Displays the number of pages. Numerator Displays the current page number. Denominator Displays the total number of pages.	--

System Configuration screen

The following figure shows the System Configuration screen.

```

+-----+ System Configuration -----+<< 1/ 3>>+
|
| 1 --- LP ID LP_1721620553 | Virtual Console Port 20801 | 8
| 2 --- LP IP Address 172.16.205.53 |
| 3 --- Subnet Mask 255.255.0.0 | SYS2 Processors Default(2) | 9
| 4 --- Default Gateway 172.16.0.254 |
| 5 --- SVP IP Address 172.16.205.1 | LP CLI1 IP Address 172.16.0.254 | 10
| | LP CLI2 IP Address 172.16.0.250 |
| | LP CLI3 IP Address 0.0.0.0 |
| | LP CLI4 IP Address 0.0.0.0 |
| | LP CLI5 IP Address 0.0.0.0 |
| | LP CLI6 IP Address 0.0.0.0 |
| | LP CLI7 IP Address 0.0.0.0 |
| | LP CLI8 IP Address 172.16.0.246 |
|
| 6 --- Management Path Default | LP-SVP Communication IPv4 | 12
| 7 --- VNIC System No: 613 |
|
+-----+
|
| 11 --- F10:Update System Config F11:Left F12:Right Esc:Menu |
+-----+

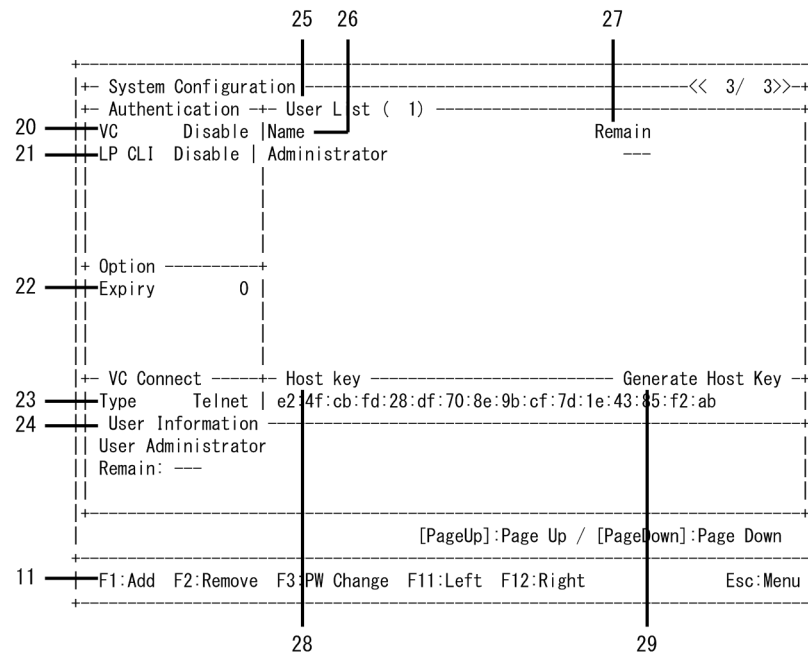
```

The following figure shows the window when the screen is scrolled to the right.

```

+-----+ System Configuration -----+<< 2/ 3>>+
|
| +-----+ IPv6 Address Configuration -----+
|
| 13 --- IPv6 Static Address Disable |
|
| 14 --- LP IP Address xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx |
| 15 --- Prefix Length xxx |
| 16 --- Default Gateway xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx |
| 17 --- SVP IP Address xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx |
| 18 --- LP CLI1 IP Address xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx |
| | LP CLI2 IP Address xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx |
| | LP CLI3 IP Address xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx |
| | LP CLI4 IP Address xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx |
| | LP CLI5 IP Address xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx |
| | LP CLI6 IP Address xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx |
| | LP CLI7 IP Address xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx |
| | LP CLI8 IP Address xxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx |
|
| 19 --- IPv6 Stateless Address Disable |
|
+-----+
|
| 11 --- F11:Left F12:Right Esc:Menu |
+-----+

```

On the System Configuration screen, you can operate the configuration information of LPAR manager shown below.

- Changing the LP ID
- Changing the VNIC system number
- Changing the virtual console port (TCP port to be connected to the guest console via Telnet or SSH)
- Changing the LPAR manager CLI IP address
- Applying the changes to LPAR manager

The following table describes the items on the System Configuration screen.

Table 10-22 Items on the System Configuration screen and their descriptions

No.	Item	Description	Initial value
1	LP ID	<p>Sets the ID to identify LPAR manager.</p> <p>Move the cursor to LP ID, and then press Enter. On the displayed Change of LP ID sub-screen, you can set the ID used to identify LPAR manager.</p> <p>You can change the LP ID only if all LPARs are deactivated.</p> <p>When more than one LPAR manager exists, you can set the ID to identify LPAR manager. For example, when using LPAR manager from HCSM, use this ID to identify LPAR manager. For this reason, set a unique value across the LPAR manager system. LPAR manager does not check if the set ID is used for other LPAR manager.</p> <p>A maximum of 16 characters can be set.</p> <p>Characters that can be specified for the LP ID</p>	LP_0000

No.	Item	Description	Initial value
		<p>Alphanumeric characters and the following symbols: ~ @ # \$ % ^ - + = _ . []</p> <p>An LP ID is automatically set according to the following specification by default. When you set an IPv4 address as an LP IP address, the numbers between which the periods have been omitted from the IPv4 address are reflected following "LP_". When you set only an IPv6 address as the LP IP address, the numbers between which the colons have been omitted from the IPv6 address without omitting the 0s, or the twelve low-order digits of the IPv6 address in hexadecimal notation, are reflected following "LP_".</p>	
2	LP IP Address	<p>Displays the LPAR manager IP address.</p> <p>The LPAR manager IP address set for the management module is applied.</p>	--
3	Subnet Mask	<p>Displays the subnet mask.</p> <p>The subnet mask set for the management module is applied.</p>	--
4	Default Gateway	<p>Displays the default gateway.</p> <p>The default gateway set for the management module is applied.</p>	--
5	SVP IP Address	<p>Displays the SVP IP address.</p> <p>The SVP IP address set for the management module is applied.</p>	--
6	Management Path	<p>[LPAR manager firmware version: 02-10 or earlier]</p> <p>Displays the PCI device of NIC to be used as the management path.</p> <p>Default</p> <p>Use the segment of which network segment is 1a or 1b as the management path.</p> <p>The management path indicates the path used when LPAR manager communicates with the management server (a server where HVM Navigator, or HvmSh commands, etc, are running).</p>	Default
7	VNIC System No	<p>Sets the VNIC system number. ³A value from 1 to 1024 can be set as the VNIC system number.</p> <p>Move the cursor to VNIC System No, and then press Enter. On the displayed VNIC System No Setting sub-screen, you can set the VNIC system number.</p> <p>VNIC System No is used for generating a MAC address in order to avoid duplication of the MAC address for the logical NIC. For this reason, set a unique value across the LPAR manager system.</p> <p>Set a unique number within the entire LPAR manager system including blade servers. This value is used as part of a MAC address for the logical NIC.</p> <p>VNIC System No is set to 0 at the initial setting, but you cannot use LPAR manager if you do not set a value other than 0 when starting LPAR manager for the first time. LPAR manager does not check if the set VNIC System No is duplicated in other LPAR manager.</p>	0

No.	Item	Description	Initial value
8	Virtual Console Port	<p>Set the TCP port used to connect to the guest console via Telnet or SSH.⁴ The virtual console port can be changed only when all LPARs are deactivated.</p> <p>Move the cursor to Virtual Console Port, and then press Enter. On the displayed Virtual Console Port Setting sub-screen, you can set the TCP port used to connect to the guest console via Telnet or SSH.</p> <p>A value from 1024 to 65520 can be set for the TCP port. However, if the connection method of the Virtual COM console is "user authentication-enabled Telnet" or "SSH", a value from 1024 to 65504 can be set.⁶</p> <p>On the System Configuration screen, you can set only the TCP port used to connect to VC 1. For TCP ports after VC 2, the value increments by one in accordance with each increment of the VC number.</p> <p>When LPAR manager starts, the TCP port obtained by LPAR manager (serial number from 20801) is applied as the initial value.</p>	20801
9	SYS2 Processors	<p>[LPAR manager firmware version: 02-62 or later]</p> <p>Displays the upper limit of the number of the physical processors used by SYS2.</p> <p>"Default(n)" is displayed if the value is not changed from the default value.</p> <p>The SYS2 Processors setting can be changed only when all LPARs are in Deactivate status.</p> <p>Move the cursor to SYS2 Processors, and then press Enter. On the displayed SYS2 Processors Setting sub-screen, you can change the SYS2 Processors setting.</p> <p>Setting SYS2 Processors to 3 improves the response time in LPAR manager operation.</p>	2
10	LP CLI1 IP Address to LP CLI8 IP Address	<p>Set the LPAR manager CLI IP Address. ^{1, 2}</p> <p>Move the cursor to LPAR manager CLI IP Address, and then press Enter. On the displayed Change of LP CLI1 IP Address sub-screen, you can set the LPAR manager CLI IP address.</p> <p>Sets the IP address of the server on which the management tool is executed.</p>	0.0.0.0
11	Function Key	<p>Displays the function keys that can be used on the System Configuration screen.</p> <p>F1</p> <p>Adds a user account used for user authentication. On the displayed Add User(Name) sub-screen, specify a user name.</p> <ul style="list-style-type: none"> For user names, you can use alphanumeric characters, dots (.), hyphens (-), and underscores (_). The first character must be an alphabetic character. Specify a user name consisting of a character string of 1 to 31 characters. 	--

No.	Item	Description	Initial value
		<p>Next, specify a password.</p> <ul style="list-style-type: none"> For a password, you can use alphanumeric characters and symbols. However, you cannot use space characters. Specify a password consisting of a character string of 1 to 31 characters. <p>F2</p> <p>Deletes an account used for user authentication. On the displayed User[<i>User Name</i>] User Erase. Do you continue? sub-screen, specify the user name you want to delete.</p> <p>F3</p> <p>Changes a password used for user authentication. On the displayed User[<i>User Name</i>] Please input a new password. sub-screen, specify a password.</p> <ul style="list-style-type: none"> For a password, you can use alphanumeric characters and symbols. However, you cannot use space characters. Specify a password consisting of a character string of 1 to 31 characters. <p>F10⁵</p> <p>Apply the changes to LPAR manager. You can apply the changes on the displayed sub-screen for checking settings. When Yes is selected, it takes two to three minutes for changes to complete, and you cannot use LPAR manager during that period.</p> <p>To cancel changes, press F10 to select No on the sub-screen for checking settings. The state before changes can be restored.</p> <p>It takes time to apply the changes to LPAR manager. Therefore, other changes or transitions to another screen are suppressed to prevent other changes from being made until the change process completes. If you want to move to another screen, press the F10 key, and select Yes on the setting confirmation sub-screen to apply the changes. Alternatively, select No on the setting confirmation screen to cancel the changes.</p> <p>Operation performed by using the F10 key provides measures to make temporal changes on the System Configuration screen while LPAR manager is running. If you restart LPAR manager, the settings will be lost. To save settings, press the F9 key on the LPAR manager Menu screen.</p> <p>F11</p> <p>Scrolls the page to the left.</p> <p>F12</p> <p>Scrolls the page to the right.</p>	
12	LP-SVP Communication	<p>[LPAR manager firmware version: 02-25 or later]</p> <p>This item displays the protocol that is used for communication between the LPAR manager and management module.</p>	IPv4

No.	Item	Description	Initial value
		IPv4 IPv4 is used. IPv6(Static) IPv6 is used. The protocol set on the management module is applied to this item.	
13	IPv6 Static Address	[LPAR manager firmware version: 02-25 or later] This item displays whether use of the IPv6 static address is enabled or disabled. Enable The IPv6 static address is used. Disable The IPv6 static address is not used. The IPv6 static address set on the management module is applied to this item.	Disable
14	LP IP Address	[LPAR manager firmware version: 02-25 or later] This item displays the LP IPv6 address. The LP IPv6 address set on the management module is applied to this item.	--
15	Prefix Length	[LPAR manager firmware version: 02-25 or later] This item displays the prefix length of the LP IPv6 address. The prefix length set on the management module is applied to this item.	--
16	Default Gateway	[LPAR manager firmware version: 02-25 or later] This item displays the default gateway for the LP IPv6 address. The default gateway set on the management module is applied to this item.	--
17	SVP IP Address	[LPAR manager firmware version: 02-25 or later] This item displays the SVP IPv6 address. The SVP IPv6 address set on the management module is applied to this item.	--
18	LP CLI1 IP Address to LP CLI8 IP Address	[LPAR manager firmware version: 02-25 or later] Set the LP CLI IPv6 Address. ¹ By placing the cursor on the LP CLI IP Address and then pressing the Enter key, you can set the LP CLI IP Address in the Change of LP CLI1 IP Address subscreen. Set the IP address of the server on which the management tool runs.	::
19	IPv6 Stateless Address	[LPAR manager firmware version: 02-25 or later] This item displays whether use of the IPv6 stateless address is enabled or disabled. Enable The IPv6 stateless address is used. Disable	Disable

No.	Item	Description	Initial value
		<p>The IPv6 stateless address is not used.</p> <p>The IPv6 stateless address set on the management module is applied to this item.</p>	
20	VC ⁷	<p>[LPAR manager firmware version: 02-05 or later]</p> <p>Displays whether user authentication is used when connecting to the guest console.</p> <p>Disable</p> <p>Does not perform user authentication.</p> <p>Enable</p> <p>Performs user authentication.</p> <p>-----</p> <p>Displayed when the connection method of the Virtual COM console is SSH.</p> <p>In addition, you can specify whether to use user authentication on the Authentication Setting (Virtual Console) sub-screen, which is displayed by pressing Enter. You cannot perform an operation by pressing the F10 key because the configuration information for user authentications is automatically saved after settings are specified.</p> <p>If the IPv4 LP IP address is not set, you cannot set "Disable" to "VC". Set "Enable" to "VC" or set "ssh" to "Type".</p> <p>If "VC" is "Disable", Telnet connections cannot be established to IPv6 LP IP addresses.</p>	Disable
21	LP CLI ⁷	<p>[LPAR manager firmware version: 02-05 or later]</p> <p>Displays whether user authentication is used when connecting by using the LP CLI.</p> <p>Disable</p> <p>Does not perform user authentication.</p> <p>Enable</p> <p>Performs user authentication.</p> <p>In addition, you can specify whether to use user authentication on the Authentication Setting (LP CLI) sub-screen, which is displayed by pressing Enter. You cannot perform an operation by pressing the F10 key because the configuration information for user authentications is automatically saved after settings are specified.</p>	Disable
22	Expiry ⁷	<p>[LPAR manager firmware version: 02-05 or later]</p> <p>Set the validity period of the password. You can specify the setting on the Setting Password Expiry sub-screen, which is displayed by pressing Enter.</p> <p>0</p> <p>The password does not expire (no limitation).</p> <p>1 to 365</p> <p>Sets the validity period of the password to a value from 1 to 365 days.</p>	0

No.	Item	Description	Initial value
		You cannot perform an operation by pressing the F10 key because the configuration information for user authentications is automatically saved after settings are specified.	
23	Type ⁷	<p>[LPAR manager firmware version: 02-05 or later]</p> <p>Set the connection method of the virtual COM. You can specify the setting on the Virtual Console Connection Type sub-screen, which is displayed by pressing Enter.</p> <p>Telnet</p> <p>Connects via Telnet.</p> <p>ssh</p> <p>Connects via SSH.</p> <p>You cannot perform an operation by pressing the F10 key because the configuration information for user authentications is automatically saved after settings are specified.</p>	Telnet
24	User Information ⁸	<p>[LPAR manager firmware version: 02-05 or later]</p> <p>Displays user information.</p> <p>Name</p> <p>Displays a user name.</p> <p>Remain</p> <p>Displays the validity period of the password. The number of remaining days (excluding the expiration date) is displayed as the validity period. The number of remaining days decreases at 0:00 UTC.</p>	--
25	User List ⁸	<p>[LPAR manager firmware version: 02-05 or later]</p> <p>Displays a list of users. The number of registered users is displayed in parentheses.</p> <ul style="list-style-type: none"> • User names are displayed in ASCII code in ascending order. • A maximum of 10 user names are displayed per page. 	--
26	Name ⁸	<p>[LPAR manager firmware version: 02-05 or later]</p> <p>Displays a user name.</p>	--
27	Remain ⁸	<p>[LPAR manager firmware version: 02-05 or later]</p> <p>Displays the validity period of the password. The number of remaining days (excluding the expiration date) is displayed as the validity period. The number of remaining days decreases at 0:00 UTC.</p> <p>---</p> <p>No validity period.</p> <p>Number</p> <p>Indicates the number of remaining days of the validity period.</p> <p>*</p> <p>The number of remaining days of the validity period is 14 days or less.</p> <p>Expired</p>	--

No.	Item	Description	Initial value
		<p>The password has expired.</p> <p>NaN</p> <p>In a state other than above.</p>	
28	Host key ⁸	<p>[LPAR manager firmware version: 02-05 or later]</p> <p>Displays the host key used for SSH connections from the virtual COM.</p>	--
29	Generate Host Key ⁷	<p>[LPAR manager firmware version: 02-05 or later]</p> <p>Re-creates the host key used for SSH connections from the virtual COM. The host key is re-created if you select Yes on the Execute Generate Host Key? sub-screen, which is displayed by pressing Enter.</p> <p>You cannot perform an operation by pressing the F10 key because the configuration information for user authentications is automatically saved after settings are specified.</p>	--
<p>Notes:</p> <ol style="list-style-type: none"> To apply the changes, you do not need to press F10. Note that it might take about 10 seconds to apply the changes. Do not set multicast and broadcast addresses. Do not change the VNIC system number of LPAR manager during system operation. If you change the number, the following symptoms might occur: <ul style="list-style-type: none"> The MAC address of the logical NIC assigned to the guest OS that belongs to the applicable LPAR manager is changed. If you reuse the VNIC system number used for another LPAR manager, the MAC address of the logical NIC might be duplicated. If you change a value of the virtual console port, the TCP port is changed. Therefore, you need to reconnect to the guest screen. If the new value of the virtual console port conflicts with the value of the TCP port used for another application, you might not connect to the guest console. Use the F10 key when there is no activated LPAR. If you perform this operation when there is an activated LPAR, network communication of the LPAR is disconnected for a few minutes. Operation performed by using the F10 key provides measures to make temporal changes on the System Configuration screen while LPAR manager is running. If you restart LPAR manager, the settings will be lost. To save settings, press the F9 key on the LPAR manager Menu screen. Lists the LPAR status for the items on the System Configuration screen. This item cannot be set for the TCP ports used by LPAR manager. For details about the TCP ports used by the LPAR manager, see Appendix E, Port numbers used by LPAR manager on page E-1. If the LPAR manager firmware version is 02-45 or later, the item can be operated only when the user who logged in to the management module has the LPAR manager security permission. If the LPAR manager firmware version is 02-45 or later, the item can be displayed only when the user who logged in to the management module has the LPAR manager security permission. 			

Table 10-23 LPAR status for the items on the System Configuration screen

Item	LPAR status			Remarks
	Activated	Deactivated	Failed	
LP ID	N	Y	N	--
LP IP Address (IPv4)	N	N	N	Display only
Subnet Mask	N	N	N	Display only
Default Gateway (IPv4)	N	N	N	Display only
SVP IP Address (IPv4)	N	N	N	Display only
Management Path	N	N	N	[LPAR manager firmware version: 02-10 or earlier] Display only
VNIC System No	N	Y	N	--
Virtual Console Port	N	Y	N	--
SYS2 Processors	N	Y	Y	[LPAR manager firmware version: 02-62 or later]
LP CLI1 IP Address to LP CLI8 IP Address (IPv4)	Y	Y	Y	--
LP-SVP Communication	N	N	N	Display only
IPv6 Static Address	N	N	N	Display only
LP IP Address (IPv6)	N	N	N	Display only
Prefix Length	N	N	N	Display only
Default Gateway (IPv6)	N	N	N	Display only
SVP IP Address (IPv6)	N	N	N	Display only
LP CLI1 IP Address to LP CLI8 IP Address (IPv6)	Y	Y	Y	--
IPv6 Stateless Address	N	N	N	Display only
VC	Y	Y	Y	When the VC item is changed, the Virtual COM console is disconnected.
LP CLI	Y	Y	Y	--
Expiry	Y	Y	Y	--
Type	Y	Y	Y	When the VC item is changed, the Virtual COM console is disconnected.
User List	N	N	N	Display only
Name	N	N	N	Display only
Remain	N	N	N	Display only
Host key	N	N	N	Display only

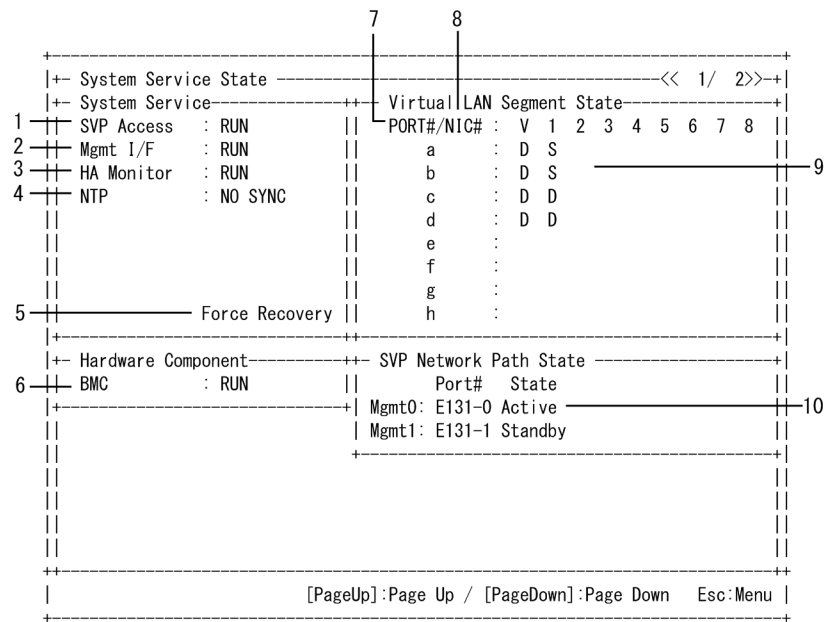
Item	LPAR status			Remarks
	Activated	Deactivated	Failed	
Generate Host Key	Y	Y	Y	--
User Information	N	N	N	Display only
Legend: Y: Can be changed N: Cannot be changed				

Related topics

- [LPAR manager Menu screen on page 10-5](#)

System Service State screen

The following figure shows the System Service State screen.



+-----+ System Service State -----+ Shared PCI Device Port State-<< 2/ 2>>+-----+	
11	TYPE : N F
12	NIC# : 1* -
13	PORT#/SLOT# : E131 13B
14	0 : U D
	2 : U A
	3 : U
	4 :
	5 :
	6 :
	7 :
	8 :
	9 :
	10 :
	11 :
	12 :
	13 :
	14 :
	15 :
+-----+ [PageUp]:Page Up / [PageDown]:Page Down Esc:Menu +-----+	

On the System Service State screen, the following operations can be performed:

- Displaying the LPAR manager service status
- Restoring the normal state of the LPAR manager system service
- The Force Recovery operation might affect the system.
Before the Force Recovery operation, be sure to read the notes on the Force Recovery operation.

The following table describes the items on the System Service State screen.

Table 10-24 Items on the System Service State screen and their descriptions

No.	Item	Description	Initial value
1	SVP Access	Displays the access status of the management module. RUN The service is running normally. STOP The service stops. ERROR The service contains an error. UNKNOWN No update is performed from the service patrol.	STOP
2	Mgmt I/F	Displays the access status of the management server. RUN The service is operating normally. STOP The service stops. ERROR The service contains an error.	STOP

No.	Item	Description	Initial value
		UNKNOWN No update is performed from the service patrol.	
3	HA Monitor	Displays the HA Monitor status. RUN The service is operating normally. STOP The service stops. ERROR The service contains an error. UNKNOWN No update is performed from the service patrol.	STOP
4	NTP	Displays the NTP status. SYNC Synchronization with NTP is successfully completed. NO SYNC Synchronization with NTP is not performed. ERROR Synchronization with NTP failed. INACTIVE Synchronization with NTP is stopped. When multiple NTP servers are set, if the time is obtained from any server, "SYNC" is displayed. If you cannot obtain the time from any server, "ERROR" is displayed. If the difference between the correct time and the time to be corrected by NTP time synchronization that takes place at regular intervals (15 minutes) exceeds 60 seconds, INACTIVE is displayed, and NTP time synchronization stops. If this phenomenon occurs, in the LP System Logs screen, find a message that includes "An abnormal time difference was detected", and then take action as described in the message.	NO SYNC
5	Force Recovery ¹	Perform this operation if the system service is not running normally, or to restore the system service. Move the cursor to Force Recovery, and then press Enter . On the displayed setting confirmation sub-screen, you can specify the setting. If Yes is selected, it will take a few minutes to complete force recovery. During the period, you cannot manipulate LPAR manager. Perform force recovery when there is no activated LPAR. If you perform this operation when there is an activated LPAR, network communication of the LPAR is disconnected for a few minutes.	--
6	BMC	Displays the BMC status. RUN The service is operating normally. ERROR The service contains an error.	RUN

No.	Item	Description	Initial value
7	PORT#	Displays the port number.	--
8	NIC#	Displays the NIC number.	--
9	Virtual LAN Segment State	<p>Displays the virtual LAN segment status.</p> <p>A Activated.</p> <p>S Stand by.</p> <p>D Down.</p> <p>F Fault.</p> <p>Blank Not a shared NIC. Not supported by VF NIC.</p>	--
10	SVP Network Path State	<p>Displays the management path status.</p> <p>Connect Displays the possibility of management path connection.</p> <p>Success Communication with the management module is enabled.</p> <p>Fail Communication with the management module is disabled.</p> <p>Link Displays the link status of the management path.</p> <p>Yes Linked up.</p> <p>No Linked down.</p> <p>Port# Displays the port number of the management path.</p> <p>LPAR manager firmware versions 02-20 or later</p> <p>Port# Displays the NIC and port number of the management path.</p> <p>State Displays the management path status.</p> <p>Active The path is in the active state, and is used for communication with the management module.</p> <p>Standby The path is in the standby state, and can be used for external communication.</p>	--

No.	Item	Description	Initial value
		<p>Error</p> <p>The path is in a network failure state.</p> <p>Link down</p> <p>The path is in a link-down state, or the management path is in a blocked state.</p> <p>Unknown</p> <p>LPAR manager is unable to communicate externally.</p> <p>-----</p> <p>No port is specified for the path.</p>	
11	TYPE	<p>Displays the type of the PCI device in shared mode.</p> <p>N</p> <p>NIC (Network interface Card)</p> <p>For VF NICs, "v" is displayed at the end.</p> <p>F</p> <p>FC (Fibre Channel)</p>	--
12	NIC#	<ul style="list-style-type: none"> When the device type is N <p>Displays the shared NIC number.</p> <ul style="list-style-type: none"> When the device type is F <p>Displays "-".</p>	--
13	PORT#	Displays the port number.	--
14	SLOT#	Displays the slot number.	--
15	Shared PCI Device Port State	<p>Displays the PCI device status in shared mode.</p> <p>When the device type is N:</p> <p>U</p> <p>Link up state.</p> <p>D</p> <p>Link down state.</p> <p>E</p> <p>Cannot be used because of an unrecoverable failure.</p> <p>--</p> <p>The status is unclear.</p> <p>Blank</p> <p>The shared NIC is not defined.</p> <p>When the device type is F:</p> <p>A (Available)</p> <p>Can be used normally.</p> <p>D (LinkDown)</p> <p>Cannot be used because a cable is not connected.</p> <p>C (ConfigCheck)</p> <p>Cannot be used due to a configuration problem.</p> <p>E (ErrorCheck)</p>	D

No.	Item	Description	Initial value
		Cannot be used because of an unrecoverable failure.	
<p>Notes:</p> <ol style="list-style-type: none"> The Force Recovery operation might affect the system. Note the following when using Force Recovery operation. <ul style="list-style-type: none"> Do not perform the Force Recovery operation when the management module and LPAR manager cannot communicate with each other. If the Force Recovery operation is performed while an LPAR to which a shared NIC is assigned is running, network communication of the shared NIC on the LPAR is disconnected for a few minutes. If the Force Recovery operation is performed while an LPAR for which a VF NIC is defined is running, the VF NIC cannot be used from the OS on the LPAR. To recover the VF NIC, reboot the OS on the LPAR after the Force Recovery operation is completed. If the Force Recovery operation is performed during the operation using the LPAR manager IP address, the operation using the LPAR manager IP address ends in error. If the Force Recovery operation is performed, communication with the management module is disconnected for a few minutes. 			

Related topics

- [Influence when management path communication is not available on page 1-16](#)
- [Notes on communication on the management path on page 1-17](#)

Date and Time screen

The following figures show the Date and Time screen. Display of the Date and Time screen differs, depending on whether the time setting from the NTP server is performed.

When the time is not set from the NTP server

		4	5	6	7	1	8	
	+----- Logical Partition(LPAR) Date and Time -----				+----- LPAR RTC -----			
2	++ # Name	Sta	Time	Mode	Date and Time	Time Zone	Current	RTC
	++ 1 LPAR1	Dea	-----	-----	yyyy/mm/dd hh:mm:ss	-----	0	
3	++ 2 LPAR2	Dea	-----	-----	yyyy/mm/dd hh:mm:ss	-----	0	
	++ 3							
	++ 4							
	++ 5							
	++ 6							
	++ 7							
	++ 8							
	++ 9							
	++ 10							
	+-----							
	[PageUp]:Page Up / [PageDown]:Page Down							
	+-----							
	++ System Date and Time							
	+-----							
9	++ Date and Time	yyyy/mm/dd	hh:mm:ss	Time Zone	+ 9:00	Adjust LPAR Time		
12	++ Setting						+-----	
13	++ Import Config						None	
14	++ TimeSync						Disable	
	+-----							
	+-----							
16	++ F6:Change System Date and Time				F7:Change System Time Zone		Esc:Menu	
	+-----							

When the time is set from the NTP server

		4	5	6	7	1	8	
	Logical Partition(LPAR) Date and Time				LPAR RTC			
2	# Name	Sta Time Mode	Date and Time	Time Zone	Current	RTC		
	1 LPAR1	Dea	yyyy/mm/dd hh:mm:ss		0			
3	2 LPAR2	Dea	yyyy/mm/dd hh:mm:ss		0			
	3							
	4							
	5							
	6							
	7							
	8							
	9							
	10							
	[PageUp]:Page Up / [PageDown]:Page Down							
	System Date and Time							
9	Date and Time	yyyy/mm/dd hh:mm:ss	Time Zone	+ 9:00	Adjust LPAR Time			
12	NTP(Disable)							11
15	NTP Server 1 None							12
	NTP Server 2 None							
16	F6:Change System Date and Time				F7:Change System Time Zone		Esc:Menu	

On the Date and Time screen, the following operations can be performed, including time or time zone settings:

- Displaying the RTC, or SEL time of LPARs
- Changing the time mode of LPARs
- Changing the LPAR time
- Changing the LPAR time zone

- Synchronizing the LPAR time with the LPAR manager system time
- Importing synchronization settings of the time from the management module or BMC
- Specifying the time adjustment settings for NTP
- Setting the IP address of the NTP server
- Changing the LPAR manager system time
- Changing the LPAR manager system time zone



Note:

- We recommend that you adjust the LPAR manager system time by using NTP.
When you do not adjust the LPAR manager system time by using NTP, if you restart LPAR manager after using it for a long time (due to, for example, unexpected LPAR manager system failure or N + M failover), the guest OS will have a time lag.
- After enabling NTP settings, make sure that you save the configuration information. If you restart LPAR manager without saving the configuration information, the RTC time of an LPAR might have the same time lag as the NTP correction time.
- Use the same time zone for the management module, BMC, and LPAR manager.
If you do not use the same time zone, they show different times. If a failure occurs, you cannot find out the correct time when it occurred.
- For BMC and LPAR manager, we recommend that you adjust the time by using the management module.
- The value changed on the Date and Time screen is not saved automatically. When you restart LPAR manager, the values you set will be lost. To avoid this happening, save the configuration information by pressing **F9** on the LPAR manager Menu screen.
- When setting the LPAR manager system time, change the system equipment time, or use the NTP server to synchronize the LPAR manager system time.
- The Date and Time screen is updated every second. Because of this, the display of the cursor is not stable. In addition, the time that shows the time in the middle of the update might appear.

The following table describes the items on the Date and Time screen.

Table 10-25 Items on the Date and Time screen and their descriptions

No.	Item	Description	Initial value
1	Select Display	<p>Select the time to display.</p> <p>Move the cursor to Select Display, and then press Enter. On the displayed Select Display Time sub-screen, select the time to display.</p> <p>LPAR RTC</p> <p>Displays the current RTC time for the LPAR.</p>	LPAR RTC

No.	Item	Description	Initial value
		<p>LPAR SEL Time</p> <p>Displays the logical SEL time for the LPAR.</p> <p>Last Activated</p> <p>Displays the RTC time when the LPAR was last activated (turned on).</p> <p>Last Deactivated</p> <p>Displays the RTC time when the LPAR was last deactivated (turned off).</p> <p>RTC Last Modified</p> <p>Displays the RTC time when the LPAR was last updated by the guest.</p>	
2	#	Displays the LPAR number.	--
3	Name	Displays the LPAR name.	NO_NAME
4	Sta	<p>Displays the LPAR status.</p> <p>Act (Activated)</p> <p>The LPAR is turned on.</p> <p>Dea (Deactivated)</p> <p>The LPAR is turned off.</p> <p>Fai (Failure)</p> <p>The LPAR cannot be used due to an unrecoverable failure.</p>	Dea
5	Time Mode	<p>Set the SEL time mode.</p> <p>Move the cursor to the Time Mode column of the LPAR row, and then press Enter. On the displayed SystemEventLog time mode sub-screen, you can specify the SEL time mode.</p> <p>Local-Time</p> <p>Indicates the local time mode.</p> <p>GMT</p> <p>Indicates the GMT (Greenwich Mean Time) mode.</p> <p>The SEL time mode can be set when the LPAR SEL time is displayed for Select Display.</p> <p>The SEL time mode can be changed only when the applicable LPAR is deactivated.</p> <p>When "GMT" is set, the SEL time zone is not added to the SEL time. When "Local-Time" is set, the SEL time zone is added to the SEL time.</p>	Local-Time
6	Date and Time	<p>Displays the time selected for Select Display.</p> <p>Move the cursor to the Date and Time column of the LPAR row, and then press Enter. On the displayed year, month, and date sub-screen, you can set the SEL time.</p> <p>The format is "yyyy/mm/dd hh:mm:ss".</p> <p>yyyy</p> <p>Christian Era year</p> <p>mm</p>	--

No.	Item	Description	Initial value
		<p>Month</p> <p>dd</p> <p>Day</p> <p>hh</p> <p>24-hour notation</p> <p>mm</p> <p>Minutes</p> <p>ss</p> <p>Seconds</p> <p>The minimum value is 2000/01/01 00:00:00, and the maximum value is 2099/12/31 23:59:59.</p> <p>You can also set the SEL time if LPAR SEL Time is displayed for Select Display.</p> <p>When the SEL time mode is local mode, the time with the SEL time zone added is displayed.</p> <p>When the SEL time mode is GMT, the SEL time zone is not added.</p> <p>The time stamp of logical SEL to be reported to an LPAR is the SEL time.</p> <p>The SEL time can be changed only when the applicable LPAR is deactivated.</p>	
7	Time Zone	<p>Sets the SEL time zone.</p> <p>Move the cursor to the Time Zone column of the LPAR row, and then press Enter. On the displayed time zone sub-screen, you can set the SEL time zone.</p> <p>When the SEL time mode is the local time mode, if you change this value, the SEL time is also changed.</p> <p>The value can be set in increments of one hour. The minimum value is -12 hours, and the maximum value is +12 or +14 hours.</p> <p>When the SEL time mode is the GMT mode, this field cannot be changed.</p> <p>The SEL time zone can be set only when the LPAR SEL time is displayed for Select Display.</p> <p>The SEL time zone can be set only when the applicable LPAR is deactivated.</p>	LPAR manager system time zone
8	Current RTC	Displays in decimal the difference between the LPAR RTC time and the LP system time.	0
	Init RTC	<p>Displays in decimal the difference between the LPAR RTC time and the LPAR manager system time saved in the configuration information. This value is determined immediately after LPAR manager starts, and cannot be changed while LPAR manager is running.</p> <p>The Init RTC value is displayed when RTC Last Modified is selected for Select Display.</p>	
9	Date and Time	Displays the LPAR manager system time.	--

No.	Item	Description	Initial value
		The system equipment time is applied as the initial value when LPAR manager starts.	
10	Time Zone	<p>Change the LPAR manager system time zone. ¹</p> <p>Indicates the time lag between the LPAR manager system time and GMT. If you change this value, the LPAR manager system time is not changed.</p> <p>The value can be set in increments of one hour. The minimum value is -12 hours, and the maximum value is +12 or +14 hours.</p> <p>The LPAR manager system time zone is set in the SEL time zone while LPAR is being created.</p>	+ 0:00
11	Adjust LPAR Time	<p>Adjust the RTC time and the SEL time of an LPAR to the LPAR manager system time or the UTC time.</p> <p>When doing so, the RTC time when the LPAR to change was last activated and deactivated, and when last updated are also cleared.</p> <p>Move the cursor to Adjust LPAR Time, and then press Enter. On the displayed Select Source time to adjust LPAR time sub-screen, you can set the time source.</p> <p>LP System Time</p> <p>Adjust the RTC time and the SEL time of an LPAR to the LPAR manager system time. When adjusting the time to the LPAR manager system time from the NTP server, set the "TimeSync" item for adjusting the time by using the management module.</p> <p>Specified Zone</p> <p>Adjust the RTC time and the SEL time of an LPAR to the LPAR manager system time in the specified time zone.</p> <p>When Specified Zone is selected, set the time zone, and then press Enter.</p> <p>UTC</p> <p>Adjust the RTC time and the SEL time of an LPAR to UTC time.</p> <p>Table 10-28 Examples of using Adjust LPAR Time and the time source (LP System Time, Specified Zone, and UTC) on page 10-73 provides examples of using Adjust LPAR Time, and the time source (LP System Time, Specified Zone, and UTC).</p> <p>Select the time source, and then press Enter. On the displayed Time Adjust LPAR sub-screen, you can set the target LPAR, or the time zone from the time setting sub-screen.</p> <p>If you select LP System Time on the Time Adjust LPAR sub-screen, you can select the target LPAR.</p> <p>All LPAR</p> <p>Adjust the time of all LPARs.</p> <p>LPAR name</p> <p>Adjust the time of the LPAR you selected.</p>	--

No.	Item	Description	Initial value
		On the LPAR manager Menu screen, press F9 to save the configuration information.	
12	Select Setting Display	<p>Select to display NTP settings.</p> <p>Move the cursor to Setting or NTP, and then press Enter. On the displayed Select Setting Display sub-screen, you can specify the NTP display settings.</p> <p>Setting</p> <p>Displays Import Config and TimeSync.</p> <p>NTP</p> <p>Displays NTP Server 1 and NTP Server 2.</p>	Setting
13	Import Config	<p>Select the import source of NTP settings. ²</p> <p>Move the cursor to Import Config, and then press Enter. On the displayed Select Time Setting Import sub-screen, you can select the import source of NTP settings.</p> <p>None</p> <p>NTP settings are not imported.</p> <p>SVP</p> <p>Imports NTP settings and the time zone of the management module.</p> <p>BMC</p> <p>Imports NTP settings and the time zone of BMC.</p>	None
14	TimeSync	<p>Select time synchronization settings by using the NTP server. ³</p> <p>Move the cursor to TimeSync, and then press Enter. On the displayed Select NTP Server sub-screen, you can select time synchronization settings by using the NTP server.</p> <p>Disable</p> <p>The NTP server does not adjust the time.</p> <p>NTP</p> <p>The NTP server adjusts the time set for NTP servers 1 and 2.</p> <p>SVP</p> <p>Uses the NTP server set for the management module to adjust the time.</p> <p>The NTP server synchronizes the LPAR manager system time immediately after LPAR manager starts, and then every 15 minutes.</p>	Disable
15	NTP Server 1, NTP Server 2	<p>Set the IP address of the NTP server. ⁴On the NTP Server 1 or NTP Server 2 sub-screen that is displayed by pressing Enter, you can set the IP address of the NTP server.</p> <p>Enabled only when TimeSync is NTP.</p> <p>Set the NTP server for NTP Version 3 or 4.</p> <p>To cancel the NTP server settings, delete the IP address of the NTP server on the NTP Server 1 or NTP Server 2 sub-screen, and then press Enter. When the settings are canceled, None appears.</p>	None

No.	Item	Description	Initial value
16	Function Key	<p>Displays the function keys that can be used on the Date and Time screen.</p> <p>F6⁵</p> <p>Change the LPAR manager system time. On the displayed Change System Date and Time sub-screen, you can set the LPAR manager system time.</p> <p>F7</p> <p>Change the LPAR manager system time zone.</p>	--

Notes:

- The SEL time zone for LPARs and LPAR manager system time zone must match. If they do not match, the SEL time of an LPAR does not show the correct time, and you cannot determine the correct time when a failure occurred.
If the times match, there is no problem.
- When importing system synchronization settings from the management module or BMC, make sure there is no problem in system synchronization settings of the import source.
 - The setting values for NTP server 2, and NTP server 3 of the management module are not imported.
 - On LPAR manager, only the hour part of the imported time value is valid on (the minutes part is ignored).
 - Daylight saving time is not supported.

Move the cursor to Import Config, and then press **Enter**. On the displayed Select Time Setting Import sub-screen, you can select the import source of NTP settings.

After selecting the import source, save the configuration information by pressing **F9** on the LPAR manager Menu screen.

[Describes the display on the Date and Time screen when the time setting of the management module is imported.](#)

[Describes the display on the Date and Time screen when the time setting of BMC is imported.](#)

- When adjusting the time by using the management module (recommended):
 - Shut down all guest OS.
 - Move the cursor to **LPAR RTC**, and then press **Enter**. On the displayed **Select Display Time** sub-screen, select **LPAR SEL Time**.
 - Move the cursor to **Time Zone**, and then press **Enter**. On the displayed time zone sub-screen, you can set the time zone.
 - Move the cursor to **LPAR SEL Time**, and then press **Enter**. On the displayed **Select Display Time** sub-screen, select **LPAR RTC**.
 - Move the cursor to **TimeSync**, and then press **Enter**. On the displayed **Select NTP Server** sub-screen, select **Disable**.

When NTP linkage is activated, the time zone cannot be changed. Therefore, you must disable NTP linkage.

```

|| 7 ||
|| 8 ||
|| 9 ||
||10 ||
+-----+
| Select NTP Server |
| Disable          |
| NTP              |
| SVP              |
| e Up / [PageDown]:Page Down |
+-----+
+- System Date and Time -+
|| Date and Time 2014/09/03 15:23:17 Time Zone + 9:00 Adjust LPAR Time ||
+-Setting-+
|| Import Config None ||
|| TimeSync Disable  ||
+-----+

```

- On the time zone sub-screen, which is displayed by pressing **F7**, set the time zone.

No.	Item	Description	Initial value
7.		Move the cursor to Setting , and then press Enter . On the displayed Select Setting Display sub-screen, select Setting .	
		<pre> 7 8 Select Setting Display 9 10 Setting NTP p / [PageDown]:Page Down +-----+ + System Date and Time + Date and Time 2014/09/03 15:21:13 Time Zone + 9:00 Adjust LPAR Time + Setting + Import Config None + TimeSync Disable </pre>	
8.		Move the cursor to TimeSync , and then press Enter . On the displayed Select NTP Server sub-screen, select SVP .	
		<pre> 7 8 Select NTP Server 9 10 Disable NTP SVP le Up / [PageDown]:Page Down +-----+ + System Date and Time + Date and Time 2014/09/03 15:23:17 Time Zone + 9:00 Adjust LPAR Time + Setting + Import Config None + TimeSync Disable </pre>	
		On the System Service State screen, make sure NTP is set to "SYNC".	
		<pre> +-----+ + System Service + SVP Access : RUN + Mgmt I/F : RUN + HA Monitor : RUN + NTP : SYNC + Force Recovery +-----+ + Virtual LAN Segment State + PORT#/NIC# : V 1 2 3 4 5 6 7 8 + a : D A D + b : D A D + c : D + d : D + e : + f : + g : + h : </pre>	
9.		On the Date and Time screen, use Adjust LPAR Time to adjust the LPAR time.	
10.		On the LPAR manager Menu screen, press F9 to save the configuration information.	
		When adjusting the time using the NTP server set for NTP Server 1 and NTP Server 2:	
1.		Shut down all guest OSs.	
2.		Move the cursor to LPAR RTC, and then press Enter . On the displayed Select Display Time sub-screen, select LPAR SEL Time .	
3.		Move the cursor to Time Zone , and then press Enter . On the displayed time zone sub-screen, you can set the time zone.	
4.		Move the cursor to LPAR SEL Time, and then press Enter . On the displayed Select Display Time sub-screen, select LPAR RTC .	
5.		Move the cursor to TimeSync , and then press Enter . On the displayed Select NTP Server sub-screen, select Disable .	
		When NTP linkage is activated, the time zone cannot be changed. Therefore, you must disable NTP linkage.	
6.		On the time zone sub-screen, which is displayed by pressing F7 , set the time zone.	
7.		Move the cursor to Setting, and then press Enter . On the displayed Select Setting Display sub-screen, select NTP .	

No.	Item	Description	Initial value
		<pre> 7 8 9 10 +-----+ Select Setting Display +-----+ +-----+ System Date and Time Date and Time 2014/09/03 15:21:13 Time Zone + 9:00 Adjust LPAR Time Setting Import Config None TimeSync Disable +-----+ </pre>	
8.	Set the IP address of the NTP server.	<pre> +-----+ System Date and Time Date and Time 2014/09/03 15:21:24 Time Zone + 9:00 Adjust LPAR Time NTP (Disable) NTP Server 1 XXX.XXX.XXX.XXX NTP Server 2 XXX.XXX.XXX.XXX +-----+ </pre>	
9.	Move the cursor to NTP, and then press Enter . On the displayed Select Setting Display sub-screen, select Setting .		
10.	Move the cursor to TimeSync , and then press Enter . On the displayed Select NTP Server sub-screen, select NTP .		
11.	On the System Service State screen, make sure NTP is set to SYNC.		
12.	On the Date and Time screen, use Adjust LPAR Time to adjust the LPAR time.		
13.	On the LPAR manager Menu screen, press F9 to save the configuration information.		
4.	<ul style="list-style-type: none"> When setting the IP address of the NTP server, make sure that there is no problem with NTP and time zone settings of the NTP server. An error occurs if you enter a value other than the IP address (in XXX.XXX.XXX.XXX format). 		
5.	Set in advance the system equipment time to use in the range from 2000 to 2037. If it is not set, normal operation of time setting processing on this screen cannot be guaranteed.		
	<p>In addition, when setting the SEL time or the System Manager system time of an LPAR on this screen, you can set a value within the range from years 2000 to 2099. However, if the time when setting the time is later than year 2037, normal operation of the LPAR manager time setting cannot be guaranteed. Therefore, when setting the time, use the value that does not exceed year 2037 while LPAR manager is running.</p>		

Table 10-26 Display on the Date and Time screen when the time setting of the management module is imported

Management module time setting		Date and Time screen			
		Import Config	TimeSync	NTPServer 1	NTPServer 2
Time synchronization setting	Disable	SVP	Disable	NTP server 0	NTP server 1
	Enabled	SVP	NTP	NTP server 0	NTP server 1

Table 10-27 Display on the Date and Time screen when the time setting of BMC is imported by using Import Config

BMC time setting		Date and Time screen			
		Import Config	TimeSync	NTP Server 1	NTP Server 2
Time adjustment method	Adjust the time to the management module by using NTP	BMC	SVP	None	None

The following table describes examples of using Adjust LPAR Time (LP System Time, Specified Zone, and UTC).

Table 10-28 Examples of using Adjust LPAR Time and the time source (LP System Time, Specified Zone, and UTC)

Guest OS timer mode	Guest OS time zone	Adjust LPAR Time		
		LP System Time	Specified Zone	UTC
LocalTime	Same time zone as LPAR manager	Y	N	N
	Different time zone from LPAR manager	N	Y	N
	Guest OS time zone is unknown.	N	N	N
UTC	Same time zone as LPAR manager	N	N	Y
	Different time zone from LPAR manager	N	N	Y
	Guest OS time zone is unknown.	N	N	Y
Unknown	Same time zone as LPAR manager	N	N	N
	Different time zone from LPAR manager	N	N	N
	Guest OS time zone is unknown.	N	N	N
Legend:				
Y: Use Adjust LPAR Time to adjust the time.				
N: Do not use Adjust LPAR Time, and use the guest EFI or guest OS to adjust the time.				

The following table describes the LPAR status for the items on the Date and Time screen.

Table 10-29 LPAR status for the items on the Date and Time screen

Item		LPAR status			Remarks
		Activated	Deactivated	Failed	
LPAR Date and Time	Select Display	Y	Y	Y	--
	Name	N	N	N	Display only
	Sta	N	N	N	Display only

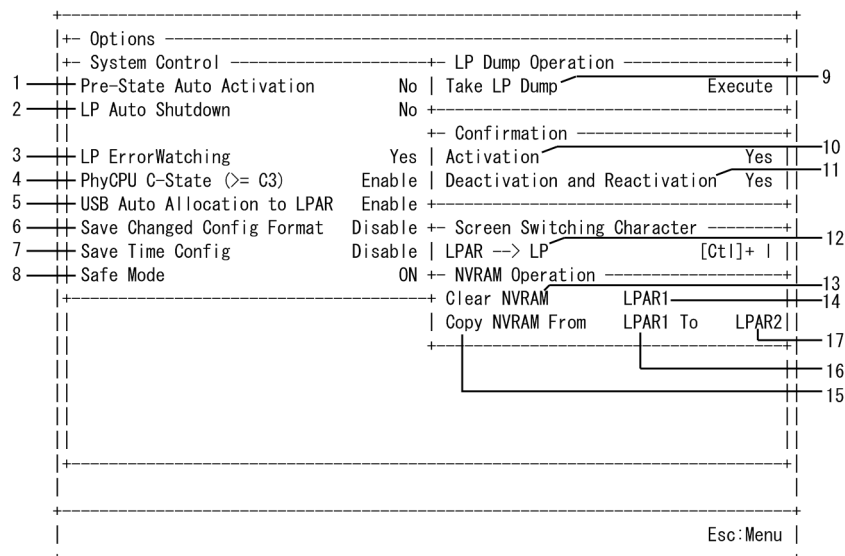
Item		LPAR status			Remarks
		Activated	Deactivated	Failed	
	Time Mode	N	C	N	Only when the time display is LPAR SEL Time
	Date and Time	N	C	N	Only when the time display is LPAR SEL Time
	Time Zone	N	C	N	Only when the time display is LPAR SEL Time Only when the SEL time mode is Local-Time
	Current RTC Init RTC	N	N	N	Display only
System Date and Time	Date and Time	C	C	C	Only when TimeSync is disabled
	Time Zone	C	C	C	Only when TimeSync is disabled
	Adjust LPAR Time	N	Y	N	--
	Select Setting Display	Y	Y	Y	--
	Import Config	Y	Y	Y	--
	TimeSync	Y	Y	Y	--
	NTP Server 1, NTP Server 2	Y	Y	Y	--
Legend: Y: Can be changed N: Cannot be changed C: Can be changed with conditions					

Related topics

- [LPAR manager Menu screen on page 10-5](#)
- [System Service State screen on page 10-58](#)

LP Options screen

The following figure shows the LP Options screen.



On the LP Options screen, the following operations can be performed:

- Restoring the status before restarting the LPAR
- Changing the setting to restore setting before restarting LPAR
- Changing the method for shutting down LPAR manager automatically
- Detecting LPAR manager hang up
- Changing the power saving functionality
- Changing the target LPARs for the USB Auto Attach functionality
- Changing the functionality for automatically saving configuration information
- Changing the functionality for saving time information automatically
- Changing Safe Mode to OFF.
- Collecting LPAR manager dumps

The following table describes the items on the LP Options screen.

Table 10-30 Items on the LP Options screen and their descriptions

No.	Item	Description	Initial value
1	Pre-State Auto Activation ¹	<p>Set whether to restore the status before restarting the LPAR if you restart LPAR manager without shutting it down.</p> <p>Move the cursor to Pre-State Auto Activation, and then press Enter. On the displayed AutoAct Setting sub-screen, you can specify the setting.</p> <p>Yes</p> <p>Restores the LPAR status before restarting LPAR manager.</p> <p>No</p> <p>Does not restore the LPAR status before restarting LPAR manager.</p>	No

No.	Item	Description	Initial value
		Rebooting LPAR manager without shutting down occurs in the following cases. <ul style="list-style-type: none"> N+M cold standby starts Hardware failure LPAR manager error Power supply controller failure 	
2	LP Auto Shutdown	Set whether to shut down LPAR manager if all LPARs are deactivated. ² Move the cursor to LP Auto Shutdown, and then press Enter . On the displayed AutoShutdown Setting sub-screen, you can specify the setting. Yes Shuts down LPAR manager. No Does not shut down LPAR manager.	No
3	LP ErrorWatching	Set whether to detect the hang up state of LPAR manager. Move the cursor to LPAR manager ErrorWatching, and then press Enter . On the displayed ErrorWatching Setting sub-screen, you can specify the setting. Yes Detects LPAR manager hang up. If detected, LPAR manager dumps are automatically collected, and LPAR manager is restarted. No Does not detect LPAR manager hang up.	Yes
4	PhyCPU C-State (>= C3)	Set whether to enable the power saving functionality. ³ Move the cursor to PhyCPU C-State (>= C3), and then press Enter . On the displayed Physical CPU C-State (>=C3) Setting sub-screen, you can specify the setting. Enable Enables the power saving functionality. Disable Disables the power saving functionality.	Enable
5	USB Auto Allocation to LPAR	Set the target LPARs for the USB Auto Attach functionality. A USB device which is in exclusively shared mode and is not attached to any LPARs is automatically attached to the target LPAR when the LPAR is activated or reactivated. Move the cursor to USB Auto Allocation to LPAR, and then press Enter . On the displayed USB Auto Allocation Setting sub-screen, you can specify the setting. Enable All LPARs are targeted. Disable	Enable

No.	Item	Description	Initial value
		Only the LPAR you specified is targeted. For details about how to specify an LPAR, see PCI Device Assignment screen on page 10-30 .	
6	Save Changed Config Format	<p>If configuration format conversion is not saved when LPAR manager starts, set whether to save the configuration information automatically.</p> <p>Move the cursor to Save Changed Config Format, and then press Enter. On the displayed Save Changed LPAR manager Configuration Format Setting sub-screen, you can specify the setting.</p> <p>Enable</p> <p>Enables the functionality for saving configuration information automatically.</p> <p>Disable</p> <p>Disables the functionality for saving configuration information automatically.</p> <p>The functionality for saving configuration information automatically does not save it automatically and regularly.</p>	Disable
7	Save Time Config	<p>Set whether to save the corrected time information in the physical RTC and LPAR manager configuration information automatically if the LPAR manager system time and LPAR time are corrected. ⁴</p> <p>Enable</p> <p>Enables the functionality for saving time information automatically. We recommend this setting.</p> <p>Disable</p> <p>Disables the functionality for saving time information automatically.</p>	Disable
8	Safe Mode	<p>LPAR manager firmware versions 02-20 or later</p> <p>Displays whether safe mode is enabled. Move the cursor to Safe Mode, and then press Enter. A sub-screen appears. Select Yes and press Enter to exit safe mode.</p> <p>ON</p> <p>LPAR manager is running in safe mode.</p> <p>OFF</p> <p>LPAR manager is running in normal mode.</p>	OFF
9	Take LP Dump	<p>Collects LPAR manager dumps.</p> <p>Use the LPAR manager dumps collected by performing this operation to analyze a failure when it occurs.</p> <p>Under normal operation, it is not necessary to collect LPAR manager dumps. If an error occurs in the equipment, we might ask you to collect LPAR manager dumps.</p> <p>Move the cursor to Execute of Take LP Dump, and then press Enter. On the displayed If there was LP Dump file, it will be overwritten. Do you want to continue? sub-screen, you can specify the setting. For details, see Collecting LPAR manager dumps on page 9-18.</p>	Execute

No.	Item	Description	Initial value
10	Activation	<p>When you perform activation on the LPAR manager screen, set whether to display the confirmation sub-screen.</p> <p>Move the cursor to Activation, and then press Enter. On the displayed Activation confirmation sub-screen, you can specify the setting.</p> <p>Yes</p> <p>Displays the confirmation sub-screen.</p> <p>No</p> <p>Does not display the confirmation sub-screen.</p> <p>In addition, if you activate an LPAR and select Continue(Don't show this message) on the confirmation screen, the confirmation screen will not be displayed.</p>	Yes
11	Deactivation and Reactivation	<p>When you perform deactivation and reactivation on the LPAR manager screen, set whether to display the confirmation sub-screen.</p> <p>Move the cursor to Deactivation and Reactivation, and then press Enter. On the displayed Deactivation confirmation sub-screen, you can specify the setting.</p> <p>Yes</p> <p>Displays the confirmation sub-screen.</p> <p>No</p> <p>Does not display the confirmation sub-screen.</p> <p>Alternatively, if you deactivate an LPAR and select Yes(Don't ask anymore) on the confirmation sub-screen, the confirmation screen will not be displayed after that. If you reactivate an LPAR and select Yes(Don't ask anymore) on the confirmation screen, the confirmation screen will not be displayed after that.</p>	Yes
12	Screen Switching Character	<p>Set a character used to switch from the guest screen to the LPAR manager screen. By default, "l" (lower case "L") is set.</p> <p>Characters you can set</p> <p>Lower-case alphabetical except b, h, i, j, m, q, s, and z.</p> <p>Move the cursor to Ctrl +l, and then press Enter. On the displayed Screen Switching Character sub-screen, you can specify the setting.</p>	l
13	Clear NVRAM	<p>Initialize NVRAM for the LPAR displayed to the right of this item.</p> <p>When "Select" is displayed instead of an LPAR, this operation cannot be performed (the cursor does not move).</p> <p>Operation when Clear NVRAM is performed</p> <ul style="list-style-type: none"> • EFI driver settings: Not initialized • Boot order: Initialized 	--
14	<i>LPAR to be initialized</i>	<p>Displays the LPAR to be initialized for NVRAM.</p> <p>This setting can be specified for deactivated LPARs. If LPAR is not defined, or all LPARs for which LPAR is defined are activated, "Select" is displayed.</p>	--

No.	Item	Description	Initial value
		When the set LPAR is activated, it is changed to a deactivated LPAR automatically.	
15	Copy NVRAM	<p>Copies the content of the NVRAM for the LPAR displayed in From, to the NVRAM for the LPAR displayed in To.</p> <p>When Select is displayed in From or in To instead of an LPAR, this operation cannot be performed (the cursor does not move).</p> <p>Operation when Copy NVRAM is performed</p> <ul style="list-style-type: none"> EFI driver setting: Not copied Boot order: Copied 	--
16	<i>LPAR of copy source</i>	<p>Displays the LPAR that is the copy source for copying NVRAM contents.</p> <p>When the LPAR is not defined, Select is displayed.</p>	--
17	<i>LPAR of copy destination</i>	<p>Displays the LPAR that is the copy destination for copying NVRAM contents.</p> <p>This setting can be specified for deactivated LPARs. If LPAR is not defined, or all LPARs for which an LPAR is defined are activated, "Select" is displayed.</p> <p>When the set LPAR is activated, it is changed to a deactivated LPAR automatically.</p>	--

Notes:

1. What is Pre-State Auto Activation

When an LPAR is activated or deactivated, and the status is confirmed, the LPAR status is saved. If a power failure occurs, or LPAR manager is restarted after a server blade is forcibly turned off, the LPAR is activated automatically in the saved state and the status before restarting the LPAR is restored.

- When the LPAR manager start up after shutting down normally, the setting of **Pre-State Auto Activation** is ignored. LPARs are automatically activated in the setting order of **Auto Activation Order** in the **Logical Partition Configuration** screen.
- For auto-activation by using **Pre-State Auto Activation**, LPARs are activated in ascending order of LPAR number. At that time, the **Auto Activation Order** setting is not applied.

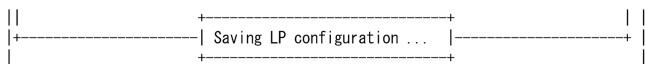
However, if the following LPARs exist, LPARs are automatically activated in a different order:

- In **MN** (memory node) of the **Logical Partition Configuration** screen, a memory node number is set for an LPAR.
- NUMA is enabled for an LPAR.

In such a case, LPARs are activated in the order of the attribute groups below. Note that, for LPARs that belong to the same attribute group, they are activated in ascending order of LPAR number.

- LPARs for which the memory node number is set
LPARs for which NUMA is enabled, and bind physical processors
- LPARs for which NUMA is enabled, and bind physical NUMA nodes
- LPARs that do not meet the above conditions

If an LPAR cannot be activated for any reason, such as no allocation memory can be reserved, the LPAR is no longer activated automatically.

No.	Item	Description	Initial value
		<p>For 15 seconds before starting auto-activation, you can cancel auto-activation. If you want to cancel auto-activation, press Ctrl + c during this period. Note that once auto-activation is started, you cannot cancel it.</p> <p>2. To turn off the system equipment by using UPS, set LP Auto Shutdown to Yes.</p> <p>3. If all the following conditions are met, the time lag of the OS system might increase. If this happens, disable the power saving functionality.</p> <ul style="list-style-type: none"> Use Windows Server 2008 R2 or later. An application program that uses a multimedia timer, such as Media Player, is running. <p>To change the power saving functionality, you must deactivate all LPARs.</p> <p>4. When Save Time Config is disabled, if you use LPAR manager for a long time, and then restart it (due to, for example, unexpected LPAR manager system failure or N + M failover), there will be a time lag in the guest OS time.</p> <p>Save Time Config settings can be changed while the LPAR is running.</p> <p>When Save Time Config is enabled, the LPAR manager configuration information is saved automatically when the time is corrected (the timing cannot be identified). But if LPAR manager configuration or LPAR configuration is changed, you must save the LPAR manager configuration information when the change operation is completed.</p> <p>After LPAR manager configuration information is saved when the time is corrected, the LPAR manager screen opens, the system event log is collected, and an alert is issued. These operations can be suppressed by disabling Save Time Config.</p> <ul style="list-style-type: none"> <LPAR manager screen> <div>  </div> <System event log> <div> <pre> + LP System Logs ----- All level -+ Level Date Time Event Info. 2014/09/03 14:58:18 LP saved configuration. Info. 2014/09/03 14:58:12 LP saved configuration. Info. 2014/09/03 14:57:56 LP saved configuration. Info. 2014/09/03 14:42:27 LP detected available Shared FC Link. </pre> </div> <Alert> <div> <p>ID: 0x1531</p> <p>Message: LP configuration was saved. (RC=6)</p> <p>This alert is displayed for HCSM.</p> </div> 	

When NTP is used

- On the Date and Time screen, check the LPAR manager system time. If there is a time lag in LPAR manager system time, remove the lag by restoring the network status of the NTP server.
- On the Date and Time screen, set the time of deactivated LPARs by performing Adjust LPAR Time (LP System Time, Specified Zone, UTC). Check the time zone of the guest OS, perform Adjust LPAR Time in the same time zone as the guest OS.
Set the time of activated LPARs by using the guest OS or NTP time synchronization of a guest.

No.	Item	Description	Initial value
		"---" is displayed.	
7	Srv(%)	<p>In shared mode</p> <p>Displays the service time ratio of the applicable LPAR against the total value of the service time owned by a normally running physical processor assigned to the LPAR in shared mode.</p> <p>If the service percentage calculated within LPAR manager does not match the service ratio percentage, an asterisk (*) is displayed to the right. If they match, an asterisk (*) is not displayed.</p> <p>For Grp (ALL)</p> <p>"---" is displayed.</p> <p>In dedicated mode, "---" is displayed.</p>	--
8	Srv(ms)	<p>The total service time for the applicable LPAR is displayed in milliseconds.</p> <p>In dedicated mode</p> <p>The value for the field is calculated as follows:</p> $\text{Srv(ms)} = \text{number-of-normally-running-physical-processors-of-applicable-LPAR} \times 1000$ <p>In shared mode</p> <p>The value for the field is calculated as follows:</p> $\text{Srv(ms)} = \text{number-of-normally-running-physical-processors-assigned-to-LPAR-in-shared-mode} \times \text{Srv(\%)-of-applicable-LPAR} \times 1000$ <p>At that time, if Srv(%) shows "*", an asterisk (*) is displayed to the right of this field.</p>	--
9	Dsp(ms)	<p>Displays the execution time for the applicable LPAR in milliseconds.</p> <p>This is the total execution time of logical processors that belong to the applicable LPAR.</p> <p>If either of the following is met, the value is the same as Srv(ms) because logical processors are always being dispatched to physical processors.</p> <ul style="list-style-type: none"> • N is selected for ID on the Logical Partition Configuration screen. • MWAIT is selected for Guest Idle Mode. 	--
10	Busy(%)	<p>Displays the busy ratio of the applicable LPAR. This is the ratio of the execution time for the service time of the applicable LPAR.</p> <p>How to calculate the busy ratio</p> $\text{Busy(\%)} = \text{execution-time-of-applicable-LPAR} / \text{service-time-of-applicable-LPAR} \times 100$ <p>Use the value of this field as a guideline when changing resources. If the value of this field exceeds 100 percent, the LPAR is running out of resources.</p> <p>When the processor capping functionality is enabled, the busy ratio is controlled so that it does not exceed 100 percent. Because of this, you cannot use the value of this field as a guideline when changing resources.</p> <p>When processor capping is enabled, due to a margin of LPAR manager service ratio control, a maximum of one percent of the total value of the service time owned by normally running physical processors assigned to an LPAR in shared mode. As a result, the busy ratio might exceed 100 percent.</p>	--
11	Dsp(%)	In shared mode	--

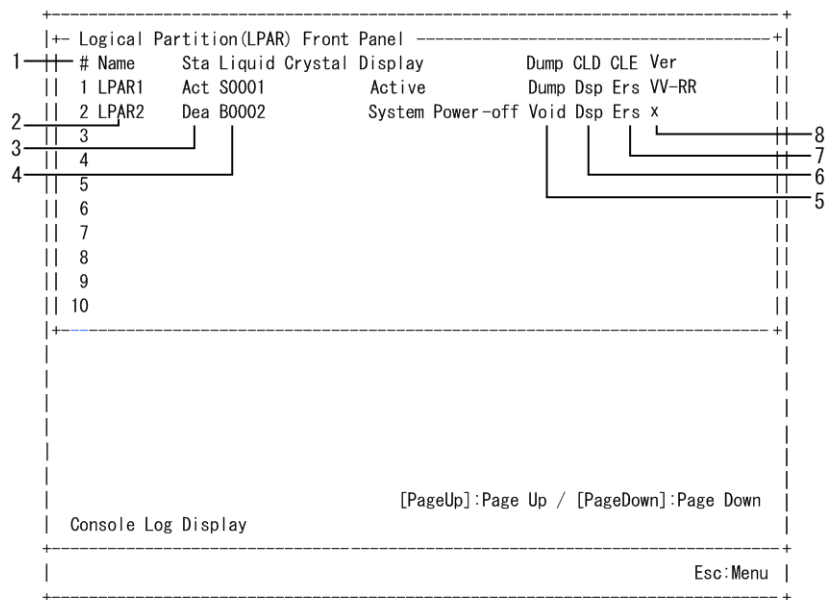
No.	Item	Description	Initial value
		<p>Displays the service time ratio of the applicable LPAR against the total value of the service time owned by normally running physical processors assigned to an LPAR in shared mode.</p> <p>The value for the field is calculated as follows:</p> $\text{Dsp(\%)} = \frac{\text{execution-time-of-applicable-LPAR}}{\text{total-value-of-service-time-owned-by-normally-running-physical-processor-assigned-to-LPAR-in-shared-mode}} \times 100$ <p>For Grp(ALL), "---" is displayed.</p> <p>In dedicated mode "---" is displayed.</p>	
12	PC	<p>Displays the setting status of the processor capping functionality set on the Logical Partition Configuration screen.</p> <p>Y Processor capping is enabled in shared mode.</p> <p>N Processor capping is disabled in shared mode.</p> <p>* Processor capping is disabled in dedicated mode.</p> <p>-- The applicable LPAR is not activated.</p>	--
13	Sampling time	<p>Sets the update interval of the LPAR Usage screen in seconds.</p> <p>A value from 1 to 60 can be set as the update interval.</p> <p>Move the cursor to Sampling time, and then press Enter. On the displayed Change Interval Time sub-screen, you can set the update interval of the LPAR Usage screen.</p>	5
14	Proc	<p>Displays the number of physical processors assigned to dedicated and shared modes.</p> <p>D Displays the total number of physical processors assigned to dedicated mode. The format is "<i>n (m)</i>". <i>n</i>: Displays the total number of normally running physical processors assigned to dedicated mode. <i>m</i>: Displays the total number of all physical processors assigned to dedicated mode.</p> <p>S Displays the number of physical processors assigned to shared mode. The format is "<i>n (m)</i>". <i>n</i>: Displays the total number of normally running physical processors assigned to dedicated mode. <i>m</i>: Displays the total number of all physical processors assigned to shared mode.</p> <p>S = total-number-of-physical-processors - total-number-of-physical-processors-assigned-to-dedicated-mode</p>	--

No.	Item	Description	Initial value
15	Grp	<p>Selects the processor group to display.</p> <p>All</p> <p>Displays the entire system.</p> <p>Processor group number</p> <p>Displays the processor group specification.</p> <p>When the processor group number is specified, only information belonging to the group is displayed.</p> <p>Move the cursor to Grp, and then press Enter. On the displayed Change Group Number sub-screen, you can set the processor group number.</p>	All
16	Ded LPAR Total	<p>Displays various total number values in dedicated mode.</p> <ul style="list-style-type: none"> • "---" is displayed for SrvRatio and Srv(%). • For Srv(ms), the total value of the service hours in dedicated mode is displayed. • For Dsp(ms), the total value of the execution time in dedicated mode is displayed. • For Busy(%), the total value of the busy ratio in dedicated mode is displayed. <p>How to calculate the field value</p> $\text{Busy(\%)} = \frac{\text{total-value-of-execution-time-of-LPAR-in-dedicated-mode}}{\text{total-value-of-service-time-of-LPAR-in-dedicated-mode}} \times 100$	--
17	Shr LPAR Total	<p>Displays various total values in shared mode.</p> <ul style="list-style-type: none"> • For SrvRatio, the total value of SrvRatio in shared mode is displayed. • For Grp (ALL), "---" is displayed. • For Srv(%), the total value of Srv(%) in shared mode is displayed. If the Srv(%) value with an asterisk (*) is included in the LPAR in shared mode, an asterisk (*) is displayed to the right of the value. • For Grp (ALL), "---" is displayed. • For Srv(ms), the total service time in shared mode is displayed. If the Srv(ms) value with an asterisk (*) is included in the LPAR in shared mode, an asterisk (*) is displayed to the right of the value. • For Dsp(ms), the total execution time in shared mode is displayed. • For Busy(%), the total busy ratio in shared mode is displayed. <p>How to calculate the field value</p> $\text{Busy(\%)} = \frac{\text{total-value-of-execution-time-of-LPAR-in-shared-mode}}{\text{total-value-of-service-time-of-LPAR-in-shared-mode}} \times 100$	--
18	LPAR Total	<p>Displays various total values of all LPARs.</p> <ul style="list-style-type: none"> • For Dsp(ms), the total execution time of all LPARs is displayed. • For Busy(%), the total busy ratio of all LPARs is displayed. <p>How to calculate the field value</p> $\text{Busy(\%)} = \frac{\text{total-value-of-execution-time-of-all-LPAR}}{\text{system-service-time}} \times 100$	--
19	SYS1	<p>Displays the execution time and the busy ratio.</p> <ul style="list-style-type: none"> • SYS1 indicates processing of the LPAR manager kernel component. 	--

No.	Item	Description	Initial value
		<p>The execution time and the busy ratio of an isolated failed processor are included in SYS1.</p> <ul style="list-style-type: none"> For Dsp(ms), the execution time of SYS1 is displayed. For Busy(%), the busy ratio of SYS1 is displayed. <p>How to calculate the field value</p> $\text{Busy(\%)} = \text{execution-time-of-SYS1} / \text{system-service-time} \times 100$	
20	SYS2	<p>Displays the execution time and the busy ratio.</p> <ul style="list-style-type: none"> SYS2 indicates processing of LPAR manager communication and service control components. For Dsp(ms), the execution time of SYS2 is displayed. For Busy(%), the busy ratio of SYS2 is displayed. <p>How to calculate the field value</p> $\text{Busy(\%)} = \text{execution-time-of-SYS2} / \text{system-service-time} \times 100$	--
21	System Total	<p>Displays the system service time, system busy time, and system busy ratio.</p> <ul style="list-style-type: none"> For Srv(ms), the system service time is displayed. This value is the total service time owned by the normally running physical processors in the system, and is calculated as follows: $\text{Srv(ms)} = \text{number-of-normally-running-physical-processors} \times 1000$ For Dsp(ms), the system busy time is displayed. This value is the total execution time for all LPARs, and the execution time of SYS1 and SYS2. For Busy(%), the system busy ratio is displayed. This is the busy ratio across the system, and the value for this field is calculated as follows: $\text{Busy(\%)} = \text{system-busy-time} / \text{system-service-time} \times 100$ 	--

Front Panel screen

The following figure shows the Front Panel screen.



On the Front Panel screen, the following operations can be performed:

- Checking the system status of the LPAR
- Collecting the guest OS dump
- Collecting guest screen data (console log data)
- Removing guest screen data (console log data)
- Restoring the Migration Failed LPAR



Tip:

Console log data indicates the screen data that is output when a guest OS is executed. LPAR manager saves character data of screen data in an internal buffer (up to 1500 lines). If the amount of console log data exceeds 1500 lines, data is overwritten in the order from oldest.

The following table describes the items on the Front Panel screen.

Table 10-32 Items on the Front Panel screen and their descriptions

No.	Item	Description	Initial value
1	#	Displays the LPAR number.	--
2	Name	Displays the LPAR name.	NO_NAME
3	Sta	Displays the power status of an LPAR. Act (Activated) The LPAR is turned on. Dea (Deactivated) The LPAR is turned off. Fai (Failure) The LPAR cannot be used due to an unrecoverable failure.	Dea

No.	Item	Description	Initial value
4	Liquid Crystal Display	Displays the LPAR system status or error information. Active The LPAR is turned on. System Power-off The LPAR is turned off. Ignite dump Indicates the status when dumps were collected.	--
5	Dump ^{1, 2}	Instructs the guest OS to collect dumps. Move the cursor to the Dump column of the LPAR row, and then press Enter . On the displayed Dump logical partition sub-screen, select Yes to collect dumps. You can collect dumps only when the applicable LPAR is activated.	Void/Dump
6	CLD	Displays the selected guest screen data (console log data). Move the cursor to the CLD column of the LPAR row, and then press Enter . On the displayed Console Log Display sub-screen, if you select Yes, you can collect console log data. It takes a few minutes to display the entire log. During the period, no LPAR manager manipulation can be performed. Note that if the applicable LPAR guest screen is updated when the console log is displayed, the updated contents might not be applied to the log. To collect console log data, display the console log data on the screen, and collect the guest screen data as scroll buffer data of the terminal software. The collected screen data can be viewed.	Dsp
7	CLE	Removes the selected guest screen data (console data) from the buffer within LPAR manager. Move the cursor to the CLE column of the LPAR row, and then press Enter . On the displayed Console Log Erase sub-screen, you can remove the console log data.	Ers
8	Ver	[LPAR manager firmware version: 02-28 or later] Displays the LPAR manager firmware version. - Indicates that the LPAR is deactivated. VV-RR Displays the LPAR manager firmware version in which the LPAR is working. <ul style="list-style-type: none"> Displays the oldest LPAR manager firmware version on the LPAR manager that executes concurrent maintenance if the LPAR is migrated through concurrent maintenance. Displays the current LPAR manager firmware version in which the LPAR is working if the LPAR is restarted after it is migrated through concurrent maintenance. x <ul style="list-style-type: none"> Indicates an LPAR for which concurrent maintenance has been executed via an LPAR manager whose firmware version is 02-27 or earlier. 	--

No.	Item	Description	Initial value
		<ul style="list-style-type: none"> If an LPAR for which an "x" is displayed is re-activated, the firmware version of the current LPAR manager is displayed. 	
Notes: 1. To check the status of the guest OS before collecting the dump log, collect the console log data and a logical VGA snapshot image before collecting the dump log of the guest OS. 2. Through operation of collecting guest OS dumps, issue an NMI interrupt to the LPAR.			

The following table lists the LPAR status for the items on the Front Panel screen.

Table 10-33 LPAR status for the items on the Front Panel screen

Item	LPAR status			Remarks
	Activated	Deactivated	Failed	
Name	N	N	N	Display only
Sta	N	N	N	Display only
Liquid Crystal Display	N	N	N	Display only
Dump	Y	N	N	--
CLD	Y	Y	Y	--
CLE	Y	Y	Y	--
Ver	N	N	N	Display only
Legend: Y: Can be changed N: Cannot be changed				

LP System Logs screen

The following figure shows the LP System Logs screen.

- Checking the LPAR manager firmware version, or the internal version of the LPAR manager firmware
- Checking the EFI firmware version
- Checking the BMC firmware version
- Checking the LPAR manager model
- Checking the serial number of LPAR manager
- Checking the validity period of an LPAR manager license
- Checking the fibre channel adapter firmware version

The following table describes the items on the Firmware Version Information screen.

Table 10-35 Items on the Firmware Version Information screen and their descriptions

No.	Item	Description	Initial value
1	LP F/W	Displays the LPAR manager firmware version and the internal version of the LPAR manager firmware.	--
2	BIOS	Displays the EFI firmware version.	--
3	BMC	Displays the BMC firmware version.	--
4	LP Model	Displays the LPAR manager model. Essential Indicates the Essential model. Advanced Indicates the Advanced model. Enterprise Indicates the Enterprise model.	--
5	LP Serial#	Displays the LPAR manager serial number.	--
6	Hitachi Fibre Channel F/W	Displays the firmware version of the fibre channel adapter with the applicable slot number.	--
7	Valid Thru	[LPAR manager firmware version: 02-27 or later] For LPAR manager licenses with a validity period, displays the year, month, and date of expiration. This item is displayed only for the server blades and LPAR manager firmware versions that support a temporary LPAR manager license. YYYY/MM/DD: Indicates the expiration date. Permanent: Indicates that there is no expiration date.	--

LPAR manager sub-screens

This section describes sub-screens of LPAR manager.

Memory Allocation Display sub-screen

The following figure shows the Memory Allocation Display sub-screen.

Memory Allocation Display				3	4	5
2	1	#	Mem Org Addr (Hex)	Mem Size	Node#	Name
		1	00000000 00000000	1024MB	0	SYS2
		2	00000000 40000000	256MB	0	LPAR1
		3	00000000 50000000	768MB	0	SYS1
		4	00000001 00000000	1792MB	0	LPAR1
		5	00000001 70000000	4352MB	0	*****
		6	00000002 80000000	7936MB	1	*****
		7	00000004 70000000	256MB	1	SYS1
		8	----- END -----			

On the Memory Allocation Display sub-screen, the memory allocation status is displayed in ascending order of address.

Items displayed on the Memory Allocation Display sub-screen are explained below.

Items

#

Indicates the serial number of memory blocks to display.

Mem Org Addr (Hex)

Displays the starting address of the allocated memory in hexadecimal. The addresses are listed in ascending order. When there is no more memory allocation information to display, ----- END ----- appears. If there is more than one screen to display, use the **PageUp** or **PageDown** key to change the display.

Mem Size

Displays the memory size in megabytes in decimal.

Node#

Displays the memory node number. If the NUMA setting of the EFI is disabled, '-' is displayed.

Name

According to the addresses listed under Mem Org Addr, indicates the name of the system that uses the memory area listed in Mem Size. SYS1: Used by the LPAR manager kernel component. SYS2: Used by the LPAR manager communication component and service control component. LPARx: Used by the LPAR with the number x. Only activated LPARs are displayed, but LPAR names are not displayed. ISOLATED: Indicates memory that is isolated because a memory failure was detected.

*****: Indicates an unallocated area.

LPAR manager Messages

This chapter describes messages output by LPAR manager and HCSM alarm messages.

- ☐ [LPAR manager boot messages](#)
- ☐ [LPAR manager screen operation messages](#)
- ☐ [LPAR manager system log messages](#)
- ☐ [Audit log messages](#)
- ☐ [HCSM alert messages](#)

LPAR manager boot messages

The following table shows LPAR manager boot messages, which are displayed when LPAR manager is started.

Table 11-1 List of LPAR manager boot messages

Message	Description	Solution
4-SMP with this blade is unsupported. So, the LP can't boot. Reconfigure the server partition.	LPAR manager startup was suppressed because 4-blade SMP configurations are not supported.	Change the server partition to a supported SMP configuration and then start LPAR manager.
Capacity on demand is unsupported.	Capacity on demand is not supported.	Update the LPAR manager to a version supporting the feature.
Connection to SVP is tried again. retryCount=X, statusCode=0xXXXX XXXX: EFI Status code	The operation was retried because communication with the management module failed.	There is no need to take action because the communication is enabled due to a retry. If this LPAR manager system log is collected whenever LPAR manager starts, contact your reseller or maintenance personnel.
Error: Could not allocate memory, error code: [0xXXXX]. XXXX: Memory Allocate Error Code	Memory allocation failed.	On the Web console, check whether memory is being recognized correctly. If memory is not being recognized correctly, contact your reseller or maintenance personnel. If this message appears even when memory is being recognized correctly, contact your reseller or maintenance personnel.
Error: Could not find IPMI Device Information (Type38) in SMBIOS, error code:[0xXXXX]. XXXX: EFI Status code	The IPMI table was not found on SMBIOS.	Contact your reseller or maintenance personnel.
Error: Could not find loader image in Management Module, error code:[0xXXXX]. XXXX: EFI Status code	The LPAR manager loader image was not found in the management module.	Check whether the LPAR manager firmware is installed in the management module. If this message appears even when you cannot find any problems, contact your reseller or maintenance personnel.
Error: Could not find network controller, error code:[0xXXXX]. XXXX: EFI Status code	Communication NIC detection failed.	Check whether there are any problems in the management path

Message	Description	Solution
		configuration and NIC and port settings. If this message appears even when you cannot find any problems, contact your reseller or maintenance personnel.
Error: Could not get ip address from BMC, error code:[0xXXXX]. XXXX: EFI Status code	Acquisition of the IP address from the BMC failed.	On the LPAR manager setting screen of the Web console, check whether the IP address is set correctly. If the IP address is not set correctly, reset the IP address. If this message appears even when the IP address is set correctly, contact your reseller or maintenance personnel.
Error: Could not get loader image size from Management Module, error code:[0xXXXX]. Please check network connection with management module and network settings. XXXX: EFI Status code	Acquisition of the LPAR manager loader image size failed.	Check whether there are any problems in the network or LAN switch settings. If this message appears even when you cannot find any problems, contact your reseller or maintenance personnel.
Error: Could not load loader image from Management Module, error code:[0xXXXX]. Please check network connection with management module and network settings. XXXX: EFI Status code	Reading of the LPAR manager loader failed.	Check whether there are any problems in the network or LAN switch settings. If this message appears even when you cannot find any problems, contact your reseller or maintenance personnel.
Error: Could not set VLAN ID[0xXXXX],Port[0xYY],error code:[0xZZZZ]. XXXX: VLAN ID YY: Port number ZZZZ: EFI Status code	Assignment of the VLAN ID tag failed.	Verify that the VLAN ID is set to a value in the range from 1 to 4094. If this message appears even when you cannot find any problems, contact your reseller or maintenance personnel.
Error: Could not start loader.(XXXX)[0xYYYY] XXXX indicates one of the following reasons: LoadImage Error: Expansion error of the program image that was expanded in memory Handle protocol Error: EFI internal error Start Image Error: LP-Loader execution error YYYY: EFI Status code	The LPAR manager loader failed to start.	Contact your reseller or maintenance personnel.

Message	Description	Solution
Error: Ipmi driver initialization failed, error code:[0XXXXX]. XXXX: EFI Status code	An error was detected before IPMI command execution.	Contact your reseller or maintenance personnel.
Error: Network error occurred,retry after a few seconds.(PortX,Cmd:[0XXXXX],detected code[0XXXXX],error code[0XXXXX])	Because a network error occurred, communication with the management path will be retried at communication port PortX (MGMTX).	Check whether there are any problems in the network or LAN switch settings.
Error: Network error occurred,retry using the other port.(Port0->Port1,Cmd:[0XXXXX],detected code[0XXXXX],error code[0XXXXX])	Because a network error occurred, the communication port will be switched from Port0 (MGMT0) to Port1 (MGMT1), and then communication will be retried.	Check whether there are any problems in the network or LAN switch settings.
Error: Notification to BMC failed. (Step: [0XXXXX],SubStep:[0XXXXX],status: [0XXXXX],code:[0XXXXX]). WWW: Step code	Failed to notify the management module of the operating status.	Access to the BMC failed. If this message appears whenever LPAR manager starts, contact your reseller or maintenance personnel.
LP-Loader could not find any network controller.	Communication NIC detection failed.	Contact your reseller or maintenance personnel.
LP-Loader could not find VfcSeed.dat in management module.	The VfcSeed.dat file, which contains Vfc seed information, could not be found in the management module during N+M cold standby failover.	N+M cold standby failover might have failed. If you cannot find any errors, contact your reseller or maintenance personnel.
LP-Loader could not update OEM FRU.	Update of Vfc seed information for the FRU failed during N+M cold standby failover.	An error might have occurred on the BMC. In addition, the FRU might be damaged. Contact your reseller or maintenance personnel.
LP-Loader detected a value of Emulex NIC(Bus:0xXX) Personality unsupported for this LP. Please reset Emulex NIC Personality to a value supported for the LP. XX: Bus number	LPAR manager cannot start because a value not supported by LPAR manager is set for the Personality for Emulex NIC.	Set a value supported by LPAR manager for the Personality. For details about how to configure this setting, see the manual <i>Hitachi Compute Blade Emulex Adapter User's Guide for Hardware</i> . Note, however, that you cannot change the setting in LP mode. To change the setting, change the mode to Basic mode.

Message	Description	Solution
LP-Loader detected configuration error in management path portX, [Code:X SlotType:XX BladeNo:XX SlotNo:XX PortNo:XX].	A configuration error in the management path was detected.	Check whether there are any problems in the management path configuration and NIC and port settings. If this message appears even when you cannot find any problems, contact your reseller or maintenance personnel.
LP-Loader detected Emulex Multi Channel mode (Bus:0xXX, Dev:0xYY, Fnc:0xZZ), which is not supported. Please disable Emulex Multi Channel mode. XX: Bus number YY: Device number ZZ: Function number	LPAR manager cannot start because MultiChannel Support for Emulex NIC is set to Enabled.	Set MultiChannel Support to Disabled. For details about how to configure this setting, see the manual <i>Hitachi Compute Blade Emulex Adapter User's Guide for Hardware</i> . Note, however, that you cannot change the setting in LP mode. To change the setting, change the mode to Basic mode.
LP-Loader detected invalid configuration files. [version is unmatched] (ErrorCode:XXXXXXXXXXXXXXXXX AdditionalCode:XXXXXXXXXXXXXXXXX) Please Power Off Partition.	LPAR manager cannot start because the configuration files are invalid.	Restore valid configuration files.
LP-Loader detected invalid Virtualization Technology setting in this system. MSR INFO [0XXXXXXXXXXXXXXXXXX] Please set Virtualization Technology setting to enable.	LPAR manager cannot start because Virtualization Technology is set to Disable.	From the EFI setup menu, set Intel Virtualization Technology to Enable. For details about how to configure this setting, see the manual <i>Hitachi Compute Blade 2500 Series UEFI Setup Guide</i> .
LP-Loader detected OEM FRU was unsupported version.(ver:XXXX)	The FRU version is not supported.	Contact your reseller or maintenance personnel.
LP-Loader detected VfcSeed.dat format error. (Error Info:0xXXXX)	N+M cold standby failover was attempted but the VfcSeed.dat file, which contains Vfc seed information, was invalid. XXXX indicates one of the following reasons: 0x0001: The file size is 0 bytes. 0x0002: The ChassisSeed serial number key was not found.	On the standby blade, the VfcSeed.dat file, which contains Vfc seed information, might be corrupted. N+M cold standby failover therefore becomes impossible. Contact your reseller or maintenance personnel.

Message	Description	Solution
	<p>0x0003: The size of the LPAR manager serial number data is 0 bytes (no data).</p> <p>0x0004: The LPAR manager serial number data contains a character string.</p>	
LP-Loader recovery communication to SVP.	Because a communication failure between LPAR manager and the management module was detected, recovery from the communication failure will be performed.	If this LPAR manager system log is collected whenever LPAR manager starts, contact your reseller or maintenance personnel.
LP-Loader switched NIC port0 to port1.	Recovery from a communication failure was performed between LPAR manager and the management module. However, because communication could not be recovered on Port0 (MGMT0), communication processing will be performed on Port1 (MGMT1).	If this LPAR manager system log is collected whenever LPAR manager starts, contact your reseller or maintenance personnel.
LP-Loader updated LP Serial Number in OEM FRU.	FRU was updated when N+M cold standby failover was detected. (You can confirm that N +M cold standby failover occurred from this message.)	None.
LP-Loader updated VfcSeed.dat in management module.	<p>This message is output after you move a server blade or install a server blade in a server chassis slot on which LPAR manager has previously run.</p> <p>The FRU information was synchronized with the Vfc seed information that was managed on the management module.</p>	None.
set variable error occurred [valname:XXXX] [ErrorCode:8000000000000009]	LPAR manager cannot start due to shortage of NVRAM resources.	Remove an unnecessary boot order from the UEFI setup menu.

Message	Description	Solution
		For details about how to remove a boot order, see the manual <i>Hitachi Compute Blade 2500 Series UEFI Setup Guide</i> .
Stop LP initializing.(LP License is disabled.) Please set LP license setting to enable.	The LPAR manager license is invalid.	Contact the reseller from which you purchased this equipment or consult maintenance personnel.
The value of MM Config Base is invalid. Change the value to 2GB.	The MM Config Base value was invalid. Change the value to 2 GB.	Use the EFI setup menu to set MM Config Base to 2 GB and then restart LPAR manager.
The value of MM Config Base is invalid. Change the value to 3GB	The MM Config Base value was invalid. Change the value to 3 GB.	Use the EFI setup menu to set MM Config Base to 3 GB and then restart LPAR manager.
This LP F/W is not supported for this blade(BladeSymphony XXXXXX). Please install another LP F/W supported for this blade. XXXX: Server blade model	This server blade does not support this LPAR manager firmware.	Install the LPAR manager firmware that is supported by this server blade.

If an error message other than the above message appears, contact your reseller or maintenance personnel.

LPAR manager screen operation messages

The following table shows LPAR manager screen messages displayed during LPAR manager screen operations.

Table 11-2 List of LPAR manager screen operation messages

Message	Description	LPAR manager operation	Solution
A NUMA configuration error has occurred. Set the scheduling mode of processor to a value of dedicated mode.	A setting for an LPAR for which NUMA is enabled is invalid. The scheduling mode for the processor is not dedicated mode.	Cancels the specified processing.	Change the scheduling mode for the processor to dedicated mode.
A user with the administrators role is required in the system.	At least one user with the administrators role assigned is required in the system.	Aborts the specified process.	To execute this processing, assign the administrators role to a different user.
Active LPAR Exist	The LPAR to be set cannot be set because it is activated.	Cancels the specified processing.	Deactivate the LPAR, and then retry the setting.
All groups are already added.	No group that can be added exists.	Cancels the specified processing.	Revise the specified processing.

Message	Description	LPAR manager operation	Solution
All LPARs are already defined.	No LPAR that can be defined exists.	Cancel the specified processing.	Revise the specified processing.
Auto activation for LPARx results in error.	Auto Activation for LPARx failed.	Cancel the specified processing.	Take appropriate actions according to subsequent messages.
Can not change LP System Time due to NTP enabled.	The LPAR manager system time cannot be changed because NTP is enabled.	Cancel the specified processing.	Disable NTP, and then change the LPAR manager system time.
Can not change timezone of LP System Time due to NTP enabled.	The LPAR manager system time zone cannot be changed because NTP is enabled.	Cancel the specified processing.	Disable NTP, and then change the LPAR manager system time zone.
Cannot remove the last user.	You cannot remove the last user.	Abort the specified process.	Review the specified process.
Change LP IP address	You need to change the LPAR manager IP address to an address other than 0.0.0.0.	Wait until the LPAR manager IP address is changed.	Change the LPAR manager IP address.
Change VNIC System No	You need to change the VNIC system number to a value other than 0.	Wait until the VNIC system number changes.	Change the VNIC system number.
Count Over Shared NIC Config.	Scheduling mode cannot be changed to shared mode because the maximum number of shared NICs has been exceeded.	Cancel the specified processing.	Revise the specified processing.
Device Assign error.	Activation of an LPAR failed. Alternatively, connection or disconnection of a device failed.	During the processing to activate an LPAR, LPAR manager cancels the processing. When an LPAR used by a device is being changed, LPAR manager cancels processing to connect or disconnect the device.	Make sure that dedicated mode is supported for the assigned devices. Alternatively, deactivate the target LPARs, reassign the devices that were assigned to those LPARs before this error occurred, and then reactivate the LPARs.
Device Schedule Mode is not Exclusive Shared.	The scheduling mode of the operation target device is not exclusively shared mode.	Terminate the specified operation.	Select a device whose scheduling mode is exclusively shared mode (Schd:E).
Error Character	Settings failed because an entered character is invalid.	Cancel the processing to set the characters.	Review the entry restrictions.

Message	Description	LPAR manager operation	Solution
Failed to save LP configuration	Failed to save the configuration.	Cancels the specified processing.	On the System Service State screen, check SVP Network Path State. If the value of Link is No, or if the value of Connect is Fail, check the internal LAN switch module settings.
Go to Shared FC Assign on Type=F & Schd=S.	Because the relevant device is a shared FC, change the settings on the Shared Assignment screen.	Cancels the specified processing.	Configure the settings on the Shared Assignment screen.
Go to VNIC Assign on Type=N & Schd=S.	Because the relevant device is a shared NIC, change the settings on the VNIC Assignment screen.	Cancels the specified processing.	Configure the settings on the VNIC Assignment screen.
Guest operating system may not remove USB device(s) safely. Force to detach.	During disconnection processing, the guest OS might not have removed the USB device completely.	Disconnects the USB device and cancels attaching the USB device to other LPARs.	Attach the USB device again.
LP cannot activate LPAR due to safe mode.	An LPAR could not be activated because safe mode is enabled.	Cancels the specified processing.	Exit safe mode, and then try again.
LP cannot save configuration due to safe mode.	Configuration information could not be saved because safe mode is enabled.	Cancels the specified processing.	Exit safe mode, and then try again.
LP could not import Time Setting of SVP.	Failed to import time settings from the management module.	Cancels the specified processing.	Check whether the version of the management module supports the NTP linkage functionality.
LP IPv4 address is needed for specified connection method of the virtual COM.	To use the connection method of the specified virtual COM console, set the LP IPv4 address.	Cancels the specified processing.	Set the LP IPv4 address and then try the operation again.
LP is busy with another LPAR(X) activation process.	During LPAR activation, activation of the LPAR failed because an error occurred in processing other than allocation of resources.	Cancels the specified processing.	Wait a while, and then execute the specified processing again.
LP is executing LPAR Migration, Please try again after it is finished.	Operation is not allowed because LPAR migration is in progress.	Cancels the specified processing.	Verify that the LPAR migration is complete, and then re-execute the specified processing.
LP is executing LPAR Migration. LP System Shutdown was canceled.	LPAR manager shutdown will be canceled because LPAR migration is in progress.	Cancels LPAR manager shutdown.	Verify that the LPAR migration is complete, and then re-execute the specified processing.

Message	Description	LPAR manager operation	Solution
LP is not executable condition for this request. Please wait.	LPAR manager cannot execute the specified processing.	Cancels the specified processing.	Wait a while, and then re-execute the processing.
LP is not ready for the operation	The configuration could not be saved.	Cancels the specified processing.	On the System Service State screen, execute Force Recovery.
LP is recovering specified LPAR from failed-migration state. This operation prevents some operations from performing.	Screen operations are prohibited because an LPAR that was placed in a failure status during LPAR migration is being recovered.	Performs the processing to recover the LPAR that was placed in a failure status during LPAR migration.	None.
Inhibit ICV request for the operation	The configuration could not be saved.	Cancels the specified processing.	Wait a while, and then re-execute the processing.
Insufficient Processor resource	An attempt to set the number of dedicated logical processors was made, but there are not enough physical processors available for the number of dedicated logical processors. An attempt to activate an LPAR was made, but physical processors that were to be assigned to the LPAR were not available.	Cancels LPAR activation.	Decrease the number of assigned processors or deactivate any LPARs that are currently activated, and then activate the target LPAR again. Alternatively, check the Logical Processor Configuration screen. If core scheduling is enabled, see What is a core scheduling? on page 5-11
Internal error (Cannot get lock).	The LPAR manager logical firmware detected an internal error.	Aborts the specified process.	Contact your reseller or maintenance personnel.
Invalid hour data.	An attempt to change the LPAR manager system time was made, but the specified value is invalid.	Cancels the specified processing.	Specify a correct value, and then try again.
Invalid in the scheduling mode.	This operation cannot be performed in the scheduling mode set for the target device.	Cancels the specified processing.	Revise the specified processing.
Invalid Input Data.	Setting of new data failed because the data is invalid.	Cancels the setting processing.	Specify different data.
Invalid minute data.	An attempt to change the LPAR manager system time was made, but the specified value is invalid.	Cancels the specified processing.	Specify a correct value, and then try again.

Message	Description	LPAR manager operation	Solution
Invalid month data.	An attempt to change the LPAR manager system time was made, but the specified value is invalid.	Cancels the specified processing.	Specify a correct value, and then try again.
Invalid second data.	An attempt to change the LPAR manager system time was made, but the specified value is invalid.	Cancels the specified processing.	Specify a correct value, and then try again.
Invalid separator.	An attempt to change the LPAR manager system time was made, but the specified value is invalid.	Cancels the specified processing.	Specify a correct value, and then try again.
Invalid year data.	An attempt to change the LPAR manager system time was made, but the specified value is invalid.	Cancels the specified processing.	Specify a correct value, and then try again.
IP address of NTP server is needed.	The IP address is required for the NTP server settings.	Cancels acquisition of the time from the NTP server.	Set the NTP server IP address for NTP Server 1 or NTP Server 2.
LPAR activation failed(Insufficient LPAR memory(System Used:xxMB))	The memory size (memory-size-that-is-allocated-to-an-LPAR - memory-size-that-is-used-by-the-system) that can be used by the LPAR is insufficient.	Cancels LPAR activation.	Increase the memory size to be assigned to the LPAR, and then try activating the LPAR again.
LPAR activation failed.	The LPAR cannot be activated.	Cancels LPAR activation.	Check that no LPAR manager system log that indicates a failure has been collected. If you cannot solve the problem, contact your reseller or maintenance personnel.
LPAR activation failed(Insufficient LPAR memory(System Used:xxMB))	The memory size (memory-size-that-is-allocated-to-an-LPAR - memory-size-that-is-used-by-the-system) that can be used by the LPAR is insufficient.	Cancels LPAR activation.	Increase the memory size to be assigned to the LPAR, and then try activating the LPAR again.
LPAR corrupted in a LPAR Migration exist, Please try again after recovering the LPAR.	Operations cannot be performed because there is an LPAR that was placed in a failure status during LPAR migration.	Cancels the specified processing.	Recover the LPAR that was placed in a failure status during LPAR migration, and re-execute the specified processing.
LPAR deactivation failed.	The LPAR cannot be deactivated.	Cancels LPAR deactivation.	Check that no LPAR manager system log that indicates a failure has been collected. If you cannot solve the problem, contact your

Message	Description	LPAR manager operation	Solution
			reseller or maintenance personnel.
LPAR start failed.	Failed to restart the target LPAR.	Cancels the specified processing.	Re-execute the specified processing.
Maximum number of users exceeded.	The maximum number of users has already been registered.	Aborts the specified process.	Delete unnecessary users, and then try adding a user again.
Memory allocation failed (Fragmentation).	An attempt to activate the LPAR was made, but the specified memory capacity could not be allocated.	Cancels LPAR activation.	The memory could not be allocated due to fragmentation. Decrease the allocated memory capacity, or deactivate any LPARs that are currently activated, and then try activating the target LPAR again.
Memory allocation failed (Insufficient).	An attempt to activate the LPAR was made, but the specified memory capacity could not be allocated.	Cancels LPAR activation.	Decrease the allocated memory capacity, or deactivate any LPARs that are currently activated, and then try activating the target LPAR again. If memory allocation by a specified node is enabled, decrease the allocated memory capacity so that it is within the unused memory capacity, or deactivate the LPARs that use the memory of the node, and then try activating the target LPAR again.
Memory size is zero.	The LPAR cannot be activated because the memory size is zero.	Cancels LPAR activation.	Set the memory size and activate the LPAR.
No groups can be removed.	There is no group that can be deleted.	Cancels the specified processing.	Revise the specified processing.
Not Changed!! Select Device is Management Path.	An attempt to change the scheduling mode of the selected NIC was made, but it was set as an NIC for the management path.	Cancels the specified processing.	Revise the specified processing.
NTP server is not set.	NTP server settings are not configured.	Cancels acquisition of the time from the NTP server.	Set the NTP server IP address for NTP Server 1 or NTP Server 2.
NUMA configuration error. Set processor scheduling mode to dedicated and bind	A setting for an LPAR for which NUMA is enabled is invalid. Change the scheduling mode for the	Cancels the specified processing.	Change the scheduling mode for the processors to dedicated mode. Assign

Message	Description	LPAR manager operation	Solution
logical processor to physical processor manually.	processor to dedicated mode. Assign physical processors to logical processors.		physical processors to logical processors.
Operation failed because system configuration is being updating.	The operation was not accepted because the LPAR manager configuration information is now being saved.	Aborts the specified process.	Wait a while, and then retry the specified process.
Over Max VLAN ID count (16).	The number of specified VLAN IDs exceeds 16.	Displays the sub-screen until you re-specify a maximum of 15 VLAN IDs or press the Esc key.	Re-specify a maximum of 15 VLAN IDs, or press the Esc key to cancel VLAN ID settings.
Over the maximum number of activated LPARs (X).	The LPAR cannot be activated because the maximum number (X) of LPARs that can be activated for Essential/Advanced/Enterprise model was exceeded.	Cancels LPAR activation.	Deactivate any LPARs that are currently activated, and then try activating the target LPAR again.
Password mismatch.	The password you entered did not match.	Aborts the specified process.	Try setting the password again.
Port number for virtual console is out of range for specified connection mode.	The specified port number is outside the range of values that can be used for the current connection mode for the virtual COM console.	Aborts the specified process.	Check the connection mode and port number for the virtual COM console, and then retry the process.
Press any key first. Then press F10 key next.	You need to press the F10 key to apply changed settings.	Waits until you press the F10 key.	Enter any key, wait until the output message disappears, and then press the F10 key.
Resource lock failure.	Acquisition of a lock during an update of the configuration failed. Acquisition of a lock during an operation for the system or the LPAR failed. Acquisition of a lock during an LPAR update for the NIC failed.	Cancels the specified processing.	Re-execute the specified processing.
Sampling time Error	Setting of the sampling time on the LPAR Usage screen failed.	Cancels setting of the sampling time.	Specify a value in the range from 1 to 60.
Save Configuration request(F9 Key) is already accepted. Please wait.	A request to save the configuration has been already accepted. Wait a while.	Cancels the specified processing.	Wait until the configuration starts to be saved.

Message	Description	LPAR manager operation	Solution
Select Device is Single Port NIC. Can not change Management Path.	The NIC that was selected in NIC management path settings has 1 port.	Cancels the specified processing.	Revise the specified processing.
Service Ratio must be 1-999	The specified service ratio cannot be set because it is not in the range from 1 to 999.	Cancels setting of the service ratio.	Specify a value in the range from 1 to 999 for the service ratio.
Specified user is not registered.	The specified user is not registered.	Aborts the specified process.	Check the user name, and then retry the process.
Specified user is reserved.	The specified user name is reserved by LPAR manager.	Aborts the specified process.	Use another user name to retry user registration.
Target Device is in invalid type.	This operation cannot be performed on the target device.	Cancels the specified processing.	Revise the specified processing.
Target LPAR is active.	The LPAR to be set cannot be set because it is activated.	Cancels the specified processing.	Deactivate the LPAR, and then retry the setting.
Target LPAR is coming to foreground.	Switchover to the LPAR guest screen is running.	Switchover to the LPAR guest screen is running.	Wait a while.
Target LPAR is deactive.	An attempt to deactivate the specified LPAR was made, but it was already deactivated.	Cancels the specified processing.	Activate the LPAR, and then try again.
Target LPAR is Executing Migration.	Operation for the specified LPAR is not allowed because LPAR migration is in progress.	Cancels the specified processing.	Cancels the specified processing.
Target LPAR is Executing Rollback.	Operation for the specified LPAR is not allowed because a rollback due to LPAR migration is in progress.	Cancels the specified processing.	Confirm that the LPAR rollback has ended, and then try again.
Target LPAR is undefined.	An attempt to operate the specified LPAR was made, but the LPAR was not defined. An attempt to change the virtual NIC configuration was made, but the LPAR to be changed was not defined.	Cancels the specified processing.	Re-execute the specified processing.
Target LPAR must be shared mode.	The LPAR cannot be set because it is in dedicated mode.	Cancels the specified processing.	Change the scheduling mode of the LPAR to shared mode, and then try setting the LPAR again.

Message	Description	LPAR manager operation	Solution
The input value exceeds the assignable memory size.	The value exceeds the memory size that can be allocated to the LPAR.	Cancels the specified processing.	Review the memory size.
The LP license expired. LP cannot activate LPAR.	You are not able to activate the LPARs because the LPAR manager license has expired.	Cancels LPAR activation.	<p>Purchase an LPAR manager license, or use the LPAR manager as an Essential model by performing the following steps:</p> <ol style="list-style-type: none"> 1. Stop the LPAR manager. 2. Backup the LPAR manager configuration. 3. Update the LPAR manager license by using the management module firmware A0135. 4. Start the LPAR manager. <p>For details about updating an LPAR manager license, see Upgrading LPAR manager licenses.</p>
The LPAR Migration is in progress. This LPAR Migration prevents some operations such as activation, deactivation and LPAR-reconfiguration from performing.	Operations on screens are prohibited because LPAR migration is in progress.	LPAR migration is in progress.	Wait until the LPAR migration ends.
The name is used for other group.	An attempt to set the specified group name was made, but a group with the same name already existed.	Cancels the group name change.	Specify a different group name.
The name is used for other LPAR.	An attempt to set the specified LPAR name was made, but an LPAR with the same name already existed.	Cancels the LPAR name change.	Specify a different group name.
The specified LPAR has corrupted in a LPAR Migration, please try to recover the LPAR.	Operation for the LPAR is not allowed because the LPAR was placed in a failure status during LPAR migration.	Operation for the LPAR is not allowed because the LPAR was placed in a failure status during LPAR migration.	Recover the LPAR that was placed in a failure status during LPAR migration.
The VF is already assigned the maximum assignable times to LPARs.	This message indicates that connection or disconnection of a device failed.	Cancels the operation to activate the LPAR. Cancels the operation to connect or	Reassign the devices that were assigned to target LPARs before this error, and then reactivate the LPARs.

Message	Description	LPAR manager operation	Solution
		disconnect a device.	
There is no permission to execute the operation.	The management module user does not have the access permissions required to execute this processing.	Cancels the specified process.	Assign a role with access permissions for this processing, to the management module user.
This request has been cancelled. The logical processor topology setting mode for the guest NUMA is set to the Physical NUMA Node Binding Mode.	You cannot assign physical processors to logical processors, for LPARs that bind physical NUMA nodes.	Cancels the specified processing.	To specify physical processor numbers, change the method to set logical processors for NUMA to bind physical processors.
This request through the LP screen is not supported. The logical processor topology setting mode for the guest NUMA is set to the Physical NUMA Node Binding Mode.	You cannot assign physical processors to logical processors, for LPARs that bind physical NUMA nodes.	Cancels the specified processing.	For LPARs for which physical NUMA node binding is set, set the number of logical processors for each node from HvmSh command.
Updating LP firmware, Please try again after it is finished.	LPAR manager shutdown and the F10 key are not allowed because the LPAR manager firmware is being updated.	Cancels the specified processing.	Confirm that the LPAR manager firmware has been completely updated, and then re-execute the specified processing.
Updating LP firmware, Please wait until it is finished.	LPAR manager is waiting to be shut down because the LPAR manager firmware is being updated.	Temporarily waits to perform the specified processing.	Wait until the LPAR manager firmware has been completely updated.
Virtual console authentication mode cannot be changed when virtual console connection mode is SSH.	You cannot change the authentication mode if the virtual COM console connection mode is SSH.	Aborts the specified process.	Review the specified process.
VLAN ID is not set.	The VLAN ID to be displayed is not set.	Terminates the specified operation.	Check the network segment identifier to be displayed.

If an error message other than the above message appears, contact your reseller or maintenance personnel.

Related topics

- [Upgrading LPAR manager licenses on page 9-3](#)
- [Logical Processor Configuration screen on page 10-20](#)
- [Virtual NIC Assignment screen on page 10-34](#)
- [Shared FC Assignment screen on page 10-42](#)

- [System Service State screen on page 10-58](#)

LPAR manager system log messages

The following LPAR manager system log messages are displayed on the LP System Logs screen:

- **Error**
Indicates a failure message. A failure occurred in LPAR manager.
- **Warn**
Indicates a warning message. No failure occurred, but an event that requires special attention occurred.
- **Info**
Indicates an information message. An event with a level other than the above levels occurred.

Error log messages for the LPAR manager system

The following table shows error log messages for the LPAR manager system.

Table 11-3 List of error log messages for the LPAR manager system

Message	Description	Solution
An abnormal time difference was detected.	Periodic time synchronization via NTP was canceled because an abnormal time difference was detected.	Take action as follows: <ul style="list-style-type: none"> • Check the status of the NTP server. • If there is no problem with the NTP server, disable time synchronization in the Date and Time screen, and set the original values to restart time synchronization. • Check the LPAR manager system time and OS system time. Then, if necessary, use an OS command or Adjust LPAR Time to set the logical RTC time of the LPAR.
An error-level event occurred on the LP.	An error-level event occurred on the LPAR manager.	See the adjacent LPAR manager system log, which is described in the details of this event.
Dmar Fault occurred.	A DMAR fault occurred.	Contact your reseller or maintenance personnel.
Guest, Watchdog timer has expired.	A timeout of the guest watchdog timer was detected.	See other collected LPAR manager system logs that indicate a failure, and take appropriate actions. If you cannot solve the problem, contact your reseller or maintenance personnel.
H/W Corrected MCK logging was suppressed.	Error logging was suppressed because the number of times that corrected machine check	Contact your reseller or maintenance personnel.

Message	Description	Solution
	events were logged exceeded the threshold.	
H/W Corrected MCK occurred.	A corrected machine check event occurred.	None.
H/W Fatal MCK occurred.	A fatal machine check event occurred.	Contact your reseller or maintenance personnel.
Hardware Component BMC access error occurred.	A failure occurred in accessing the physical BMC.	Contact your reseller or maintenance personnel.
LP Assist damage occurred.	An LPAR manager failure (an LPAR manager Assist failure) occurred.	Contact your reseller or maintenance personnel.
LP Assist damage occurred. (due to H/W error)	An LPAR manager failure (an LPAR manager Assist failure) due to a hardware failure occurred.	Contact your reseller or maintenance personnel.
LP could not delete the specified PCI slot configuration data.	Deletion of device definitions failed during processing to reduce PCI devices.	Contact your reseller or maintenance personnel.
LP could not detect PCI device.	LPAR manager detected reduction of the number of PCI devices.	Back up the LPAR manager configuration and exit safe mode. Check whether PCI devices are isolated. If you cannot resolve the problem, contact your reseller or maintenance personnel.
LP could not power off the PCI slot.	An attempt to turn off the physical I/O adapter slot failed.	Contact your reseller or maintenance personnel.
LP could not power on the PCI slot.	An attempt to turn on the physical I/O adapter slot failed.	Contact your reseller or maintenance personnel.
LP could not terminate the shared NIC.	An attempt to terminate the shared NIC failed during physical hot removal of the shared NIC.	Contact your reseller or maintenance personnel.
LP damage occurred.	An LPAR manager failure occurred.	Contact your reseller or maintenance personnel.
LP damage occurred. (due to H/W error)	An LPAR manager failure due to a hardware failure occurred.	Contact your reseller or maintenance personnel.
LP detected a failure of retrying the setting of TxRate configuration.	Retry of the operation to configure TxRate failed.	A network failure might have occurred. Check the status of the network to which this device is connected. If you cannot find any network problem, a device failure might have occurred. Contact your reseller or maintenance personnel.
LP detected a network communication error on the active port.	A communication failure in the active path occurred on the LPAR manager management NIC.	Check the network connection and settings between LPAR manager and the management module.

Message	Description	Solution
		If you cannot solve the problem, contact your reseller or maintenance personnel.
LP detected Activation error for Shared NIC at expansion card.	An error in activating the shared NIC was detected.	Contact your reseller or maintenance personnel.
LP detected Activation error for Shared NIC at on-board.	An error in activating the shared NIC was detected.	Contact your reseller or maintenance personnel.
LP detected Activation error for Shared NIC.	An error in activating the shared NIC was detected.	Contact your reseller or maintenance personnel.
LP detected different version of firmware on the NIC device.	A fault in the combination of the firmware versions of NIC devices was detected.	Check that all NIC firmware versions on the server blade are the same. If you cannot solve the problem, contact your reseller or maintenance personnel.
LP detected error of network communication at management path.	A fault in the management path was detected. An internal LAN segment duplicates the management LAN segment.	Review the setting of the LPAR manager IP address.
LP detected error of network communication for SVP access.	A communication failure occurred between LPAR manager and the management module.	Contact your reseller or maintenance personnel.
LP detected Hardware error for Shared FC at expansion card.	A shared FC fatal failure was detected.	Contact your reseller or maintenance personnel.
LP detected uninitialized Shared device.	A shared I/O device that has not been initialized was detected.	Contact your reseller or maintenance personnel.
LP detected Hardware error for Shared FC.	A shared FC fatal failure was detected.	Contact your reseller or maintenance personnel.
LP detected Initialization error for Shared NIC at expansion card.	An error in initializing the shared NIC was detected.	Contact your reseller or maintenance personnel.
LP detected Initialization error for Shared NIC at on-board.	An error in initializing the shared NIC was detected.	Contact your reseller or maintenance personnel.
LP detected Initialization error for Shared NIC.	An error in initializing the shared NIC was detected.	Contact your reseller or maintenance personnel.
LP detected Link Down error for Shared FC at expansion card.	A link down on the shared FC was detected.	Check connections to the shared FC. If you cannot solve the problem, contact your reseller or maintenance personnel.
LP detected Link Down error for Shared FC.	A link down on the shared FC was detected.	Check connections to the shared FC. If you cannot solve the problem, contact your reseller or maintenance personnel.
LP detected Link Down error for Shared NIC at expansion card.	A link down on the shared NIC was detected.	Check connections to the shared NIC. If you cannot solve the problem, contact your reseller or maintenance personnel.

Message	Description	Solution
LP detected Link Down error for Shared NIC at on-board.	A link down on the shared NIC was detected.	Check connections to the shared NIC. If you cannot solve the problem, contact your reseller or maintenance personnel.
LP detected Link Down error for Shared NIC.	A link down on the shared NIC was detected.	Check connections to the shared NIC. If you cannot solve the problem, contact your reseller or maintenance personnel.
LP detected MCKINT for Shared FC at expansion card.	A shared FC temporary failure was detected.	Contact your reseller or maintenance personnel.
LP detected MCKINT for Shared FC.	A shared FC temporary failure was detected.	Contact your reseller or maintenance personnel.
LP detected PCI bus error for Shared FC at expansion card.	A shared-FC PCI bus failure was detected.	Contact your reseller or maintenance personnel.
LP detected reduction of CPUs.	LPAR manager detected reduction of the number of physical processors.	Back up the LPAR manager configuration and exit safe mode. Check whether physical processors are isolated. If you cannot resolve the problem, contact your reseller or maintenance personnel.
LP detected reduction of memory.	LPAR manager detected reduction of the memory size.	Back up the LPAR manager configuration and exit safe mode. Check whether memory is isolated. If you cannot resolve the problem, contact your reseller or maintenance personnel.
LP detected Link Down error for Shared FC.	A link down on the shared FC was detected.	Check connections to the shared FC. If you cannot solve the problem, contact your reseller or maintenance personnel.
LP detected MCKINT for Shared FC.	A shared FC temporary failure was detected.	Contact your reseller or maintenance personnel.
LP detected Hardware error for Shared FC.	A shared FC fatal failure was detected.	Contact your reseller or maintenance personnel.
Network configuration error for Shared FC.	A shared FC interface failure was detected.	Check the connections to the shared FC. If you cannot solve the problem, contact your reseller or maintenance personnel.
LP detected unsupported version of firmware on a NIC device.	An unsupported firmware version was detected on the NIC device.	Verify that the firmware version of the NIC is supported by LPAR manager. If you cannot solve the problem, contact your reseller or maintenance personnel.
LP failed to get Personality and Multichannel Mode on a NIC device.	LPAR manager failed to obtain the Personality setting and Multichannel mode from the NIC device.	Restart LPAR manager. If this LPAR manager system log is collected even after you restart LPAR manager, contact your reseller or maintenance personnel.
LP failed to get the firmware version on a NIC device.	An attempt to obtain the firmware version from the NIC device failed.	Restart LPAR manager. If this LPAR manager system log is collected even

Message	Description	Solution
		after you restart LPAR manager, contact your reseller or maintenance personnel.
LP failed to have SR-IOV device enabled.	LPAR manager detected that SR-IOV is enabled for some ports in the controller and disabled for other ports in the controller.	Check the SR-IOV settings of the PCI devices. Alternatively, make sure that the Personality setting is set to NIC mode. For details about how to check this setting, see the manual <i>Hitachi Compute Blade Emulex Adapter User's Guide for Hardware</i> . Note, however, that you cannot change the setting in LP mode. To change the setting, change the mode to Basic mode.
LP Loader could not update LP Serial Number in OEM FRU.	N+M cold standby failover was detected. An attempt to update the FRU at LPAR manager boot was made, but failed.	An error might have occurred on the BMC. In addition, the FRU might be damaged. Contact your reseller or maintenance personnel.
LP Loader detected format error in the initial parameter.	An error in the initial parameter file was detected. The file is invalid because it does not contain the required data, or the file size is 0 bytes.	Contact your reseller or maintenance personnel.
LP-LFW detected internal error.	The LPAR manager logical firmware detected an internal error.	Contact your reseller or maintenance personnel.
LPAR damage occurred.	An LPAR manager failure (an LPAR failure) occurred.	Contact your reseller or maintenance personnel.
LPAR damage occurred. (due to H/W error)	An LPAR manager failure (an LPAR failure) due to a hardware failure occurred.	Contact your reseller or maintenance personnel.
Network configuration error for Shared FC at expansion card.	A shared FC interface failure was detected.	Check connections to the shared FC. If you cannot solve the problem, contact your reseller or maintenance personnel.
Network configuration error for Shared FC.	A shared FC interface failure was detected.	Check connections to the shared FC. If you cannot solve the problem, contact your reseller or maintenance personnel.
Network Segment damage occurred.	A failure occurred on the network segment for the shared NIC or the virtual NIC.	Contact your reseller or maintenance personnel.
PCI device error was detected.	A PCI device error was detected.	Contact your reseller or maintenance personnel.
Physical Processor Isolation.	The physical processor was degenerated.	Contact your reseller or maintenance personnel.
Shadow Command is rejected.	A request to LPAR manager Assist was discarded.	Contact your reseller or maintenance personnel.
SR-IOV device of LPAR was damaged and isolated.	A failure occurred on a PCI device. As a result, the PCI	Immediately shut down the guest OS to which the blocked PCI device was assigned.

Message	Description	Solution
	device was forcibly isolated from the LPAR.	If the PCI device does not recover automatically, perform the operation Force Recovery to recover from the blocked state. After the PCI device recovers, if you boot the guest OS, you will be able to use the PCI device again.
SVGA Initialization failed.	Initialization of the physical SVGA failed.	Contact your reseller or maintenance personnel.
SYS2 dump data collection failed.	SYS2 dump data collection failed.	Contact your reseller or maintenance personnel.
SYS2 dump service failed to start.	SYS2 dump service failed to start.	Contact your reseller or maintenance personnel.
SYS2 dump service failed to stop.	SYS2 dump service failed to stop.	Contact your reseller or maintenance personnel.
System Service request command failed.	A system service request command failed.	Contact your reseller or maintenance personnel.
The LPAR migration functionality is unavailable owing to an error.	The LPAR migration functionality has stopped functioning because the LPAR manager cannot access the LPAR manager configuration file.	Check the network connection between the LPAR manager and the management module, and its setting. Then, perform the Force Recovery operation to recover the LPAR manager from isolation. If you cannot solve the problem, contact your seller or maintenance personnel.
The virtual COM consoles are unavailable owing to port duplication.	The virtual COM consoles stopped functioning because some of the ports used by LPs and the ports used by the virtual COM consoles overlapped.	Check for ports that are not used by LPAR managers, and then change the port settings for virtual COM consoles.
There are not enough H/W resources for SR-IOV feature.	LPAR manager detected a shortage of hardware resources for the SR-IOV functionality.	Make sure that the SR-IOV functionality is supported by all firmware versions that are being used. For details about combinations of firmware versions, see the manual <i>Hitachi Compute Blade Emulex Adapter User's Guide for Hardware</i> .
This LP detected an adapter unsupported on an I/O Slot Expansion Unit.	Installation of fibre channel adapters on PCI Express x4 slots of an I/O slot expansion unit is not supported. The LP does not display these fibre channel adapters.	Contact your reseller or maintenance personnel.
This LP detected an unsupported adapter in a 4-blade SMP server configuration.	Installation of devices on I/O board module slots is not supported in a 4-blade SMP configuration in which an I/O slot expansion unit is connected. The LP does not display these devices.	Contact your reseller or maintenance personnel.

Message	Description	Solution
VNIC damage occurred.	A failure occurred on the virtual NIC.	Contact your reseller or maintenance personnel.
VNIC damage on LP Assist occurred.	A failure occurred on the virtual NIC (LPAR manager Assist).	Contact your reseller or maintenance personnel.

Related topics

- [Chapter 9, LPAR manager Screen](#)
- [Date and Time screen on page 10-63](#)

Warning log messages for the LPAR manager system

The following table shows warning log messages for the LPAR manager system.

Table 11-4 List of warning log messages for the LPAR manager system

Message	Description	Solution
A caution-level event occurred on the LP.	A caution-level event occurred on the LPAR manager.	See the adjacent LPAR manager system log, which is described in the details of this event.
An abnormal time difference was detected.	An abnormal time difference was detected when the LP time had been synchronized automatically with NTP server.	Take action as follows: <ul style="list-style-type: none"> • Check the status of the NTP server. • If there is no problem with the NTP server, disable time synchronization in the Date and Time screen, and set the original values to restart time synchronization. • Check the LPAR manager system time and OS system time. Then, if necessary, use an OS command or Adjust LPAR Time to set the logical RTC time of the LPAR.
Guest dump failed.	Execution of guest memory dump failed.	By executing an HVM management command (HvmSh command) to get the progress of the guest memory dump, you can obtain the information about a guest memory dump execution error and the reason for the error. Take appropriate actions according to the contents of "Status Codes and Messages" that is displayed by the relevant command.
H/W Corrected MCK occurred.	A corrected machine check event occurred.	None. You do not need to take action for this message because the number of machine check events is managed by the threshold. If the number of machine check events exceeds the threshold, another message is displayed. Take appropriate actions according to that message.

Message	Description	Solution
LP changed Management Path and the LPAR configuration was changed.	Because a NIC whose scheduling mode was set to dedicated mode was specified as a management NIC, the scheduling mode of the NIC was changed from dedicated mode to shared mode. The dedicated assignment of the NIC to an LPAR was removed from the NIC.	Because safe mode is enabled, review NIC assignment to LPARs and then exit safe mode.
LP changed a NIC to dedicated mode and the LPAR configuration was changed.	The scheduling mode of a NIC was changed to dedicated mode because the scheduling mode of a NIC that was specified as a management NIC was changed to shared mode, and the maximum number of shared NICs was exceeded. The shared assignment of the NIC to an LPAR was removed.	Because safe mode is enabled, review NIC assignment to LPARs and then exit safe mode.
LP could not import Time Setting of BMC.	Failed to import time settings from the BMC.	Check whether the version of the BMC supports the NTP linkage functionality. Review the time settings of the BMC, and import the time settings from the BMC again.
LP could not import Time Setting of SVP.	Failed to import time settings from the management module.	Check whether the version of the management module supports the NTP linkage functionality. Review the time settings of the management module, and import the time settings from the management module again.
LP could not retrieve Time Setting from SVP.	Failed to import time settings from the management module.	Check whether the version of the management module supports the NTP linkage functionality. Review the time settings of the management module.
LP detected a lack of I/O interrupt vectors.	A lack of I/O interrupt vectors was detected.	Check the PCI device configuration. If PCI devices that are not supported by the product are included in the configuration, remove them.
LP detected a network communication error on the standby port.	A communication failure in the standby path occurred on the LPAR manager management NIC.	Check the network connection and settings between LPAR manager and the management module. If you cannot solve the problem, contact your reseller or maintenance personnel.
LP detected an invalid date and time.	Date and Time was reset because an invalid system equipment time was detected when LPAR manager started.	Take action as follows: <ul style="list-style-type: none"> Check the LPAR manager system time. Then, if necessary, set it again. Check the OS system time. Then, if necessary, use an OS command or Adjust LPAR Time to set the logical RTC time of the LPAR. Save the LPAR manager configuration information.

Message	Description	Solution
LP detected AP initialization timeout.	A timeout occurred during initialization of the guest OS.	Review the service ratio allocated to the LPAR.
LP detected Driver Ver Error for Shared FC at expansion card.	An FC driver that does not support shared FC was detected.	Upgrade the driver to a version that supports shared FC.
LP detected Driver Ver Error for Shared FC.	An FC driver that does not support shared FC was detected.	Upgrade the driver to a version that supports shared FC.
LP detected failed SR-IOV device was assigned to LPAR.	LPAR manager detected the activation of the LPAR to which the blocked PCI device was assigned.	You cannot use the PCI device on the LPAR because the PCI device is in an error state. If the PCI device does not recover automatically, perform the operation Force Recovery to recover from the blocked state. After the PCI device recovers, if you boot the guest OS, you will be able to use the PCI device again.
LP detected initial parameter error.	Incorrect data was detected in the initial parameter file.	Revise the settings on the System Configuration screen.
LP detected invalid I/O slot expansion unit number.	The LP detected an invalid I/O slot expansion unit number.	Contact your reseller or maintenance personnel.
LP detected PCI bus error for Shared FC.	A shared-FC PCI bus failure was detected.	Contact your reseller or maintenance personnel.
LP detected PCI dev assign error.	LPAR manager detected incorrect PCI device assignment information.	Reassign PCI devices on the PCI Device Assignment screen. If this LPAR manager system log is collected again, contact your reseller or maintenance personnel.
LP detected the duplication of I/O slot expansion unit number.	The LP detected duplication of an I/O slot expansion unit number.	Contact your reseller or maintenance personnel.
LP detected too many physical CPUs, some CPUs are ignored.	Because the number of physical processors exceeded the maximum number of processors that LPAR manager can recognize, LPAR manager was started by ignoring the excess processors.	Contact your reseller or maintenance personnel.
LP detected unsupported H/W configuration.	A hardware configuration that is not supported was detected.	A PCI device might be installed in the I/O adapter slot of the PCI expansion blade. The PCI device cannot be used, because the I/O adapter slot of the PCI expansion blade is not supported.
LP detected unsupported settings in the configuration.	An invalid value is specified in the LPAR manager configuration information.	Check the detailed message in the LP system log, and then check values specified in the configuration information.
LP dump generation failed.	Collection of the LPAR manager dump failed.	Contact your reseller or maintenance personnel.

Message	Description	Solution
LP dump is lost.	The LPAR manager dump was lost.	Contact your reseller or maintenance personnel.
LP dump management file access error occurred.	An error in accessing the LPAR manager dump management information file occurred.	Contact your reseller or maintenance personnel.
LP dump transfer failed.	Transmission of the LPAR manager dump to the management module failed.	Contact your reseller or maintenance personnel.
LP failed deletion of the initial parameter file.	Deletion of the initial parameter file failed.	If this LPAR manager log is frequently collected, contact your reseller or maintenance personnel.
LP failed in network time synchronization by NTP	Synchronization of the LPAR manager system time via NTP failed.	Check the following: <ul style="list-style-type: none"> • The specified IP address is correct. • The NTP server is running. • The LAN path to the NTP server is connected.
LP Loader deleted the initial parameter.	The initial parameter file InitParam.dat required for starting LPAR manager was detected and deleted.	The initial parameter file was deleted because of the reasons below. The reasons can be divided as follows, based on the detailed messages of LPAR manager system logs: <ul style="list-style-type: none"> • Restoration was performed on the Web console or the CLI console. • Initialization was performed on the Web console or the CLI console. • N+M cold standby failover was executed. • The blade serial numbers of the source and destination server blades do not match.
LP Loader detected load error and recovered.	Loading the configuration failed, but the error was corrected.	If this LPAR manager system log is collected whenever LPAR manager starts, contact your reseller or maintenance personnel.
LP started retrying the setting of TxRate configuration.	Failed to configure TxRate. Try to configure TxRate again.	Wait a while for the retry to finish.
LP System Shutdown Failed.	LPAR manager shutdown failed.	Contact your reseller or maintenance personnel.
LP-LFW detected failure of getting bootdevice.	The LPAR manager logical firmware detected a BootDevice acquisition error.	Contact your reseller or maintenance personnel.
LP-LFW detected failure of setting bootorder.	The LPAR manager logical firmware detected a BootOrder settings error.	Review the contents of the BootOrder settings file. If you cannot solve the problem, contact your reseller or maintenance personnel.
LP-LFW detected internal error.	The LPAR manager logical firmware detected an internal error, but the error was corrected.	If this LPAR manager system log is frequently collected, contact your reseller or maintenance personnel.

Message	Description	Solution
LP-LFW detected tftp error.	The LPAR manager logical firmware detected a network failure when a network boot was being executed.	Review the network load, and then execute a network boot again. If this LPAR manager system log is collected again, contact your reseller or maintenance personnel.
Lock timeout was recovered.	A lock timeout occurred.	A lock timeout occurred, but the error was corrected.
Logical CPU slowdown due to too many logical CPUs.	A performance degradation due to the excess of LPARs or logical CPUs was detected.	Review the numbers of LPARs and logical CPUs. This event might be output during shutdown of an OS or deactivation of an LPAR. However, this is not a serious problem if "Logical CPU performance returns to normal." is output within a few minutes.
LPAR Migration failed.	LPAR migration failed.	For details about the action to be taken, see the manual <i>Hitachi Command Suite Compute Systems Manager User Guide</i> , the manual <i>Hitachi Compute Blade HVM Navigator User's Guide - Migration</i> , or the manual <i>Hitachi Compute Blade LPAR Migration Guide</i> .
NTP server settings contain invalid characters.	The NTP server settings contain invalid characters.	Set the NTP server IP address for NTP Server 1 or NTP Server 2.
RTC time synchronization has failed.	RTC synchronization via NTP failed.	Check the NTP settings.
RTC time wasn't successfully synchronized last time.	RTC synchronization failed because of a temporary reason.	When RTC synchronization failed more than a day after this log message was collected, save the configuration and then perform RTC synchronization. If no RTC synchronization system log is collected even when you saved the configuration, contact your reseller or maintenance personnel.
SVP access initialization failed.	Initialization of access to the management module failed.	Contact your reseller or maintenance personnel.
The Essential model is applied to this LP.	The LPAR manager started as an Essential model, because the temporary LPAR manager license has expired.	Continue to use the LPAR manager as an Essential model or purchase an LPAR manager license.
The temporary LP license expiration date is getting closer.	The temporary LPAR manager license will expire soon. After the temporary license expires, the following operations will be suppressed: <ul style="list-style-type: none"> • Operation to activate LPARs • OS startup after reactivating LPARs • OS startup after restarting OSs 	Purchase an LPAR manager license, or use the LPAR manager as an Essential model by performing the following steps: <ol style="list-style-type: none"> 1. Stop the LPAR manager. 2. Backup the LPAR manager configuration. 3. Update the LPAR manager license by using the management module firmware A0135. 4. Start the LPAR manager.

Message	Description	Solution
	<ul style="list-style-type: none"> Operations that include the operation to activate LPARs (such as boot order configuration and boot device acquisition) 	For details about updating an LPAR manager license, see Upgrading LPAR manager licenses.
The temporary LP license has expired.	<p>The temporary LPAR manager license has expired.</p> <p>The following operations are suppressed.</p> <ul style="list-style-type: none"> Operation to activate LPARs OS startup after reactivating LPARs OS startup after restarting OSs Operations that include the operation to activate LPARs (such as boot order configuration and boot device acquisition) 	<p>Purchase an LPAR manager license, or use the LPAR manager as an Essential model by performing the following steps:</p> <ol style="list-style-type: none"> 1. Stop the LPAR manager. 2. Backup the LPAR manager configuration. 3. Update the LPAR manager license by using the management module firmware A0135. 4. Start the LPAR manager. <p>For details about updating an LPAR manager license, see Upgrading LPAR manager licenses.</p>
Thermal error occurred.	A temperature rise warning event occurred.	Remove dust from the air vent of the system unit to improve ventilation. If this LPAR manager event log is collected even after ventilation is improved, contact your reseller or maintenance personnel.
TSC difference was left between processors.	LPAR manager could not eliminate the TSC (Time Stamp Counter) difference between processors.	Contact your reseller or maintenance personnel.
Unknown event occurred.	An unknown event was collected.	Contact your reseller or maintenance personnel.

Related topics

- [Upgrading LPAR manager licenses on page 9-3](#)
- [PCI Device Assignment screen on page 10-30](#)
- [System Configuration screen on page 10-47](#)

Information log messages for the LPAR manager system

The following table shows information log messages for the LPAR manager system.

Table 11-5 List of information log messages for the LPAR manager system

Message	Description	Solution
An information-level event occurred on the LP	An information-level event occurred on the LPAR manager.	No particular action required. For more detail, see the adjacent LPAR

Message	Description	Solution
		manager system log, which is described in the details of this event.
Configuration will not be saved during safe mode.	Configuration information cannot be saved while LPAR manager is running in safe mode.	Exit safe mode and, if necessary, save configuration information.
Found the machine type mismatch LP initialized the configuration files.	The configuration and the server blade configuration do not match.	Check the configuration and the server blade configuration.
Guest dump completed.	An execution of guest memory dump ended.	None.
Guest dump started.	A guest memory dump started because of an operation for starting the guest memory dump.	None.
Guest dump was cancelled.	A guest memory dump was canceled because of an operation for canceling the guest memory dump.	None.
Guest, Double Fault(#DF) occurred.	A guest double fault occurred.	Check the operating status of the guest OS.
Guest, INIT occurred.	A guest INIT interrupt occurred.	Check the operating status of the guest OS.
Guest, NMI occurred.	A guest NMI interrupt occurred.	Check the operating status of the guest OS.
Guest, Triple Fault occurred.	A guest triple fault occurred.	Check the operating status of the guest OS.
H/W Corrected MCK cumulative count was logged.	The total number of corrected machine check events was logged.	None.
Hardware Component BMC access error was recovered.	A failure in accessing the physical BMC was corrected.	None.
LP activates LPAR in auto activation process.	The LPAR was activated in Auto Activate processing.	None.
LP auto activation process is cancelled.	Auto Activate processing was canceled.	None.
LP auto activation process is ended.	Auto Activate processing ended.	None.
LP auto activation process is started.	Auto Activate processing started.	None.
LP booted with copied configuration files.	LPAR manager started with a configuration that was generated by cloning.	None.
LP booted with initial parameter file.	LPAR manager started by using the settings in the initial parameter file.	None.
LP changed Management Path.	A management NIC was changed.	None.
LP changed NIC to dedicated mode.	The scheduling mode of a NIC was changed to dedicated mode because the	None.

Message	Description	Solution
	scheduling mode of a NIC that was specified as a management NIC was changed to shared mode, and the maximum number of shared NICs was exceeded.	
LP completed deletion of the initial parameter file.	The initial parameter file was completely deleted.	None.
LP detected a network communication recovery on the active port.	A communication failure in the active path was corrected on the LPAR manager management NIC.	None.
LP detected a network communication recovery on the standby port.	A communication failure in the standby path was corrected on the LPAR manager management NIC.	None.
LP detected failed SR-IOV feature was recovered.	LPAR manager detected the recovery of the blocked PCI device.	The PCI device recovered from the error state. After you reboot the guest OS, the PCI device that was blocked on the LPAR will operate normally.
LP detected Driver request MCK for Shared FC.	A failure recovery request from the guest OS was accepted on the shared FC.	Check the operating status of the guest OS.
LP detected Driver request Port-Isolation for Shared FC.	A port-isolation request from the guest OS was accepted on the shared FC.	Check the operating status of the guest OS.
LP detected Link Up recovery at Shared NIC at expansion card.	Recovery to the Link Up state on the shared NIC was detected.	None.
LP detected Link Up recovery at Shared NIC at on-board.	Recovery to the Link Up state on the shared NIC was detected.	None.
LP detected Link Up recovery at Shared NIC.	Recovery to the Link Up state on the shared NIC was detected.	None.
LP detected MCK recovery for Shared FC at expansion card.	Failure recovery occurred on the shared FC.	None.
LP detected MCK recovery for Shared FC.	Failure recovery occurred on the shared FC.	None.
LP detected PCI Configuration unmatched and recovered.	The settings for the PCI device were changed because the configuration information did not match the hardware configuration.	Check the configuration and the hardware configuration.
LP detected PCI Configuration unmatched.	The configuration and the PCI device configuration do not match.	Check the configuration and the PCI device configuration.
LP detected recovery of network communication at SVP access.	A communication failure between LPAR manager and the management module was corrected.	None.
LP detected recovery Port-Isolation for Shared FC.	A port-isolation recovery request from the guest OS was accepted on the shared FC.	Check the operating status of the guest OS.

Message	Description	Solution
LP detected Shared FC Link is Available at expansion card.	The shared FC link is enabled.	None.
LP detected Shared FC Link is Available.	The shared FC link is enabled.	None.
LP detected the success of retrying the setting of TxRate configuration.	Retry of the operation to configure TxRate finished.	None.
LP detected CSTP of Core for Shared FC at expansion card.	An error occurred in the shared FC.	None.
LP detected CSTP of Core for Shared FC.	An error occurred in the shared FC.	None.
LP dump generation succeeded.	The LPAR manager dump was successfully collected.	None.
LP dump transfer retry.	The LPAR manager dump was re-transferred to the management module.	None.
LP dump transfer succeeded.	The LPAR manager dump was transferred to the management module.	None.
LP has successfully imported Time Setting of BMC.	Time settings were successfully imported from the BMC.	None.
LP has successfully imported Time Setting of SVP.	Time settings were successfully imported from the management module.	None.
LP has successfully retrieved Time Setting from SVP.	Time settings were successfully obtained from the management module.	None.
LP has successfully synchronized RTC with NTP server.	RTC synchronization via NTP succeeded.	None.
LP has successfully synchronized the time with RTC.	RTC synchronization succeeded.	None.
LP informs the maximum number of assignable VFs per physical port.	The number of assignable VFs is reported. Check the detailed information in this message.	The number of VFs that can be assigned is a number less than or equal to the value displayed in the detailed information in this message.
LP informs that no VFs per physical port can be assigned to LPARs.	VFs cannot be used. Check the detailed information in this message.	The number of available VFs is determined depending on hardware configurations. For details, see the maximum number of shares per port in SR-IOV functionality supported by LPAR manager on page B-12 .
LP Loader deleted the initial parameter.	The initial parameter file InitParam.dat required for starting LPAR manager was detected and deleted.	You do not need to take action for this message. If you need to take action, a

Message	Description	Solution
		warning-level message is displayed. Take the appropriate action according to the message.
LP Loader detected switching NIC port.	The NIC port was switched when LPAR manager started.	If this LPAR manager system log is frequently collected, contact your reseller or maintenance personnel.
LP Loader detected the initial parameter in SVP.	The initial parameter file InitParam.dat required to start LPAR manager was detected on the management module.	None.
LP Loader initialized the configuration files.	The configuration was initialized.	None.
LP Loader loaded configuration files from SVP.	The configuration was retrieved from the management module.	None.
LP Loader updated LP Serial Number in OEM FRU.	N+M cold standby failover was detected, and the FRU was updated at LPAR manager boot.	None.
LP Loader updated VfcSeed.dat in management module.	The Vfc seed information (VfcSeed.dat) in the management module was updated. This message is output after you move a server blade or install a server blade in a server chassis slot on which LPAR manager has previously run. The FRU information was synchronized with the Vfc seed information that was managed on the management module.	None.
LP logged the EFI-Driver log for Shared FC at expansion card.	The shared FC driver transferred logs to LPAR manager.	Check the SAN security configuration on the storage and the zoning setting on the FC switch.
LP logged the EFI-Driver log for Shared FC.	The shared FC driver transferred logs to LPAR manager.	Check the SAN security configuration on the storage and the zoning setting on the FC switch.
LP recovered from NTP error status.	The LPAR manager system time recovered from the NTP time synchronization error status.	None.
LP restarted a LPAR on the destination blade.	Concurrent maintenance was performed and the LPAR was restarted on the destination blade.	None.
LP restarted a LPAR on the source blade.	Concurrent maintenance was performed and the LPAR was restarted on the source blade.	None.
LP saved configuration.	The configuration was saved.	None.
LP Shutdown State Changed to InProgress.	The shutdown status changed to InProgress.	None.

Message	Description	Solution
LP Shutdown State Changed to Ready.	The shutdown status changed to Ready.	None.
LP skipped LPAR auto activation process.	The process to activate the LPAR was skipped in Auto Activate processing.	None.
LP started in safe mode.	<p>LPAR manager started in safe mode. The following operations are suppressed in safe mode:</p> <ul style="list-style-type: none"> • Saving configuration information • Activating the LPAR <p>Note that LPAR activation is enabled in safe mode caused by device isolation.</p>	<p>Take one of the following solutions.</p> <ul style="list-style-type: none"> • Revise the NIC and port settings specified for the management path, and then exit safe mode. • Back up the LPAR manager configuration and exit safe mode and check whether physical processors, memory, PCI devices are isolated.
LP switched a port of the NIC for SVP access.	The communication NIC port between LPAR manager and the management module was switched over.	None.
LP switched the active port.	The active and standby paths of the LPAR manager management NIC were switched.	None.
LP System Shutdown Started.	LPAR manager started to shut down.	None.
LP time has successfully synchronized with NTP server.	Time synchronization via NTP succeeded.	None.
LP took a checkpoint of the source LPAR.	Concurrent maintenance was performed and the LPAR was deactivated on the migration source.	None.
LP updated configuration format.	The format of the configuration was converted.	If Save Changed Config Format on the LP Options screen is not enabled, save the configuration again.
LP updated the configuration files with XXXXXXXX.	<p>The configuration file was automatically saved.</p> <p>XXXXXXXX indicates either of the following file names:</p> <ul style="list-style-type: none"> • InitParam.dat • CloneInf.dat 	None.
LP updated the configuration files.	The configuration format was converted from the old version to the new version.	None.
LP-LFW detected tftp error and recovered.	The LPAR manager logical firmware detected a network failure when a network boot was being executed, but the failure was corrected.	None.
I/O interrupt vector mode was changed.	The I/O interrupt vector mode was changed.	None.

Message	Description	Solution
Invalid State was recovered. (ptc.l)	LPAR manager recovered the invalid status of the ptc.l instruction.	None.
Logical CPU performance returns to normal.	A performance degradation due to the excesses of LPARs and logical CPUs was corrected.	None.
LPAR Migration event occurred.	LPAR migration started or ended due to the LPAR migration operation.	None.
Number of active CPU cores decreased.	The number of active cores was decreased.	None.
Number of active CPU cores increased.	The number of active cores was increased.	None.
Physical SEL has been cleared.	Physical SELs were cleared.	None.
Safe mode was turned off.	Safe mode was turned off. Save configuration information.	None.
Shadow Command was retried.	A request to LPAR manager Assist was re-sent.	None.
Shared FC MCK Log was logged in LPAR at expansion card.	The shared FC failure information was stored in the LPAR.	None.
Shared FC MCK Log was logged in LPAR.	The shared FC failure information was stored in the LPAR.	None.
SYS2 dump data collection succeeded.	SYS2 dump data collection succeeded.	None.
SYS2 dump service started.	SYS2 dump service started.	None.
SYS2 dump service stopped.	SYS2 dump service stopped.	None.
The LPAR migration functionality has recovered from an error.	The network connection between the LPAR manager and the management module recovered, and the LPAR manager functionality can now be used.	None.
The ports for the virtual COM consoles were recovered from port duplication.	Port duplication was eliminated, and the virtual COM console function can now be used.	None.
Thermal error was restored.	A temperature rise warning was released.	None.
Your CPU core usage license expired.	The number of CPU core licenses is not enough.	None.

Audit log messages

The following tables describe the notation used in audit log messages and list the audit log messages.

Notation used in audit log messages

The following table describes the notation used in audit log messages.

Table 11-6 Notation used in audit log messages

Item	Description
xxx	<ul style="list-style-type: none"> The parameter value is output. If there is no applicable value, "*" is output.
LPARxxx	<ul style="list-style-type: none"> The LPAR number and LPAR name are output, separated by a colon (:). (Example: "LPAR1:NO_NAME") If there is no applicable LPAR, "LPAR*" is output.
ProcessorGroupxxx	<ul style="list-style-type: none"> The processor group number and processor group name are output, separated by a colon (:). (Example: "ProcessorGroup0:NO_NAME") If an undefined processor group number is specified, an asterisk is output instead of the processor group name. (Example: "ProcessorGroup10:*")
Rolexxx	<ul style="list-style-type: none"> The role number and role name are output, separated by a colon (:). (Example: "Role0:Administrators") If an undefined role number is specified, an asterisk is output instead of the role name. (Example: "Role5:*")

Lists of audit log messages

The following table lists the audit log messages.

Table 11-7 List of audit log messages (Authentication)

ID	Message	Operation for which an audit log is collected
01001000	<ol style="list-style-type: none"> When the Virtual COM console is used: "Logged in to the LPAR manager. Username:xxx Session ID:xxx Source IP address:xxx Method:xxx LPARxxx VC:xxx Destination port:xxx" When the LP Web system or the HvmSh is used: "Logged in to the LPAR manager. Username:xxx Session ID:xxx Source IP address:xxx Method:xxx Destination port:xxx" 	When the login to LPAR manager succeeds
01001001	"Failed to login to the LPAR manager. Username:xxx Source IP address:xxx Method:xxx"	When the login to LPAR manager fails
01001002	"Logged out from the LPAR manager.Username:xxx Session ID:xxx Source IP address:xxx Method:xxx"	When the logout from LPAR manager completes

Table 11-8 List of audit log messages (StartStop)

ID	Message	Operation for which an audit log is collected
01000000	"Requested to shut down the LPAR manager. Accept:xxx"	When HvmSh and so on is used to request stop (shutdown) of LPAR manager and the request is accepted
01000002	"Requested to shut down the LPAR manager."	When the LPAR manager screen is used to request stop (shutdown) of LPAR manager and the request succeeds
01000003	"Failed to request to shut down the LPAR manager."	When the LPAR manager screen is used to request stop (shutdown) of LPAR manager and the request fails
01000004	"Requested to perform the force recovery. Accept:xxx"	When HvmSh and so on is used to request recovery (Force Recovery) of the system service and the request is accepted
01000006	"Performed the force recovery."	When the LPAR manager screen is used to request recovery (Force Recovery) of the system service and the request succeeds
01000007	"Failed to perform the force recovery."	When the LPAR manager screen is used to request recovery (Force Recovery) of the system service and the request fails
01000008	"Requested to restart the LPAR manager. Accept:xxx"	When HvmSh and so on is used to request restart of LPAR manager and the request is accepted
0100000A	"Requested to restart the LPAR manager."	When the LPAR manager screen is used to request restart of LPAR manager and the request succeeds
0100000B	"Failed to request to restart the LPAR manager."	When the LPAR manager screen is used to request restart of LPAR manager and the request fails
0100000C	"Requested to activate the LPAR. Accept:xxx LPARxxx"	When HvmSh and so on is used to request activation (turning on) of an LPAR and the request is accepted
0100000E	"Activated the LPAR. LPARxxx"	When the LPAR manager screen is used to request activation (turning on) of an LPAR and the request succeeds
0100000F	"Failed to activate the LPAR. LPARxxx"	When the LPAR manager screen is used to request activation (turning on) of an LPAR and the request fails
01000010	"Requested to activate the LPAR with GetBootDevice option. Accept:xxx LPARxxx"	"When HvmSh and so on is used to request, with the GetBootDevice option, the activation (turning on) of an LPAR and the request is accepted"
01000012	"Requested to activate the LPAR with SetBootOrder option. Accept:xxx LPARxxx"	"When HvmSh and so on is used to request, with the SetBootOrder option, the activation (turning on) of an LPAR and the request is accepted"

ID	Message	Operation for which an audit log is collected
01000014	"Requested to deactivate the LPAR. Accept:XXX LPARXXX"	When HvmSh and so on is used to request deactivation (turning off) of an LPAR and the request is accepted
01000016	"Deactivated the LPAR. LPARXXX"	When the LPAR manager screen is used to request deactivation (turning off) of an LPAR and the request succeeds
01000017	"Failed to deactivate the LPAR. LPARXXX"	When the LPAR manager screen is used to request deactivation (turning off) of an LPAR and the request fails
01000018	"Requested to reactivate the LPAR. Accept:XXX LPARXXX"	When HvmSh and so on is used to request reactivation (restart) of an LPAR and the request is accepted
0100001A	"Reactivated the LPAR. LPARXXX"	When the LPAR manager screen is used to request reactivation (restart) of an LPAR and the request succeeds
0100001B	"Failed to reactivate the LPAR. LPARXXX"	When the LPAR manager screen is used to request reactivation (restart) of an LPAR and the request fails
0100001C	"Canceled the auto activation."	When the LPAR manager screen is used to request cancellation of the automatic activation of an LPAR and the request succeeds
0100001D	"Failed to cancel the auto activation."	When the LPAR manager screen is used to request cancellation of the automatic activation of an LPAR and the request fails
0100001E	"Started retrieval of the guest memory dump. LPARXXX FTP_IP_address:XXX User:XXX Directory:XXX"	When HvmSh and so on is used to request start of guest memory dump collection for an LPAR and the request immediately succeeds
01000020	"Canceled retrieval of the guest memory dump. LPARXXX"	When HvmSh and so on is used to request start of guest memory dump collection for an LPAR and the request immediately succeeds
01000024	"Requested to activate the LPAR. LPARXXX"	When HvmSh and so on is used to request activation (turning on) of an LPAR and the request succeeds
01000025	"Failed to request to activate the LPAR. LPARXXX"	When HvmSh and so on is used to request activation (turning on) of an LPAR and the request fails
01000026	"Requested to shut down the LPAR manager."	When HvmSh and so on is used to request stop (shutdown) of LPAR manager and the request succeeds
01000027	"Failed to request to shut down the LPAR manager."	When HvmSh and so on is used to request stop (shutdown) of LPAR manager and the request fails
01010000	"Completed the request. Accept:XXX"	When a user performs an operation for setting Audit event type to StartStop asynchronously and the operation succeeds

ID	Message	Operation for which an audit log is collected
01010001	"Failed to complete the request. Accept:XXX"	When a user performs an operation for setting Audit event type to StartStop asynchronously and the operation fails

Table 11-9 List of audit log messages (ConfigurationAccess)

ID	Message	Operation for which an audit log is collected
01003000	"Requested to set the scheduling mode of the PCI device. Accept:XXX Slot#:XXX Port#:XXX PCI#:XXX Value:XXX"	When HvmSh and so on is used to request change of the scheduling mode of an PCI device and the request is accepted
01003002	"Set the scheduling mode of the PCI device. Slot#:XXX Port#:XXX PCI#:XXX Value:XXX"	When the LPAR manager screen is used to request change of the scheduling mode of an PCI device and the request succeeds
01003003	"Failed to set the scheduling mode of the PCI device. Slot#:XXX Port#:XXX PCI#:XXX Value:XXX"	When the LPAR manager screen is used to request change of the scheduling mode of an PCI device and the request fails
01003004	"Set the LPAR manager system time. Value:XXX"	When HvmSh and so on is used to request change of the LPAR manager system time and the request immediately succeeds
01003006	"Set the LPAR manager system time. Value:XXX"	When the LPAR manager screen is used to request change of the LPAR manager system time and the request succeeds
01003007	"Failed to set the LPAR manager system time. Value:XXX"	When the LPAR manager screen is used to request change of the LPAR manager system time and the request fails
01003008	"Set the time zone of the LPAR manager. Value:XXX"	When HvmSh and so on is used to request change of the time zone of the LPAR manager and the request immediately succeeds
0100300A	"Set the time zone of the LPAR manager. Value:XXX"	When the LPAR manager screen is used to request change of the time zone of the LPAR manager and the request succeeds
0100300B	"Failed to set the time zone of the LPAR manager. Value:XXX"	When the LPAR manager screen is used to request change of the time zone of the LPAR manager and the request fails
0100300C	"Requested to set the LP ID. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the LP identifier (LP ID) and the request is accepted
0100300E	"Set the LP ID. Value:XXX"	When the LPAR manager screen is used to request change of the LP identifier (LP ID) and the request succeeds
0100300F	"Failed to set the LP ID. Value:XXX"	When the LPAR manager screen is used to request change of the LP identifier (LP ID) and the request fails

ID	Message	Operation for which an audit log is collected
01003010	"Requested to set the IP address of BSM1. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the BSM1 IP address and the request is accepted
01003012	"Set the IP address of BSM1. Value:XXX"	When the LPAR manager screen is used to request change of the BSM1 IP address and the request succeeds
01003013	"Failed to set the IP address of BSM1. Value:XXX"	When the LPAR manager screen is used to request change of the BSM1 IP address and the request fails
01003014	"Requested to set the IP address of BSM2. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the BSM2 IP address and the request is accepted
01003016	"Set the IP address of BSM2. Value:XXX"	When the LPAR manager screen is used to request change of the BSM2 IP address and the request succeeds
01003017	"Failed to set the IP address of BSM2. Value:XXX"	When the LPAR manager screen is used to request change of the BSM2 IP address and the request fails
01003018	"Requested to set the IP address of BSM3. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the BSM3 IP address and the request is accepted
0100301A	"Set the IP address of BSM3. Value:XXX"	When the LPAR manager screen is used to request change of the BSM3 IP address and the request succeeds
0100301B	"Failed to set the IP address of BSM3. Value:XXX"	When the LPAR manager screen is used to request change of the BSM3 IP address and the request fails
0100301C	"Requested to set the IP address of BSM4. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the BSM4 IP address and the request is accepted
0100301E	"Set the IP address of BSM4. Value:XXX"	When the LPAR manager screen is used to request change of the BSM4 IP address and the request succeeds
0100301F	"Failed to set the IP address of BSM4. Value:XXX"	When the LPAR manager screen is used to request change of the BSM4 IP address and the request fails
01003020	"Requested to set the BSM1 alert port. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the BSM1 alert port and the request is accepted
01003022	"Set the BSM1 alert port. Value:XXX"	When the LPAR manager screen is used to request change of the BSM1 alert port and the request succeeds
01003023	"Failed to set the BSM1 alert port. Value:XXX"	When the LPAR manager screen is used to request change of the BSM1 alert port and the request fails

ID	Message	Operation for which an audit log is collected
01003024	"Requested to set the BSM2 alert port. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the BSM2 alert port and the request is accepted
01003026	"Set the BSM2 alert port. Value:XXX"	When the LPAR manager screen is used to request change of the BSM2 alert port and the request succeeds
01003027	"Failed to set the BSM2 alert port. Value:XXX"	When the LPAR manager screen is used to request change of the BSM2 alert port and the request fails
01003028	"Requested to set the BSM3 alert port. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the BSM3 alert port and the request is accepted
0100302A	"Set the BSM3 alert port. Value:XXX"	When the LPAR manager screen is used to request change of the BSM3 alert port and the request succeeds
0100302B	"Failed to set the BSM3 alert port. Value:XXX"	When the LPAR manager screen is used to request change of the BSM3 alert port and the request fails
0100302C	"Requested to set the BSM4 alert port. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the BSM4 alert port and the request is accepted
0100302E	"Set the BSM4 alert port. Value:XXX"	When the LPAR manager screen is used to request change of the BSM4 alert port and the request succeeds
0100302F	"Failed to set the BSM4 alert port. Value:XXX"	When the LPAR manager screen is used to request change of the BSM4 alert port and the request fails
01003030	"Requested to set the IP address (IPv4) of CLI1. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the LP CLI1 IPv4 address and the request is accepted
01003032	"Set the IP address (IPv4) of CLI1. Value:XXX"	When the LPAR manager screen is used to request change of the LP CLI1 IPv4 address and the request succeeds
01003033	"Failed to set the IP address (IPv4) of CLI1. Value:XXX"	When the LPAR manager screen is used to request change of the LP CLI1 IPv4 address and the request fails
01003034	"Requested to set the IP address (IPv4) of CLI2. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the LP CLI2 IPv4 address and the request is accepted
01003036	"Set the IP address (IPv4) of CLI2. Value:XXX"	When the LPAR manager screen is used to request change of the LP CLI2 IPv4 address and the request succeeds
01003037	"Failed to set the IP address (IPv4) of CLI2. Value:XXX"	When the LPAR manager screen is used to request change of the LP CLI2 IPv4 address and the request fails

ID	Message	Operation for which an audit log is collected
01003038	"Requested to set the IP address (IPv4) of CLI3. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of the LP CLI3 IPv4 address and the request is accepted
0100303A	"Set the IP address (IPv4) of CLI3. Value:xxx"	When the LPAR manager screen is used to request change of the LP CLI3 IPv4 address and the request succeeds
0100303B	"Failed to set the IP address (IPv4) of CLI3. Value:xxx"	When the LPAR manager screen is used to request change of the LP CLI3 IPv4 address and the request fails
0100303C	"Requested to set the IP address (IPv4) of CLI4. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of the LP CLI4 IPv4 address and the request is accepted
0100303E	"Set the IP address (IPv4) of CLI4. Value:xxx"	When the LPAR manager screen is used to request change of the LP CLI4 IPv4 address and the request succeeds
0100303F	"Failed to set the IP address (IPv4) of CLI4. Value:xxx"	When the LPAR manager screen is used to request change of the LP CLI4 IPv4 address and the request fails
01003040	"Requested to set the IP address (IPv4) of CLI5. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of the LP CLI5 IPv4 address and the request is accepted
01003042	"Set the IP address (IPv4) of CLI5. Value:xxx"	When the LPAR manager screen is used to request change of the LP CLI5 IPv4 address and the request succeeds
01003043	"Failed to set the IP address (IPv4) of CLI5. Value:xxx"	When the LPAR manager screen is used to request change of the LP CLI5 IPv4 address and the request fails
01003044	"Requested to set the IP address (IPv4) of CLI6. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of the LP CLI6 IPv4 address and the request is accepted
01003046	"Set the IP address (IPv4) of CLI6. Value:xxx"	When the LPAR manager screen is used to request change of the LP CLI6 IPv4 address and the request succeeds
01003047	"Failed to set the IP address (IPv4) of CLI6. Value:xxx"	When the LPAR manager screen is used to request change of the LP CLI6 IPv4 address and the request fails
01003048	"Requested to set the IP address (IPv4) of CLI7. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of the LP CLI7 IPv4 address and the request is accepted
0100304A	"Set the IP address (IPv4) of CLI7. Value:xxx"	When the LPAR manager screen is used to request change of the LP CLI7 IPv4 address and the request succeeds
0100304B	"Failed to set the IP address (IPv4) of CLI7. Value:xxx"	When the LPAR manager screen is used to request change of the LP CLI7 IPv4 address and the request fails

ID	Message	Operation for which an audit log is collected
0100304C	"Requested to set the IP address (IPv4) of CLI8. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the LP CLI8 IPv4 address and the request is accepted
0100304E	"Set the IP address (IPv4) of CLI8. Value:XXX"	When the LPAR manager screen is used to request change of the LP CLI8 IPv4 address and the request succeeds
0100304F	"Failed to set the IP address (IPv4) of CLI8. Value:XXX"	When the LPAR manager screen is used to request change of the LP CLI8 IPv4 address and the request fails
01003050	"Requested to set the VNIC System No. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the VNIC system No. and the request is accepted
01003052	"Set the VNIC System No. Value:XXX"	When the LPAR manager screen is used to request change of the VNIC system No. and the request succeeds
01003053	"Failed to set the VNIC System No. Value:XXX"	When the LPAR manager screen is used to request change of the VNIC system No. and the request fails
01003054	"Requested to set the alert language. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the Alert Language and the request is accepted
01003056	"Set the alert language. Value:XXX"	When the LPAR manager screen is used to request change of the Alert Language and the request succeeds
01003057	"Failed to set the alert language. Value:XXX"	When the LPAR manager screen is used to request change of the Alert Language and the request fails
01003058	"Requested to set the virtual COM console port. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the TCP port number of a virtual COM console and the request is accepted
0100305A	"Set the virtual COM console port. Value:XXX"	When the LPAR manager screen is used to request change of the TCP port number of a virtual COM console and the request succeeds
0100305B	"Failed to set the virtual COM console port. Value:XXX"	When the LPAR manager screen is used to request change of the TCP port number of a virtual COM console and the request fails
0100305C	"Requested to set the maximum CPU resource usage of SYS2. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the maximum number of processors for SYS2 and the request is accepted.
0100305E	"Removed the LPAR. LPARXXX"	When HvmSh and so on is used to request deletion of an LPAR and the request immediately succeeds
01003060	"Removed the LPAR. LPARXXX"	When the LPAR manager screen is used to request deletion of an LPAR and the request succeeds

ID	Message	Operation for which an audit log is collected
01003061	"Failed to remove the LPAR. LPARXXX"	When the LPAR manager screen is used to request deletion of an LPAR and the request fails
01003062	"Added the LPAR. LPARXXX"	When HvmSh and so on is used to request addition of an LPAR and the request immediately succeeds
01003064	"Added the LPAR. LPARXXX"	When the LPAR manager screen is used to request addition of an LPAR and the request succeeds
01003065	"Failed to add the LPAR. LPARXXX"	When the LPAR manager screen is used to request addition of an LPAR and the request fails
01003066	"Set the name for the LPAR. LPAR#:XXX Value:XXX"	When HvmSh and so on is used to request change of the LPAR name and the request immediately succeeds
01003068	"Set the name for the LPAR. LPAR#:XXX Value:XXX"	When the LPAR manager screen is used to request change of the LPAR name and the request succeeds
01003069	"Failed to set the name for the LPAR. LPAR#:XXX Value:XXX"	When the LPAR manager screen is used to request change of the LPAR name and the request fails
0100306A	"Set the scheduling mode for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the scheduling mode of logical processors for an LPAR and the request immediately succeeds
0100306C	"Set the service ratio for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the service ratio of an LPAR and the request immediately succeeds
0100306E	"Set the service ratio for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the service ratio of an LPAR and the request succeeds
0100306F	"Failed to set the service ratio for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the service ratio of an LPAR and the request fails
01003070	"Set the memory size for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the memory size for an LPAR with its guest NUMA disabled and the request immediately succeeds
01003072	"Set the memory size for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the memory size for an LPAR with its guest NUMA disabled and the request succeeds
01003073	"Failed to set the memory size for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the memory size for an LPAR with its guest NUMA disabled and the request fails

ID	Message	Operation for which an audit log is collected
01003074	"Set the idle detection(ID) for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the Idle Detection functionality for an LPAR and the request immediately succeeds
01003076	"Set the idle detection(ID) for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the Idle Detection functionality for an LPAR and the request succeeds
01003077	"Failed to set the idle detection(ID) for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the Idle Detection functionality for an LPAR and the request fails
01003078	"Set the auto activation(AA) order for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the automatic activation functionality for an LPAR and the request immediately succeeds
0100307A	"Set the auto activation(AA) order for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the automatic activation functionality for an LPAR and the request succeeds
0100307B	"Failed to set the auto activation(AA) order for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the automatic activation functionality for an LPAR and the request fails
0100307C	"Set the auto clear(AC) for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the automatic clear of the logical SEL for an LPAR and the request immediately succeeds
0100307E	"Set the auto clear(AC) for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the automatic clear of the logical SEL for an LPAR and the request succeeds
0100307F	"Failed to set the auto clear(AC) for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the automatic clear of the logical SEL for an LPAR and the request fails
01003080	"Set the processor capping(PC) for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the processor capping functionality for an LPAR and the request immediately succeeds
01003082	"Set the processor capping(PC) for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the processor capping functionality for an LPAR and the request succeeds
01003083	"Failed to set the processor capping(PC) for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the processor capping functionality for an LPAR and the request fails
01003084	"Set the pre-boot(PB) firmware for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the Pre-boot firmware for an LPAR and the request immediately succeeds

ID	Message	Operation for which an audit log is collected
01003086	"Set the pre-boot(PB) firmware for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the Pre-boot firmware for an LPAR and the request succeeds
01003087	"Failed to set the pre-boot(PB) firmware for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the Pre-boot firmware for an LPAR and the request fails
01003088	"Assigned the physical processor to the logical processor for the LPAR. LPARXXX LCPU#:XXX Value:XXX"	When HvmSh and so on is used to request change of logical processor assignment for an LPAR and the request immediately succeeds
0100308A	"Assigned the physical processor to the logical processor for the LPAR. LPARXXX LCPU#:XXX Value:XXX"	When the LPAR manager screen is used to request change of logical processor assignment for an LPAR and the request succeeds
0100308B	"Failed to assign the physical processor to the logical processor for the LPAR. LPARXXX LCPU#:XXX Value:XXX"	When the LPAR manager screen is used to request change of logical processor assignment for an LPAR and the request fails
0100308C	"Set the number of logical processors for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the number of logical processors for an LPAR and the request immediately succeeds
0100308E	"Set the number of logical processors for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the number of logical processors for an LPAR and the request succeeds
0100308F	"Failed to set the number of logical processors for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the number of logical processors for an LPAR and the request fails
01003090	"Assigned the logical PCI device to the LPAR. LPARXXX Slot#:XXX Port#:XXX PCI#:XXX Value:XXX"	When HvmSh and so on is used to request change of PCI device assignment for an LPAR and the request immediately succeeds
01003092	"Assigned the logical PCI device to the LPAR. LPARXXX Slot#:XXX Port#:XXX PCI#:XXX Value:XXX"	When the LPAR manager screen is used to request change of PCI device assignment for an LPAR and the request succeeds
01003093	"Failed to assign the logical PCI device to the LPAR. LPARXXX Slot#:XXX Port#:XXX PCI#:XXX Value:XXX"	When the LPAR manager screen is used to request change of PCI device assignment for an LPAR and the request fails
01003094	"Enabled or disabled the USB Auto Attach settings to the LPAR. LPARXXX Slot#:XXX PCI#:XXX Value:XXX"	When HvmSh and so on is used to request change of USB Auto Attach setting for a specified LPAR and the request immediately succeeds
01003096	"Enabled or disabled the USB Auto Attach settings to the LPAR. LPARXXX Slot#:XXX PCI#:XXX Value:XXX"	When the LPAR manager screen is used to request change of USB Auto Attach setting for a specified LPAR and the request succeeds
01003097	"Failed to enable or disable the USB Auto Attach settings to the LPAR. LPARXXX Slot#:XXX PCI#:XXX Value:XXX"	When the LPAR manager screen is used to request change of USB Auto Attach setting for a specified LPAR and the request fails

ID	Message	Operation for which an audit log is collected
01003098	"Assigned the network segment of the VNIC to the LPAR. LPARXXX VNIC#:XXX Value:XXX"	When HvmSh and so on is used to request change of a network segment to be assigned to a logical NIC port and the request immediately succeeds
0100309A	"Assigned the network segment of the VNIC to the LPAR. LPARXXX VNIC#:XXX Value:XXX"	When the LPAR manager screen is used to request change of a network segment to be assigned to a logical NIC port and the request succeeds
0100309B	"Failed to assign the network segment of the VNIC to the LPAR. LPARXXX VNIC#:XXX Value:XXX"	When the LPAR manager screen is used to request change of a network segment to be assigned to a logical NIC port and the request fails
0100309C	"Set the MAC address of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:XXX"	When HvmSh and so on is used to request change of a MAC address to be assigned to a logical NIC port and the request immediately succeeds
0100309E	"Set the MAC address of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:XXX"	When the LPAR manager screen is used to request change of a MAC address to be assigned to a logical NIC port and the request succeeds
0100309F	"Failed to set the MAC address of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:XXX"	When the LPAR manager screen is used to request change of a MAC address to be assigned to a logical NIC port and the request fails
010030A0	"Set the VLAN configuration of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:Undef"	When HvmSh and so on is used to request change of VLAN mode of a logical NIC port to Undef and the request immediately succeeds
010030A2	"Set the VLAN configuration of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:Undef"	When the LPAR manager screen is used to request change of VLAN mode of a logical NIC port to Undef and the request succeeds
010030A3	"Failed to set the VLAN configuration of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:Undef"	When the LPAR manager screen is used to request change of VLAN mode of a logical NIC port to Undef and the request fails
010030A4	"Set the VLAN configuration of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:Untagged(XXX) "	When HvmSh and so on is used to request change of VLAN mode of a logical NIC port to Untag and the request immediately succeeds
010030A6	"Set the VLAN configuration of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:Untagged(XXX) "	When the LPAR manager screen is used to request change of VLAN mode of a logical NIC port to Untag and the request succeeds
010030A7	"Failed to set the VLAN configuration of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:Untagged(XXX) "	When the LPAR manager screen is used to request change of VLAN mode of a logical NIC port to Untag and the request fails
010030A8	"Set the VLAN configuration of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:Tagged(XXX) "	When HvmSh and so on is used to request change of VLAN mode of a logical NIC port to Tag and the request immediately succeeds

ID	Message	Operation for which an audit log is collected
010030AA	"Set the VLAN configuration of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:Tagged(XXX) "	When the LPAR manager screen is used to request change of VLAN mode of a logical NIC port to Tag and the request succeeds
010030AB	"Failed to set the VLAN configuration of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:Tagged(XXX) "	When the LPAR manager screen is used to request change of VLAN mode of a logical NIC port to Tag and the request fails
010030AC	"Assigned the shared FC port to the LPAR. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of a shared FC assignment for an LPAR and the request immediately succeeds
010030AE	"Assigned the shared FC port to the LPAR. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When the LPAR manager screen is used to request change of a shared FC assignment for an LPAR and the request succeeds
010030AF	"Failed to assign the shared FC port to the LPAR. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When the LPAR manager screen is used to request change of a shared FC assignment for an LPAR and the request fails
010030B0	"Set the date and time of logical SEL time for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the SEL time for an LPAR and the request immediately succeeds
010030B2	"Set the date and time of logical SEL time for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the SEL time for an LPAR and the request succeeds
010030B3	"Failed to set the date and time of logical SEL time for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the SEL time for an LPAR and the request fails
010030B4	"Set the time mode of logical SEL time for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the SEL time mode (TimeMode) for an LPAR and the request immediately succeeds
010030B6	"Set the time zone of logical SEL time for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the SEL time zone (TimeZone) for an LPAR and the request immediately succeeds
010030B8	"Set the inter-LPAR packet filtering mode for the network segment. Segment:XXX Value:XXX"	When HvmSh and so on is used to request setting change of inter-LPAR communication packet filtering and the request immediately succeeds
010030BA	"Set the inter-LPAR packet filtering mode for the network segment. Segment:XXX Value:XXX"	When the LPAR manager screen is used to request setting change of inter-LPAR communication packet filtering and the request succeeds
010030BB	"Failed to set the inter-LPAR packet filtering mode for the network segment. Segment:XXX Value:XXX"	When the LPAR manager screen is used to request setting change of inter-LPAR communication packet filtering and the request fails

ID	Message	Operation for which an audit log is collected
010030BC	"Set the virtual COM console functionality (and specified the VC number). LPARXXX Value:XXX"	When HvmSh and so on is used to request setting change of the virtual COM console functionality for an LPAR and the request immediately succeeds
010030BE	"Set the virtual COM console functionality (and specified the VC number). LPARXXX Value:XXX"	When the LPAR manager screen is used to request setting change of the virtual COM console functionality for an LPAR and the request succeeds
010030BF	"Failed to set the virtual COM console functionality (and specified the VC number). LPARXXX Value:XXX"	When the LPAR manager screen is used to request setting change of the virtual COM console functionality for an LPAR and the request fails
010030C0	"Set the time mode of logical SEL time for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request setting change of the SEL time mode for an LPAR and the request succeeds
010030C1	"Failed to set the time mode of logical SEL time for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request setting change of the SEL time mode for an LPAR and the request fails
010030C2	"Set the time zone of logical SEL time for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request setting change of the SEL time mode for an LPAR and the request succeeds
010030C3	"Failed to set the time zone of logical SEL time for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request setting change of the SEL time mode for an LPAR and the request fails
010030C4	"Connected to the guest screen for the LPAR. LPARXXX"	When the LPAR manager screen is used to request switch from the LPAR manager screen to the guest screen and the request succeeds
010030C5	"Failed to connect to the guest screen for the LPAR. LPARXXX"	When the LPAR manager screen is used to request switch from the LPAR manager screen to the guest screen and the request fails
010030C6	"Disconnected from the guest screen for the LPAR. LPARXXX"	When the LPAR manager screen is used to request switch from the LPAR manager screen to the guest screen and the request succeeds
010030C7	"Failed to disconnect from the guest screen for the LPAR. LPARXXX"	When the LPAR manager screen is used to request switch from the LPAR manager screen to the guest screen and the request fails
010030C8	"Requested to assign the processor group to the LPAR. Accept:XXX LPARXXX ProcessorGroupXXX"	When HvmSh and so on is used to request change of processor group for an LPAR and the request is accepted
010030CA	"Assigned the processor group to the LPAR. LPARXXX ProcessorGroupXXX"	When the LPAR manager screen is used to request change of processor group for an LPAR and the request succeeds

ID	Message	Operation for which an audit log is collected
010030CB	"Failed to assign the processor group to the LPAR. LPARXXX ProcessorGroupXXX"	When the LPAR manager screen is used to request change of processor group for an LPAR and the request fails
010030CC	"Set the promiscuous mode of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:XXX"	When HvmSh and so on is used to request change of the promiscuous mode for the logical NIC port and the request immediately succeeds
010030CE	"Set the promiscuous mode of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:XXX"	When the LPAR manager screen is used to request change of the promiscuous mode for the logical NIC port and the request succeeds
010030CF	"Failed to set the promiscuous mode of the VNIC for the LPAR. LPARXXX VNIC#:XXX Value:XXX"	When the LPAR manager screen is used to request change of the promiscuous mode for the logical NIC port and the request fails
010030D0	"Set the option of pre-state auto activation. Value:XXX"	When HvmSh and so on is used to request change of the Pre-State Auto Activation option and the request immediately succeeds
010030D2	"Set the option of pre-state auto activation. Value:XXX"	When the LPAR manager screen is used to request change of the Pre-State Auto Activation option and the request succeeds
010030D3	"Failed to set the option of pre-state auto activation. Value:XXX"	When the LPAR manager screen is used to request change of the Pre-State Auto Activation option and the request fails
010030D4	"Set the option of LPAR manager auto shutdown. Value:XXX"	When HvmSh and so on is used to request change of an LPAR manager Auto Shutdown option and the request immediately succeeds
010030D6	"Set the option of LPAR manager auto shutdown. Value:XXX"	When the LPAR manager screen is used to request change of an LPAR manager Auto Shutdown option and the request succeeds
010030D7	"Failed to set the option of LPAR manager auto shutdown. Value:XXX"	When the LPAR manager screen is used to request change of an LPAR manager Auto Shutdown option and the request fails
010030D8	"Reset the shutdown state of the LPAR manager."	When HvmSh and so on is used to request change of Shutdown State and the request immediately succeeds
010030DA	"Reset the shutdown state of the LPAR manager."	When the LPAR manager screen is used to request change of Shutdown State and the request succeeds
010030DB	"Failed to reset the shutdown state of the LPAR manager."	When the LPAR manager screen is used to request change of Shutdown State and the request fails
010030DC	"Set the option of LPAR manager error watching. Value:XXX"	When HvmSh and so on is used to request change of LPAR manager ErrorWatching option and the request immediately succeeds
010030DE	"Set the option of LPAR manager error watching. Value:XXX"	When the LPAR manager screen is used to request change of LPAR manager

ID	Message	Operation for which an audit log is collected
		ErrorWatching option and the request succeeds
010030DF	"Failed to set the option of LPAR manager error watching. Value:xxx"	When the LPAR manager screen is used to request change of LPAR manager ErrorWatching option and the request fails
010030E0	"Set the option to confirm activation. Value:xxx"	When HvmSh and so on is used to request change of the confirmation option for Activation and the request immediately succeeds
010030E2	"Set the option to confirm activation. Value:xxx"	When the LPAR manager screen is used to request change of the confirmation option for Activation and the request succeeds
010030E3	"Failed to set the option to confirm activation. Value:xxx"	When the LPAR manager screen is used to request change of the confirmation option for Activation and the request fails
010030E4	"Set the option to confirm deactivation and reactivation. Value:xxx"	When HvmSh and so on is used to request change of the confirmation option for Deactivation or Reactivation. and the request immediately succeeds
010030E6	"Set the option to confirm deactivation and reactivation. Value:xxx"	When the LPAR manager screen is used to request change of the confirmation option for Deactivation or Reactivation. and the request succeeds
010030E7	"Failed to set the option to confirm deactivation and reactivation. Value:xxx"	When the LPAR manager screen is used to request change of the confirmation option for Deactivation or Reactivation. and the request fails
010030E8	"Set the Screen Switching Character. Value:xxx"	When HvmSh and so on is used to request change of the Screen Switching Character option and the request immediately succeeds
010030EA	"Set the Screen Switching Character. Value:xxx"	When the LPAR manager screen is used to request change of the Screen Switching Character option and the request succeeds
010030EB	"Failed to set the Screen Switching Character. Value:xxx"	When the LPAR manager screen is used to request change of the Screen Switching Character option and the request fails
010030EC	"Enabled or disabled the power saving functionality for physical processors. Value:xxx"	When HvmSh and so on is used to request change of the PhyCPU C-State (>= C3) option. and the request immediately succeeds
010030EE	"Enabled or disabled the power saving functionality for physical processors. Value:xxx"	When the LPAR manager screen is used to request change of the PhyCPU C-State (>= C3) option. and the request succeeds
010030EF	"Failed to enable or disable the power saving functionality for physical processors. Value:xxx"	When the LPAR manager screen is used to request change of the PhyCPU C-State (>= C3) option. and the request fails

ID	Message	Operation for which an audit log is collected
010030F0	"Enabled or disabled the option of the USB Auto Allocation to LPAR. Value:XXX"	When HvmSh and so on is used to request change of the USB Auto Allocation to LPAR option and the request immediately succeeds
010030F2	"Enabled or disabled the option of the USB Auto Allocation to LPAR. Value:XXX"	When the LPAR manager screen is used to request change of the USB Auto Allocation to LPAR option and the request succeeds
010030F3	"Failed to enable or disable the option of the USB Auto Allocation to LPAR. Value:XXX"	When the LPAR manager screen is used to request change of the USB Auto Allocation to LPAR option and the request fails
010030F4	"Enabled or disabled the option of the Save Changed Config Format. Value:XXX"	When HvmSh and so on is used to request change of the Save Changed Config Format option and the request immediately succeeds
010030F6	"Enabled or disabled the option of the Save Changed Config Format. Value:XXX"	When the LPAR manager screen is used to request change of the Save Changed Config Format option and the request succeeds
010030F7	"Failed to enable or disable the option of the Save Changed Config Format. Value:XXX"	When the LPAR manager screen is used to request change of the Save Changed Config Format option and the request fails
010030F8	"Enabled or disabled the option of the Save Time Config. Value:XXX"	When HvmSh and so on is used to request change of the Save Time Config option and the request immediately succeeds
010030FA	"Enabled or disabled the option of the Save Time Config. Value:XXX"	When the LPAR manager screen is used to request change of the Save Time Config option and the request succeeds
010030FB	"Failed to enable or disable the option of the Save Time Config. Value:XXX"	When the LPAR manager screen is used to request change of the Save Time Config option and the request fails
010030FC	"Reset the safe mode of the LPAR manager."	When HvmSh and so on is used to request release from safe mode and the request immediately succeeds
010030FE	"Reset the safe mode of the LPAR manager."	When the LPAR manager screen is used to request release from safe mode and the request succeeds
010030FF	"Failed to reset the safe mode of the LPAR manager."	When the LPAR manager screen is used to request release from safe mode and the request fails
01003100	"Requested to save the configuration. Accept:XXX"	When HvmSh and so on is used to request saving of the LPAR manager configuration and the request is accepted
01003102	"Saved the configuration."	When the LPAR manager screen is used to request saving of the LPAR manager configuration and the request succeeds
01003103	"Failed to save the configuration."	When the LPAR manager screen is used to request saving of the LPAR manager configuration and the request fails

ID	Message	Operation for which an audit log is collected
01003104	"Requested to save the configuration for LPAR manager encryption communication. Accept:XXX"	When HvmSh and so on is used to request saving of the LPAR manager configuration of encrypted communication. and the request is accepted
01003106	"Set the IO connection mode of the FC HBA. Slot#:XXX Port#:XXX VFCID:XXX Value:XXX"	When HvmSh and so on is used to request change of the IO connection mode for a shared FC port and the request immediately succeeds
01003108	"Executed an unsupported command (set VfcWWN). RelSlot:XXX Port#:XXX VFCID:XXX Value:XXX"	When HvmSh and so on is used to request change of WWN for the shared FC port and the request immediately succeeds
0100310C	"Executed an unsupported command (set LPARRTCdiff). LPARXXX Value:XXX"	When HvmSh and so on is used to request change of time difference between the LPAR RTC time and the LPAR manager system time (for LPAR relocation) and the request immediately succeeds
0100310E	"Executed an unsupported command (set ActInhibit). LPARXXX Value:XXX"	When HvmSh and so on is used to request change of LPAR activation inhibit and the request immediately succeeds
01003110	"Executed an unsupported command (set AutoVnicMac). LPARXXX VnicSystemNo:XXX LPAR#:XXX"	When HvmSh and so on is used to request information that is used in automatic generation of a MAC address for a logical NIC port (for LPAR relocation) and the request immediately succeeds
01003112	"Executed an unsupported command (set VfcIdChangeInhibit). LPARXXX Value:XXX"	When HvmSh and so on is used to request setting of VFCID change inhibit (for LPAR relocation) and the request immediately succeeds
01003114	"Requested to add the processor group. Accept:XXX ProcessorGroup#:XXX"	When HvmSh and so on is used to request addition of a processor group and the request is accepted
01003116	"Added the processor group. ProcessorGroup#:XXX"	When the LPAR manager screen is used to request addition of a processor group and the request succeeds
01003117	"Failed to add the processor group. ProcessorGroup#:XXX"	When the LPAR manager screen is used to request addition of a processor group and the request fails
01003118	"Requested to remove the processor group. Accept:XXX ProcessorGroupXXX"	When HvmSh and so on is used to request deletion of a processor group and the request is accepted
0100311A	"Removed the processor group. ProcessorGroupXXX"	When the LPAR manager screen is used to request deletion of a processor group and the request succeeds
0100311B	"Failed to remove the processor group. ProcessorGroupXXX"	When the LPAR manager screen is used to request deletion of a processor group and the request fails

ID	Message	Operation for which an audit log is collected
0100311C	"Set the name of the processor group. ProcessorGroup#:XXX Value:XXX"	When HvmSh and so on is used to request change of the processor group name and the request immediately succeeds
0100311E	"Set the name of the processor group. ProcessorGroup#:XXX Value:XXX"	When the LPAR manager screen is used to request change of the processor group name and the request succeeds
0100311F	"Failed to set the name of the processor group. ProcessorGroup#:XXX Value:XXX"	When the LPAR manager screen is used to request change of the processor group name and the request fails
01003120	"Requested to assign the processor group to the physical processor. Accept:XXX PhysicalProcessor#:XXX ProcessorGroupXXX"	When HvmSh and so on is used to request change of the processor group to which the physical processor belongs and the request is accepted
01003122	"Assigned the processor group to the physical processor. PhysicalProcessor#:XXX ProcessorGroupXXX"	When the LPAR manager screen is used to request change of the processor group to which the physical processor belongs and the request succeeds
01003123	"Failed to assign the processor group to the physical processor. PhysicalProcessor#:XXX ProcessorGroupXXX"	When the LPAR manager screen is used to request change of the processor group to which the physical processor belongs and the request fails
01003124	"Requested to set the scheduling mode for the LPAR. Accept:XXX LPARXXX Value:XXX"	When HvmSh and so on is used to request the scheduling mode of logical processors for an LPAR and the request is accepted
01003126	"Set the scheduling mode for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request the scheduling mode of logical processors for an LPAR and the request succeeds
01003127	"Failed to set the scheduling mode for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request the scheduling mode of logical processors for an LPAR and the request fails
01003128	"Requested to set the physical processor core state. Accept:XXX PhysicalProcessor#:XXX Value:XXX"	When HvmSh and so on is used to request the statuses of processor cores (physical processors) and the request is accepted
0100312A	"Set the physical processor core state. PhysicalProcessor#:XXX Value:XXX"	When the LPAR manager screen is used to request the statuses of processor cores (physical processors) and the request succeeds
0100312B	"Failed to set the physical processor core state. PhysicalProcessor#:XXX Value:XXX"	When the LPAR manager screen is used to request the statuses of processor cores (physical processors) and the request fails
0100312C	"Requested to adjust the RTC time and the SEL time for the LPAR to the LPAR manager system time or the UTC time. Accept:XXX LPARXXX TimeSource:XXX"	When HvmSh and so on is used to request the process for synchronizing the LPAR RTC time and the LPAR SEL time with the LPAR manager system time or the UTC time. and the request is accepted

ID	Message	Operation for which an audit log is collected
0100312E	"Adjusted the RTC time and the SEL time for the LPAR to the LPAR manager system time or the UTC time. LPARXXX TimeSource:XXX"	When the LPAR manager screen is used to request the process for synchronizing the LPAR RTC time and the LPAR SEL time with the LPAR manager system time or the UTC time. and the request succeeds
0100312F	"Failed to adjust the RTC time and the SEL time for the LPAR to the LPAR manager system time or the UTC time. LPARXXX TimeSource:XXX"	When the LPAR manager screen is used to request the process for synchronizing the LPAR RTC time and the LPAR SEL time with the LPAR manager system time or the UTC time. and the request fails
01003130	"Requested to adjust the RTC time and the SEL time for the LPAR to the LPAR manager system time in the specified time zone. Accept:XXX LPARXXX TimeZone:XXX"	When HvmSh and so on is used to request the process for synchronizing the LPAR RTC time and the LPAR SEL time with the LPAR manager system time and specifying the TimeZone and the request is accepted
01003132	"Adjusted the RTC time and the SEL time for the LPAR to the LPAR manager system time in the specified time zone. LPARXXX TimeZone:XXX"	When the LPAR manager screen is used to request the process for synchronizing the LPAR RTC time and the LPAR SEL time with the LPAR manager system time and specifying the TimeZone and the request succeeds
01003133	"Failed to adjust the RTC time and the SEL time for the LPAR to the LPAR manager system time in the specified time zone. LPARXXX TimeZone:XXX"	When the LPAR manager screen is used to request the process for synchronizing the LPAR RTC time and the LPAR SEL time with the LPAR manager system time and specifying the TimeZone and the request fails
01003134	"Requested to adjust the RTC time and the SEL time for all LPARs to the LPAR manager system time or the UTC time. Accept:XXX TimeSource:XXX"	When HvmSh and so on is used to request the process for synchronizing all of the LPAR RTC times and the LPAR SEL times with the LPAR manager system time or the UTC time and the request is accepted
01003136	"Adjusted the RTC time and the SEL time for all LPARs to the LPAR manager system time or the UTC time. TimeSource:XXX"	When the LPAR manager screen is used to request the process for synchronizing all of the LPAR RTC times and the LPAR SEL times with the LPAR manager system time or the UTC time and the request succeeds
01003137	"Failed to adjust the RTC time and the SEL time for all LPARs to the LPAR manager system time or the UTC time. TimeSource:XXX"	When the LPAR manager screen is used to request the process for synchronizing all of the LPAR RTC times and the LPAR SEL times with the LPAR manager system time or the UTC time and the request fails
01003138	"Requested to adjust the RTC time and the SEL time for all LPARs to the LPAR manager system time in the specified time zone. Accept:XXX TimeZone:XXX"	When HvmSh and so on is used to request process for synchronizing all of the LPAR RTC times and the LPAR SEL times with the LPAR manager system time and specifying the TimeZone and the request is accepted
0100313A	"Adjusted the RTC time and the SEL time for all LPARs to the LPAR manager	When the LPAR manager screen is used to request the process for synchronizing all of the LPAR RTC times and the LPAR SEL times with the LPAR manager system time and

ID	Message	Operation for which an audit log is collected
	system time in the specified time zone. TimeZone:XXX"	specifying the TimeZone and the request succeeds
0100313B	"Failed to adjust the RTC time and the SEL time for all LPARs to the LPAR manager system time in the specified time zone. TimeZone:XXX"	When the LPAR manager screen is used to request the process for synchronizing all of the LPAR RTC times and the LPAR SEL times with the LPAR manager system time and specifying the TimeZone and the request fails
0100313C	"Requested to clear the NVRAM for the LPAR. Accept:XXX LPARXXX"	When HvmSh and so on is used to request clearing of NVRAM of an LPAR and the request is accepted
0100313E	"Cleared the NVRAM for the LPAR. LPARXXX"	When the LPAR manager screen is used to request clearing of NVRAM of an LPAR and the request succeeds
0100313F	"Failed to clear the NVRAM for the LPAR. LPARXXX"	When the LPAR manager screen is used to request clearing of NVRAM of an LPAR and the request fails
01003140	"Requested to copy the NVRAM for the LPAR. Accept:XXX SrcLPARXXX DstLPARXXX"	When HvmSh and so on is used to request copying of NVRAM of an LPAR and the request is accepted
01003142	"Copied the NVRAM for the LPAR. SrcLPARXXX DstLPARXXX"	When the LPAR manager screen is used to request copying of NVRAM of an LPAR and the request succeeds
01003143	"Failed to copy the NVRAM for the LPAR. SrcLPARXXX DstLPARXXX"	When the LPAR manager screen is used to request copying of NVRAM of an LPAR and the request fails
01003144	"Requested to erase console log data for the LPAR. Accept:XXX LPARXXX"	When HvmSh and so on is used to request deletion of the LPAR console log and the request is accepted
01003146	"Erased the console log data for the LPAR. LPARXXX"	When the LPAR manager screen is used to request deletion of the LPAR console log and the request succeeds
01003147	"Failed to erase the console log data for the LPAR. LPARXXX"	When the LPAR manager screen is used to request deletion of the LPAR console log and the request fails
01003174	"Requested to set the synchronization method of LPAR manager system time. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the time synchronization with NTP server (TimeSync) and the request is accepted
01003176	"Set the synchronization method of LPAR manager system time. Value:XXX"	When the LPAR manager screen is used to request change of the time synchronization with NTP server (TimeSync) and the request succeeds
01003177	"Failed to set the synchronization method of LPAR manager system time. Value:XXX"	When the LPAR manager screen is used to request change of the time synchronization with NTP server (TimeSync) and the request fails

ID	Message	Operation for which an audit log is collected
01003178	"Requested to set NTP server1 to synchronize the LPAR manager system time. Accept:XXX Value:XXX"	When HvmSh and so on is used to request setting change of NTP Server1 and the request is accepted
0100317A	"Set the NTP server1 to synchronize LPAR manager system time. Value:XXX"	When the LPAR manager screen is used to request setting change of NTP Server1 and the request succeeds
0100317B	"Failed to set the NTP server1 to synchronize LPAR manager system time. Value:XXX"	When the LPAR manager screen is used to request setting change of NTP Server1 and the request fails
0100317C	"Requested to set NTP server2 to synchronize LPAR manager system time. Accept:XXX Value:XXX"	When HvmSh and so on is used to request setting change of NTP Server2 and the request is accepted
0100317E	"Set NTP server2 to synchronize LPAR manager system time. Value:XXX"	When the LPAR manager screen is used to request setting change of NTP Server2 and the request succeeds
0100317F	"Failed to set NTP server2 to synchronize LPAR manager system time. Value:XXX"	When the LPAR manager screen is used to request setting change of NTP Server2 and the request fails
01003180	"Requested to import the NTP settings of the LPAR manager. Accept:XXX From:XXX"	When HvmSh and so on is used to request importing of NTP setting (Import Config) and the request is accepted
01003182	"Imported the NTP settings of the LPAR manager. From:XXX"	When the LPAR manager screen is used to request importing of NTP setting (Import Config) and the request succeeds
01003183	"Failed to import the NTP settings of the LPAR manager. From:XXX"	When the LPAR manager screen is used to request importing of NTP setting (Import Config) and the request fails
01003184	"Initialized all options of the FC HBA driver. LPARXXX Slot#:XXX Port#:XXX"	When HvmSh and so on is used to request clearing of the options of the FC HBA driver of the logical EFI and the request immediately succeeds
01003186	"Enabled or disabled the BootFunction of the FC HBA driver option. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the bootfunc option of the FC HBA driver of the logical EFI and the request immediately succeeds
01003188	"Set the ConnectionType of the FC HBA driver option. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the ConnectionType option of the FC HBA driver of the logical EFI and the request immediately succeeds
0100318A	"Enabled or disabled the MultiplePortID of the FC HBA driver option. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the MultiplePortID option of the FC HBA driver of the logical EFI and the request immediately succeeds
0100318C	"Set the DataRate of the FC HBA driver option. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the DataRate option of the FC HBA

ID	Message	Operation for which an audit log is collected
		driver of the logical EFI and the request immediately succeeds
0100318E	"Set the SpinupDelay of the FC HBA driver option. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the SpinUpDelay option of the FC HBA driver of the logical EFI and the request immediately succeeds
01003190	"Set the LoginDelayTime of the FC HBA driver option. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the LoginDelay option of the FC HBA driver of the logical EFI and the request immediately succeeds
01003192	"Enabled or disabled the PersistentBinding of the FC HBA driver option. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the PersistentBinding option of the FC HBA driver of the logical EFI and the request immediately succeeds
01003194	"Enabled or disabled the ForceDefaultParameter of the FC HBA driver option. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the ForceDefaultParameter option of the FC HBA driver of the logical EFI and the request immediately succeeds
01003196	"Enabled or disabled the SelectBootDevice of the FC HBA driver option. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the SelectBootDevice option of the FC HBA driver of the logical EFI and the request immediately succeeds
01003198	"Set the BootDeviceList entry of the FC HBA driver option. LPARXXX Slot#:XXX Port#:XXX Entry#:XXX WWN:XXX LU:XXX"	When HvmSh and so on is used to request change of a list of LU numbers and the storage WWNs of FC ports assigned to an LPAR and the request immediately succeeds
0100319A	"Enabled or disabled the LuidScanMode of the FC HBA driver option. LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the LuidScanMode option of the FC HBA driver of the logical EFI and the request immediately succeeds
0100319C	"Requested to initialize all options of the FC HBA driver. Accept:XXX LPARXXX Slot#:XXX Port#:XXX"	When HvmSh and so on is used to request clearing of the options of the FC HBA driver of the logical EFI and the request is accepted
0100319E	"Requested to enable or disable the BootFunction of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the bootfunc option of the FC HBA driver of the logical EFI and the request is accepted
010031A0	"Requested to set the ConnectionType of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the ConnectionType option of the FC HBA driver of the logical EFI and the request is accepted
010031A2	"Requested to enable or disable the MultiplePortID of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the MultiplePortID option of the FC HBA driver of the logical EFI and the request is accepted

ID	Message	Operation for which an audit log is collected
010031A4	"Requested to set the DataRate of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the DataRate option of the FC HBA driver of the logical EFI and the request is accepted
010031A6	"Requested to set the SpinupDelay of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the SpinUpDelay option of the FC HBA driver of the logical EFI and the request is accepted
010031A8	"Requested to set the LoginDelayTime of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the LoginDelay option of the FC HBA driver of the logical EFI and the request is accepted
010031AA	"Requested to enable or disable the PersistentBinding of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the PersistentBinding option of the FC HBA driver of the logical EFI and the request is accepted
010031AC	"Requested to enable or disable the ForceDefaultParameter of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the ForceDefaultParameter option of the FC HBA driver of the logical EFI and the request is accepted
010031AE	"Requested to enable or disable the SelectBootDevice of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the SelectBootDevice option of the FC HBA driver of the logical EFI and the request is accepted
010031B0	"Requested to set the BootDeviceList entry of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Entry#:XXX WWN:XXX LU:XXX"	When HvmSh and so on is used to request change of a list of LU numbers and the storage WWNs of FC ports assigned to an LPAR and the request is accepted
010031B2	"Requested to enable or disable the LuidScanMode of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the LuidScanMode option of the FC HBA driver of the logical EFI and the request is accepted
010031B4	"Pended to request to the ConnectionType of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the ConnectionType option of the FC HBA driver of the logical EFI and the request is accepted
010031B6	"Pended to request to set the MultiplePortID of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request change of the MultiplePortID option of the FC HBA driver of the logical EFI and the request is accepted
010031B8	"Pended to request to set the DataRate of the FC HBA driver option. Accept:XXX LPARXXX Slot#:XXX Port#:XXX Value:XXX"	When HvmSh and so on is used to request suspension of changing the DataRate option of the FC HBA driver of the logical EFI and the request is accepted
010031BA	"Requested to commit all pending requests to the FC HBA drivers. Accept:XXX"	When HvmSh and so on is used to request resuming of changing the options of the FC

ID	Message	Operation for which an audit log is collected
		HBA driver of the logical EFI that has been suspended and the request is accepted
010031BC	"Requested to cancel all pending requests to the FC HBA drivers. Accept:XXX"	When HvmSh and so on is used to request cancellation of changing the options of the FC HBA driver of the logical EFI that has been suspended and the request is accepted
010031BE	"Set the entry of the boot order for the LPAR. LPARXXX Entry#:XXX Type:PXE BDF:XXX MACaddress:XXX BootName:XXX DevPath:XXX"	When HvmSh and so on is used to request registration of a PXE boot at the BootOrder of the logical EFI and the request immediately succeeds
010031C0	"Set the entry of the boot order for the LPAR. LPARXXX Entry#:XXX Type:FC BDF:XXX LU:XXX WWN:XXX BootName:XXX DevPath:XXX"	When HvmSh and so on is used to request registration of a LU boot (FC SAN boot) at the BootOrder of the logical EFI and the request immediately succeeds
010031C2	"Set the entry of the boot order for the LPAR. LPARXXX Entry#:XXX Type:iSCSI BDF:XXX LU:XXX MACaddress:XXX BootName:XXX DevPath:XXX"	When HvmSh and so on is used to request registration of an iSCSI boot of the BootOrder of the logical EFI and the request immediately succeeds
010031C4	"Set the entry of the boot order for the LPAR. LPARXXX Entry#:XXX Type:KVM BDF:XXX BootName:XXX DevPath:XXX"	When HvmSh and so on is used to request registration of a KVM-CD/DVD boot of the BootOrder of the logical EFI and the request immediately succeeds
010031C6	"Set the entry of the boot order for the LPAR. LPARXXX Entry#:XXX Type:USB BDF:XXX Port#:XXX BootName:XXX DevPath:XXX"	When HvmSh and so on is used to request registration of an Front-CD/DVD boot of the BootOrder of the logical EFI and the request immediately succeeds
010031CA	"Requested to enable or disable the multiple queue scheduling. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the forcible multiple-queue scheduling setting and the request is accepted
010031CE	"Requested to set the IP address (IPv6) of CLI1. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of LP CLI1 IPv6 address and the request is accepted
010031D0	"Set the IP address (IPv6) of CLI1. Value:XXX"	When the LPAR manager screen is used to request change of LP CLI1 IPv6 address and the request succeeds
010031D1	"Failed to set the IP address (IPv6) of CLI1. Value:XXX"	When the LPAR manager screen is used to request change of LP CLI1 IPv6 address and the request fails
010031D2	"Requested to set the IP address (IPv6) of CLI2. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of LP CLI2 IPv6 address and the request is accepted
010031D4	"Set the IP address (IPv6) of CLI2. Value:XXX"	When the LPAR manager screen is used to request change of LP CLI2 IPv6 address and the request succeeds

ID	Message	Operation for which an audit log is collected
010031D5	"Failed to set the IP address (IPv6) of CLI2. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI2 IPv6 address and the request fails
010031D6	"Requested to set the IP address (IPv6) of CLI3. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of LP CLI3 IPv6 address and the request is accepted
010031D8	"Set the IP address (IPv6) of CLI3. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI3 IPv6 address and the request succeeds
010031D9	"Failed to set the IP address (IPv6) of CLI3. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI3 IPv6 address and the request fails
010031DA	"Requested to set the IP address (IPv6) of CLI4. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of LP CLI4 IPv6 address and the request is accepted
010031DC	"Set the IP address (IPv6) of CLI4. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI4 IPv6 address and the request succeeds
010031DD	"Failed to set the IP address (IPv6) of CLI4. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI4 IPv6 address and the request fails
010031DE	"Requested to set the IP address (IPv6) of CLI5. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of LP CLI5 IPv6 address and the request is accepted
010031E0	"Set the IP address (IPv6) of CLI5. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI5 IPv6 address and the request succeeds
010031E1	"Failed to set the IP address (IPv6) of CLI5. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI5 IPv6 address and the request fails
010031E2	"Requested to set the IP address (IPv6) of CLI6. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of LP CLI6 IPv6 address and the request is accepted
010031E4	"Set the IP address (IPv6) of CLI6. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI6 IPv6 address and the request succeeds
010031E5	"Failed to set the IP address (IPv6) of CLI6. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI6 IPv6 address and the request fails
010031E6	"Requested to set the IP address (IPv6) of CLI7. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of LP CLI7 IPv6 address and the request is accepted
010031E8	"Set the IP address (IPv6) of CLI7. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI7 IPv6 address and the request succeeds

ID	Message	Operation for which an audit log is collected
010031E9	"Failed to set the IP address (IPv6) of CLI7. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI7 IPv6 address and the request fails
010031EA	"Requested to set the IP address (IPv6) of CLI8. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of LP CLI8 IPv6 address and the request is accepted
010031EC	"Set the IP address (IPv6) of CLI8. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI8 IPv6 address and the request succeeds
010031ED	"Failed to set the IP address (IPv6) of CLI8. Value:xxx"	When the LPAR manager screen is used to request change of LP CLI8 IPv6 address and the request fails
010031EE	"Set the port dedicated mode of the PCI device. Slot#:xxx Port#:xxx Value:xxx"	When HvmSh and so on is used to request change of the port dedication setting for a PCI device and the request immediately succeeds
010031F0	"Requested to set the IP address of DNS server1. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of the IP address of DNS server1 and the request is accepted
010031F2	"Requested to set the IP address of DNS server2. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of the IP address of DNS server2 and the request is accepted
010031F4	"Requested to set the IP address of DNS server3. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of the IP address of DNS server3 and the request is accepted
010031F8	"Requested to enable or disable the regular diagnosis of the standby management path. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of the periodic diagnosis setting for the alternative port for the management path and the request is accepted
010031FA	"Enabled or disabled the HBA-core dedicated mode of the physical port. Slot#:xxx Port#:xxx Value:xxx"	When HvmSh and so on is used to request setting change of HBA-core dedicated mode for shared FC ports and the request immediately succeeds
010031FC	"Set the memory node(MN) number for the LPAR. LPARxxx Value:xxx"	"When HvmSh and so on is used to request change of a memory node, which is a NUMA node number, for an LPAR and the request immediately succeeds"
010031FE	"Set the memory node(MN) number for the LPAR. LPARxxx Value:xxx"	"When the LPAR manager screen is used to request change of a memory node, which is a NUMA node number, for an LPAR and the request succeeds"
010031FF	"Failed to set the memory node(MN) number for the LPAR. LPARxxx Value:xxx"	"When the LPAR manager screen is used to request change of a memory node, which is a NUMA node number, for an LPAR and the request fails"

ID	Message	Operation for which an audit log is collected
01003202	"Set the maximum aggregate throughput (Mbps) value of VF NIC. LPARXXX VNIC#:XXX Value:XXX"	When HvmSh and so on is used to request change of the transmission band restriction for an VF NIC (TXRATE) and the request immediately succeeds
01003204	"Set the maximum aggregate throughput (Mbps) value of VF NIC. LPARXXX VNIC#:XXX Value:XXX"	When the LPAR manager screen is used to request change of the transmission band restriction for an VF NIC (TXRATE) and the request succeeds
01003205	"Failed to set the maximum aggregate throughput (Mbps) value of VF NIC. LPARXXX VNIC#:XXX Value:XXX"	When the LPAR manager screen is used to request change of the transmission band restriction for an VF NIC (TXRATE) and the request fails
01003206	"Set the guest NUMA for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the guest NUMA setting and the request immediately succeeds
01003208	"Set the guest NUMA for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the guest NUMA setting and the request succeeds
01003209	"Failed to set the guest NUMA for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the guest NUMA setting and the request fails
0100320A	"Set the memory capacity allocated to the specified LPAR for each NUMA node number. LPARXXX Node#:XXX Value:XXX"	When HvmSh and so on is used to request change of memory size for an LPAR with its guest NUMA enabled and the request immediately succeeds
0100320C	"Set the memory capacity allocated to the specified LPAR for each NUMA node number. LPARXXX Node#:XXX Value:XXX"	When the LPAR manager screen is used to request change of memory size for an LPAR with its guest NUMA enabled and the request succeeds
0100320D	"Failed to set the memory capacity allocated to the specified LPAR for each NUMA node number. LPARXXX Node#:XXX Value:XXX"	When the LPAR manager screen is used to request change of memory size for an LPAR with its guest NUMA enabled and the request fails
0100320E	"Set the guest idle mode for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the GuestIdleMode setting for an LPAR and the request immediately succeeds
01003210	"Set the Low Latency option for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the LowLatency setting for an LPAR and the request immediately succeeds
01003212	"Set the EPT1GB option for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the EPT1GB setting for an LPAR and the request immediately succeeds
01003214	"Set the PRTE option for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the PRTE setting for an LPAR and the request immediately succeeds

ID	Message	Operation for which an audit log is collected
01003216	"Set the PRTE option for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the PRTE setting for an LPAR and the request succeeds
01003217	"Failed to set the PRTE option for the LPAR. LPARXXX Value:XXX"	When the LPAR manager screen is used to request change of the PRTE setting for an LPAR and the request fails
01003218	"Set the Physical NUMA Node Binding Mode for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the logical processor assignment setting for the guest NUMA for an LPAR and the request immediately succeeds
0100321A	"Set the number of logical processors for the LPAR NUMA node. LPARXXX Node#:XXX Value:XXX"	When HvmSh and so on is used to request change of the number of processors for NUMA nodes and the request immediately succeeds
0100321C	"Set the timeout for LPAR migration. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the timeout period for LPAR migration and the request immediately succeeds
0100321E	"Set the FC login timeout for LPAR migration. Value:XXX"	When HvmSh and so on is used to request change of the timeout period for logging into a storage system and the request immediately succeeds
01003224	"Set the FC login delay for LPAR migration. Value:XXX"	When HvmSh and so on is used to request change of the storage login delay time for LPAR migration and the request immediately succeeds
01003226	"Set the FC logout delay for LPAR migration. Value:XXX"	When HvmSh and so on is used to request change of the storage logout delay time for LPAR migration and the request immediately succeeds
01003234	"Requested to cancel the LPAR migration. Accept:XXX LPARXXX"	When HvmSh and so on is used to request suspension of the migration execution and the request is accepted
0100323A	"Requested to set the LP TimerCounter Base. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of a base value for calculating the Timer Counter Base timer counter (Timer Counter Base) and the request is accepted
0100323C	"Set the LP TimerCounter Base. Value:XXX"	When the LPAR manager screen is used to request change of a base value for calculating the Timer Counter Base timer counter (Timer Counter Base) and the request succeeds
0100323D	"Failed to set the LP TimerCounter Base. Value:XXX"	When the LPAR manager screen is used to request change of a base value for calculating the Timer Counter Base timer counter (Timer Counter Base) and the request fails

ID	Message	Operation for which an audit log is collected
01003240	"Requested to set the security strength with HvmSh commands. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the encrypted communication strength for LPAR manager and HvmSh and the request is accepted
01003242	"Requested to enable or disable the security strength for communication with BSM. Accept:XXX Value:XXX"	When HvmSh and so on is used to request setting change of whether communication with LPAR manager and BSM is enabled or disabled and the request is accepted
01003244	"Requested to set the security strength for communication with HCSM. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the encrypted communication strength for LPAR manager and BSM and the request is accepted
01003246	"Requested to enable or disable the security strength through the LPAR manager Web system. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of whether http communication for LPAR managers is enabled or disabled and the request is accepted
01003248	"Requested to set the security strength for communication with LDAP servers. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the encrypted communication strength for LPAR manager and LDAP server and the request is accepted
0100324A	"Requested to enable or disable the certificate verification for communication with HCSM. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the certificate verification setting for the encrypted communication between LPAR manager and HCSM and the request is accepted
0100324C	"Requested to enable or disable the certificate verification for communication with the LDAP servers. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the certificate verification setting for the encrypted communication between LPAR manager and HCSM and the request is accepted
0100324E	"Requested to register the signed certificate of the LPAR manager. Accept:XXX IssuerCN:XXX SN:XXX"	When HvmSh and so on is used to request import of the server certificate for LPAR manager signed by the certificate authority and the request is accepted
01003250	"Requested to register the certificate of another server. Accept:XXX IssuerCN:XXX SN:XXX"	When HvmSh and so on is used to request registration of the certificate for a server with which LPAR manager communicates and the request is accepted
01003252	"Requested to generate the self-signed certificate. Accept:XXX IssuerCN:XXX"	When HvmSh and so on is used to request creation of an LPAR manager server certificate and the request is accepted
01003254	"Generated the certificate signing request (CSR) ."	When HvmSh and so on is used to request creation of a CSR for LPAR manager and the request immediately succeeds
01003256	"Requested to remove the certificate. Accept:XXX Certificate#:XXX IssuerCN:XXX SN:XXX"	When HvmSh and so on is used to request deletion of a server certificate for a server with which LPAR manager communicates and the request is accepted

ID	Message	Operation for which an audit log is collected
01003258	"Requested to enable or disable the user authentication of LP CLI. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of user authentication with an LPAR manager CLI and the request is accepted
0100325A	"Requested to enable or disable the user authentication of the virtual COM console. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of user authentication of a virtual COM console and the request is accepted
0100325C	"Enabled or disabled the user authentication of LP CLI. Value:XXX"	When the LPAR manager screen is used to request change of user authentication with an LPAR manager CLI and the request succeeds
0100325D	"Failed to enable or disable the user authentication of LP CLI. Value:XXX"	When the LPAR manager screen is used to request change of user authentication with an LPAR manager CLI and the request fails
0100325E	"Enabled or disabled the user authentication of the virtual COM console. Value:XXX"	When the LPAR manager screen is used to request change of user authentication of a virtual COM console and the request succeeds
0100325F	"Failed to enable or disable the user authentication of the virtual COM console. Value:XXX"	When the LPAR manager screen is used to request change of user authentication of a virtual COM console and the request fails
01003260	"Requested to add the local user. Accept:XXX User:XXX"	When HvmSh and so on is used to request addition of a local user and the request is accepted
01003262	"Added the local user. User:XXX"	When the LPAR manager screen is used to request addition of a local user and the request succeeds
01003263	"Failed to add the local user. User:XXX"	When the LPAR manager screen is used to request addition of a local user and the request fails
01003264	"Requested to remove the local user. Accept:XXX User:XXX"	When HvmSh and so on is used to request deletion of a local user and the request is accepted
01003266	"Removed the local user. User:XXX"	When the LPAR manager screen is used to request deletion of a local user and the request succeeds
01003267	"Failed to remove the local user. User:XXX"	When the LPAR manager screen is used to request deletion of a local user and the request fails
01003268	"Requested to change the password of the local user. Accept:XXX User:XXX"	When HvmSh and so on is used to request password change of a local user and the request is accepted
0100326A	"Changed the password of the local user. User:XXX"	When the LPAR manager screen is used to request password change of a local user and the request succeeds
0100326B	"Failed to change the password of the local user. User:XXX"	When the LPAR manager screen is used to request password change of a local user and the request fails

ID	Message	Operation for which an audit log is collected
0100326C	"Requested to set the login time valid for LP CLI of the user. Accept:XXX User:XXX Value:XXX"	When HvmSh and so on is used to request change of the valid login time by using HvmSh for a local user and the request is accepted
0100326E	"Requested to generate SSH host key used for the virtual COM console. Accept:XXX"	When HvmSh and so on is used to request creation of a host key for SSH connection of a virtual COM console and the request is accepted
01003270	"Generated SSH host key used for the virtual COM console."	When the LPAR manager screen is used to request creation of a host key for SSH connection of a virtual COM console and the request succeeds
01003271	"Failed to generate SSH host key used for the virtual COM console."	When the LPAR manager screen is used to request creation of a host key for SSH connection of a virtual COM console and the request fails
01003272	"Requested to set the virtual COM console connection method. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the connection method to a virtual COM console (connection type) and the request is accepted
01003274	"Set the virtual COM console connection method. Value:XXX"	When the LPAR manager screen is used to request change of the connection method to a virtual COM console (connection type) and the request succeeds
01003275	"Failed to set the virtual COM console connection method. Value:XXX"	When the LPAR manager screen is used to request change of the connection method to a virtual COM console (connection type) and the request fails
01003276	"Requested to set the certificate type for LP Web system. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of a server certificate for LP Web system and the request is accepted
01003278	"Requested to set the user authentication method. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the user authentication method (the method of accessing external authentication servers) and the request is accepted
0100327A	"Requested to set the login time valid for LP CLI of externally-authenticated user. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the valid login time by using HvmSh for a local user authenticated with an external server and the request is accepted
0100327C	"Requested to set name of LDAP server1. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the name of LDAP server1 and the request is accepted
0100327E	"Requested to set name of LDAP server2. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the name of LDAP server2 and the request is accepted

ID	Message	Operation for which an audit log is collected
01003280	"Requested to set name of LDAP server3. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the name of LDAP server3 and the request is accepted
01003282	"Requested to set the login ID attribution of LDAP authentication. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the login ID attribute for LDAP authentication and the request is accepted
01003284	"Requested to set the base DN for LDAP authentication. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of Base DN for LDAP authentication and the request is accepted
01003286	"Requested to set the port number of the LDAP servers. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of a port number of an LDAP server and the request is accepted
01003288	"Requested to enable or disable the anonymous bind for LDAP authentication. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the anonymous bind for LDAP authentication and the request is accepted
0100328A	"Requested to set the common role for the LDAP authentication users. Accept:XXX RoleXXX"	When HvmSh and so on is used to request change of a role for all users authenticated with an LDAP server and the request is accepted
0100328C	"Requested to set the bind DN for LDAP authentication. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of Bind DN for LDAP authentication and the request is accepted
0100328E	"Requested to change the bind the password for LDAP authentication. Accept:XXX"	When HvmSh and so on is used to request change of Bind password for LDAP authentication and the request is accepted
01003290	"Requested to set name of syslog server1. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the name of syslog server1 and the request is accepted
01003292	"Requested to set name of syslog server2. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the name of syslog server2 and the request is accepted
01003294	"Requested to set port number of the syslog servers. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of a port number of a syslog server and the request is accepted
01003296	"Requested to set the protocol used to communicate with the syslog servers. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of a protocol for communication with syslog servers and the request is accepted
01003298	"Requested to enable or disable the certificate verification for communication with syslog servers. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the certificate verification setting for communication with syslog servers and the request is accepted
0100329A	"Requested to set name of RADIUS server1. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the name of RADIUS server1 and the request is accepted

ID	Message	Operation for which an audit log is collected
0100329C	"Requested to set name of RADIUS server2. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the name of RADIUS server2 and the request is accepted
0100329E	"Requested to set name of RADIUS server3. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the name of RADIUS server3 and the request is accepted
010032A0	"Requested to set the shared secret of RADIUS server1. Accept:XXX"	When HvmSh and so on is used to request change of the shared key of RADIUS server1 and the request is accepted
010032A2	"Requested to set the shared secret of RADIUS server2. Accept:XXX"	When HvmSh and so on is used to request change of the shared key of RADIUS server2 and the request is accepted
010032A4	"Requested to set the shared secret of RADIUS server3. Accept:XXX"	When HvmSh and so on is used to request change of the shared key of RADIUS server3 and the request is accepted
010032A6	"Requested to set the port number of RADIUS server1. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the port number of RADIUS server1 and the request is accepted
010032A8	"Requested to set the port number of RADIUS server2. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the port number of RADIUS server2 and the request is accepted
010032AA	"Requested to set the port number of RADIUS server3. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the port number of RADIUS server3 and the request is accepted
010032AC	"Requested to set the time of retries of authentication by RADIUS server1. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the times of attempts in RADIUS server1 and the request is accepted
010032AE	"Requested to set the time of retries of authentication by RADIUS server2. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the times of attempts in RADIUS server2 and the request is accepted
010032B0	"Requested to set the time of retries of authentication by RADIUS server3. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the times of attempts in RADIUS server3 and the request is accepted
010032B2	"Requested to set the timeout period for accessing RADIUS server1. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of a timeout period of RADIUS server1 and the request is accepted
010032B4	"Requested to set the timeout period for accessing RADIUS server2. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of a timeout period of RADIUS server2 and the request is accepted
010032B6	"Requested to set the timeout period for accessing RADIUS server3. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of a timeout period of RADIUS server3 and the request is accepted
010032B8	"Requested to set the authentication method of RADIUS server1. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the authentication method of RADIUS server1 and the request is accepted

ID	Message	Operation for which an audit log is collected
010032BA	"Requested to set the authentication method of RADIUS server2. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the authentication method of RADIUS server2 and the request is accepted
010032BC	"Requested to set the authentication method of RADIUS server3. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the authentication method of RADIUS server3 and the request is accepted
010032BE	"Requested to set the common role for the RADIUS authentication users. Accept:XXX RoleXXX"	When HvmSh and so on is used to request change of a role for all users authenticated by a RADIUS server and the request is accepted
010032C0	"Requested to set the security permission for the user-defined role. Accept:XXX RoleXXX Value:XXX"	When HvmSh and so on is used to request change of a security permission for a users-defined role and the request is accepted
010032C2	"Requested to assign the role to the local user. Accept:XXX User:XXX RoleXXX"	When HvmSh and so on is used to request change of a role for local users and the request is accepted
010032C4	"Requested to assign the role of ManagementModuleUser. Accept:XXX RoleXXX"	When HvmSh and so on is used to request change of a role for the management module user and the request is accepted
010032D4	"Completed the LPAR migration. Position:XXX Method:XXX SrcLP:XXX SrcLPAR#:XXX LPAR_Name:XXX DstLP:XXX DstLPAR#:XXX"	When a migration execution succeeds
010032D8	"Completed the LPAR migration recovery. LPARXXX"	When a recovery operation of LPAR migration succeeds
010032DA	"Applied all pending changes to the LPAR manager."	"When the LPAR manager screen is used to request reflection of change with Update PCI Dev Schd or Update System Config and the request succeeds"
010032DB	"Failed to apply all pending changes to the LPAR manager."	"When the LPAR manager screen is used to request reflection of change with Update PCI Dev Schd or Update System Config and the request fails"
010032DC	"Canceled all pending changes to the LPAR manager."	When the LPAR manager screen is used to request cancel of change with Update PCI Dev Schd or Update System Config and the request succeeds
010032DD	"Failed to cancel all pending changes to the LPAR manager."	When the LPAR manager screen is used to request cancel of change with Update PCI Dev Schd or Update System Config and the request fails
010032DE	"Requested to set the L3_CBM for the LPAR. Accept:XXX LPARXXX Value:XXX"	When HvmSh and so on is used to request change of L3_CBM for an LPAR and the request is accepted

ID	Message	Operation for which an audit log is collected
010032E4	"Requested to set the logging policy (targets to log) of the LPAR manager. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the policy of audit log collection and the request is accepted
010032EC	"Requested to set the password expiration period (date) for local users. Accept:XXX Value:XXX"	When HvmSh and so on is used to request change of the password validity period for local users and the request is accepted
010032EE	"Set the password expiration period (date) for local users. Value:XXX"	When the LPAR manager screen is used to request change of the password validity period for local users and the request succeeds
010032EF	"Failed to set the password expiration period (date) for local users. Value:XXX"	When the LPAR manager screen is used to request change of the password validity period for local users and the request fails
010032F2	"Set the scheduling data for the LPAR. LPARXXX"	When HvmSh and so on is used to request setting of the scheduling data for an LPAR and the request succeeds
010032F3	"Failed to set the scheduling data for the LPAR. LPARXXX"	"When HvmSh and so on is used to request setting of the scheduling data for an LPAR and the request fails "
010032F4	"Set the threshold time for management path failover owing to link-down of the active port. Value:XXX"	When HvmSh and so on is used to request change of port-switching time in link-down of the management path and the request immediately succeeds
010032FA	"Enabled or disabled the option of the KeepConfig. Value:XXX"	When HvmSh and so on is used to request change of the KeepConfig option and the request immediately succeeds
010032FC	"Set the interrupt moderation type for all VNICs. Value:XXX"	When HvmSh and so on is used to request change of the interrupt moderation type for all VNICs and the request immediately succeeds
010032FE	"Set the host parameter for interrupt moderation for all VNICs. Value:XXX"	When HvmSh and so on is used to request change of the host parameter for interrupt moderation for all VNICs and the request immediately succeeds
01003300	"Set the HPET allocation for the LPAR. LPARXXX Value:XXX"	When HvmSh and so on is used to request change of the HPET allocation for the LPAR and the request immediately succeeds
01003306	"Set the maximum CPU resource usage of SYS2. Value:XXX"	When the LPAR manager screen is used to request change of the maximum number of processors for SYS2 and the request succeeds.
01003307	"Failed to set the maximum CPU resource usage of SYS2. Value:XXX"	When the LPAR manager screen is used to request change of the maximum number of processors for SYS2 and the request fails.
01003308	"Enabled or disabled the LPAR manager dump overwrite inhibition. Value:XXX"	When HvmSh and so on is used to request change of the LPAR manager dump overwrite

ID	Message	Operation for which an audit log is collected
		inhibition setting and the request immediately succeeds.
0100330A	"Set the threshold of the LPAR manager dump overwrite inhibition. Value:xxx"	When HvmSh and so on is used to request change of the LPAR manager dump overwrite inhibition time and the request immediately succeeds.
01003312	"Enabled or disabled the guest IBRS/IBPB. LPARxxx Value:xxx"	When HvmSh and so on is used to request change of the guest IBRS/IBPB and the request immediately succeeds.
01003314	"Enabled or disabled the default value for guest IBRS/IBPB. Value:xxx"	When HvmSh and so on is used to request change of the default value for guest IBRS/IBPB and the request immediately succeeds.
01003316	"Enabled or disabled the guest PCID. LPARxxx Value:xxx"	When HvmSh and so on is used to request change of the guest PCID and the request immediately succeeds.
01003318	"Enabled or disabled the default value for guest PCID. Value:xxx"	When HvmSh and so on is used to request change of the default value for guest PCID and the request immediately succeeds.
01003320	"Enabled or disabled the guest SSBD. LPARxxx Value:xxx"	When HvmSh and so on is used to request change of the guest SSBD and the request immediately succeeds.
01003322	"Enabled or disabled the default value for guest SSBD. Value:xxx"	When HvmSh and so on is used to request change of the default value for guest SSBD and the request immediately succeeds.
01003324	"Requested to enable or disable the core scheduling. Accept:xxx Value:xxx"	When HvmSh and so on is used to request change of the core scheduling setting and the request is accepted.
01003328	"Enabled or disabled the guest MDClear. LPARxxx Value:xxx"	When HvmSh and so on is used to request change of the guest MDClear and the request immediately succeeds.
0100332A	"Enabled or disabled the default value for guest MDClear. Value:xxx"	When HvmSh and so on is used to request change of the default value for guest MDClear and the request immediately succeeds.
01013000	"Completed the request. Accept:xxx"	When a user performs an operation for setting Audit event type to ConfigurationAccess asynchronously and the operation succeeds
01013001	"Failed to complete the request. Accept:xxx"	When a user performs an operation for setting Audit event type to ConfigurationAccess asynchronously and the operation fails

Table 11-10 List of audit log messages (Maintenance)

ID	Message	Operation for which an audit log is collected
01008000	"Requested to inject an NMI to the LPAR to start retrieval the guest OS dump. Accept:XXX LPARXXX"	When HvmSh and so on is used to request issuing of NMI interrupt for an LPAR to collect the memory dump of the guest OS. and the request is accepted
01008002	"Injected an NMI to the LPAR to start retrieval guest OS dump. LPARXXX"	When the LPAR manager screen is used to request issuing of NMI interrupt for an LPAR to collect the memory dump of the guest OS. and the request succeeds
01008003	"Failed to inject an NMI to the LPAR to start retrieval guest OS dump. LPARXXX"	When the LPAR manager screen is used to request issuing of NMI interrupt for an LPAR to collect the memory dump of the guest OS. and the request fails
01008008	"Requested to switch the ports for the management path. Accept:XXX NextActiveManagementPath:XXX"	When HvmSh and so on is used to request activation of the specified management path port and the request is accepted
01018000	"Completed the request. Accept:XXX"	When a user performs an operation for setting Audit event type to Maintenance asynchronously and the operation succeeds
01018001	"Failed to complete the request. Accept:XXX"	When a user performs an operation for setting Audit event type to Maintenance asynchronously and the operation fails

"HvmSh and so on" in the above messages shows the web console, HCSM, HVM Navigator, and HvmSh.

HCSM alert messages

This chapter describes the HCSM alert message format and messages:

HCSM alert message format

The following format is used in this message list:

- ID
Indicates the message ID.
- Level
Indicates the message level. (information, warning, or failure level)
- Message
Indicates the contents of the message. X and Y in the message indicate characters.

List of HCSM alert messages

The following tables show HCSM alert messages.

Table 11-11 List of HCSM alert messages (information level)

ID	Message	Description
0xFC00	LP was completely started.	Indicates that LPAR manager completely started.
0xFC01	LP started shutting down.	Indicates that LPAR manager started shutting down.
0xFC02	The LP configuration was saved. (RC=<X>)	Indicates that the LPAR manager configuration was saved. <X> indicates the trigger code for saving.
0xFC03	The format of the LP configuration was converted. (old ver. = X, new ver. = Y)	Indicates that the format of the LPAR manager configuration was converted. X indicates the version of the configuration format before the conversion. Y indicates the version of the configuration format after the conversion.
0xFC70	LPAR X was activated.	Indicates that the LPAR was activated. X indicates the LPAR number.
0xFC71	LPAR X will be activated due to a scheduled power-on request.	Indicates that scheduled activation for the LPAR starts. X indicates the LPAR number.
0xFC72	LPAR X was deactivated.	Indicates that the LPAR was deactivated. X indicates the LPAR number.
0xFC73	LPAR X will start system shutdown because of a scheduled power-off request.	Indicates that scheduled deactivation for the LPAR starts. X indicates the LPAR number.
0xFC74	LPAR migration starts on the migration-source LP. (SIP=<X>,DIP=<Y>)	Indicates that LPAR migration starts on the migration-source LPAR manager. X indicates the IP address for the migration-source LPAR manager. Y indicates the IP address for the migration-destination LPAR manager.
0xFC75	LPAR migration will start on the migration-destination LP. (SIP=<X>,DIP=<Y>)	Indicates that LPAR migration will start on the migration-destination LPAR manager. X indicates the IP address for the migration-source LPAR manager. Y indicates the IP address for the migration-destination LPAR manager.
0xFC76	LPAR migration on the migration-source LP successfully ended. (SIP=<X>,DIP=<Y>)	Indicates that LPAR migration on the migration-source LPAR manager successfully ended. X indicates the IP address for the migration-source LPAR manager. Y indicates the IP address for the migration-destination LPAR manager.
0xFC77	LPAR migration on the migration-destination LP successfully ended. (SIP=<X>,DIP=<Y>)	Indicates that LPAR migration on the migration-destination LPAR manager successfully ended. X indicates the IP address for the migration-source LPAR manager. Y indicates the IP address for the migration-destination LPAR manager.
0xFC78	The configuration for LPAR X changed.	Indicates that the information of the LPAR was updated. X indicates the LPAR number.

ID	Message	Description
0xFC79	LPAR X was added.	Indicates that the LPAR was added. X indicates the LPAR number.
0xFC7A	LPAR X was deleted.	Indicates that the LPAR was deleted. X indicates the LPAR number.

Table 11-12 List of HCSM alert messages (warning level)

ID	Message	Description	Recovery procedure
0xFCA0	Activation of LPAR X failed. (RC=<Y>)	Indicates that activation of the LPAR failed. X indicates the LPAR number. Y indicates the error reason code.	Check whether the CPU and memory are sufficiently available for LPAR activation.
0xFCA1	Deactivation of LPAR X failed. (RC=<Y>)	Indicates that deactivation of the LPAR failed. X indicates the LPAR number. Y indicates the error reason code.	Contact your reseller or maintenance personnel.
0xFCA2	For LPAR X, a watchdog timer timeout was detected. (RC=<Y>)	Indicates that a watchdog timer timeout for the LPAR was detected. X indicates the LPAR number. Y indicates the error reason code.	Contact your reseller or maintenance personnel.
0xFCA3	LPAR migration on the migration-source LP failed. (SIP=<X>,DIP=<Y>,RC=<Z>)	Indicates that LPAR migration on the migration-source LPAR manager failed. X indicates the IP address for the migration-source LPAR manager. Y indicates the IP address for the migration-destination LPAR manager. Z indicates the error reason code.	Take appropriate action according to the HCSM messages shown when the LPAR migration task is being executed.
0xFCA4	LPAR migration on the migration-destination LP failed. (SIP=<X>,DIP=<Y>,RC=<Z>)	Indicates that LPAR migration on the migration-destination LPAR manager failed. X indicates the IP address for the migration-source LPAR manager. Y indicates the IP address for the migration-destination LPAR manager. Z indicates the error reason code.	Take appropriate action according to the HCSM messages shown when the LPAR migration task is being executed.

Software License Information

This appendix provides software license information.

☐ [Software License Information](#)

Software License Information

Embedded software to the LPAR manager is constituted by the independent multiple software.

The software are developed by Hitachi, Ltd or third party, and they also have Copyright© of the software. The software which is developed by Hitachi has copyrights, properties and intellectual properties. And the documents for the software also have copyrights, properties and intellectual properties. The software and the documents are protected by copyrighted law and other relevant laws.

LPAR manager is using the open software which was developed by third party according to each software license agreement below.

The URL links below are accurate as of the date this manual was issued. Note that these links might change.

Table A-1 Software License Agreement List

Software	Related software use agreement contract
ACPI Component Architecture	<p>ACPICA License</p> <p>See the following contents.</p> <p>INTEL MAKES NO WARRANTY OF ANY KIND REGARDING ANY SOFTWARE PROVIDED HERE. ANY SOFTWARE ORIGINATING FROM INTEL OR DERIVED FROM INTEL SOFTWARE IS PROVIDED "AS IS," AND INTEL WILL NOT PROVIDE ANY SUPPORT, ASSISTANCE, INSTALLATION, TRAINING OR OTHER SERVICES. INTEL WILL NOT PROVIDE ANY UPDATES, ENHANCEMENTS OR EXTENSIONS. INTEL SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE.</p> <p>IN NO EVENT SHALL INTEL HAVE ANY LIABILITY TO LICENSEE, ITS LICENSEES OR ANY OTHER THIRD PARTY, FOR ANY LOST PROFITS, LOST DATA, LOSS OF USE OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, UNDER ANY CAUSE OF ACTION OR THEORY OF LIABILITY, AND IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.</p> <p>Licensee shall not export, either directly or indirectly, any of this software or system incorporating such software without first obtaining any required license or other approval from the U. S. Department of Commerce or any other agency or department of the United States Government. In the event Licensee exports any such software from the United States or re-exports any such software from a foreign destination, Licensee shall ensure that the distribution and export/re-export of the software is in compliance with all laws, regulations, orders, or other restrictions of the U.S. Export Administration Regulations. Licensee agrees that neither it nor any of its subsidiaries will export/re-export any technical data, process, software, or service, directly or indirectly, to any country for which the United States government or any agency thereof requires an export license, other governmental approval, or letter of assurance, without first obtaining such license, approval or letter.</p>
Broadcom Tigon3 ethernet driver	<p>GNU General Public License version 2</p> <p>Visit the following URL.</p> <p>http://www.gnu.org/licenses/gpl.html</p>

Software	Related software use agreement contract
bzip2	BSD License Visit the following URL. http://www.opensource.org/licenses/bsd-license.php
Emulex Driver for Linux	GNU General Public License version 2 Visit the following URL. http://www.gnu.org/licenses/gpl.html
glibc	GNU Lesser General Public License 2.1 Visit the following URL. http://www.gnu.org/licenses/lgpl-2.1.html
Intel(R) Gigabit Ethernet Linux driver	GNU General Public License version 2 Visit the following URL. http://www.gnu.org/licenses/gpl.html
Linux Kernel	GNU General Public License version 2 Visit the following URL. http://www.gnu.org/licenses/gpl-2.0.html
ser2net	GNU General Public License version 2 Visit the following URL. http://www.gnu.org/licenses/gpl-2.0.html
binutils	GNU General Public License version 2 Visit the following URL. http://www.gnu.org/licenses/gpl-2.0.html
openssl	OpenSSL License Visit the following URL. http://www.openssl.org/source/license.html
tianocore EFI	FAT32 License See the following contents. BSD License - Modified for the FAT32 Driver by Intel Copyright (c) 2004, Intel Corporation All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Intel nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR

Software	Related software use agreement contract
	<p>CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.</p> <p>Additional terms: In addition to the forgoing, redistribution and use of the code is conditioned upon the FAT 32 File System Driver and all derivative works thereof being used for and designed only to read and/or write to a file system that is directly managed by an Extensible Firmware Interface (EFI) implementation or by an emulator of an EFI implementation. TianoCore Contribution Agreement</p> <p>See the following contents.</p> <p>=====</p> <p>= TianoCore Contribution Agreement 1.0 =</p> <p>=====</p> <p>INTEL CORPORATION ("INTEL") MAKES AVAILABLE SOFTWARE, DOCUMENTATION, INFORMATION AND/OR OTHER MATERIALS FOR USE IN THE TIANOCORE OPEN SOURCE PROJECT (COLLECTIVELY "CONTENT"). USE OF THE CONTENT IS GOVERNED BY THE TERMS AND CONDITIONS OF THIS AGREEMENT BETWEEN YOU AND INTEL AND/OR THE TERMS AND CONDITIONS OF LICENSE AGREEMENTS OR NOTICES INDICATED OR REFERENCED BELOW. BY USING THE CONTENT, YOU AGREE THAT YOUR USE OF THE CONTENT IS GOVERNED BY THIS AGREEMENT AND/OR THE TERMS AND CONDITIONS OF ANY APPLICABLE LICENSE AGREEMENTS OR NOTICES INDICATED OR REFERENCED BELOW. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THE TERMS AND CONDITIONS OF ANY APPLICABLE LICENSE AGREEMENTS OR NOTICES INDICATED OR REFERENCED BELOW, THEN YOU MAY NOT USE THE CONTENT.</p> <p>Unless otherwise indicated, all Content made available on the TianoCore site is provided to you under the terms and conditions of the BSD License ("BSD"). A copy of the BSD License is available at http://opensource.org/licenses/bsd-license.php or when applicable, in the associated License.txt file. Certain other content may be made available under other licenses as indicated in or with such Content. (For example, in a License.txt file.) You accept and agree to the following terms and conditions for Your present and future Contributions submitted to TianoCore site. Except for the license granted to Intel hereunder, You reserve all right, title, and interest in and to Your Contributions.</p> <p>== SECTION 1: Definitions ==</p> <p>* "You" or "Contributor" shall mean the copyright owner or legal entity authorized by the copyright owner that is making a Contribution hereunder. All other entities that control, are controlled by, or are under common control with that entity are considered to be a single Contributor. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. * "Contribution" shall mean any original work of authorship, including any modifications or additions to an existing work, that is intentionally submitted by You to the TianoCore site for inclusion in, or documentation of, any of the Content. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the TianoCore site or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the TianoCore site for the purpose of discussing and improving the Content, but excluding communication that is conspicuously marked or otherwise designated in writing by You as "Not a Contribution."</p> <p>== SECTION 2: License for Contributions ==</p>

Software	Related software use agreement contract
	<p>* Contributor hereby agrees that redistribution and use of the Contribution in source and binary forms, with or without modification, are permitted provided that the following conditions are met:</p> <p>** Redistributions of source code must retain the Contributor's copyright notice, this list of conditions and the following disclaimer.</p> <p>** Redistributions in binary form must reproduce the Contributor's copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.</p> <p>* Disclaimer. None of the names of Contributor, Intel, or the names of their respective contributors may be used to endorse or promote products derived from this software without specific prior written permission. * Contributor grants a license (with the right to sublicense) under claims of Contributor's patents that Contributor can license that are infringed by the Contribution (as delivered by Contributor) to make, use, distribute, sell, offer for sale, and import the Contribution and derivative works thereof solely to the minimum extent necessary for licensee to exercise the granted copyright license; this patent license applies solely to those portions of the Contribution that are unmodified. No hardware per se is licensed.</p> <p>* EXCEPT AS EXPRESSLY SET FORTH IN SECTION 3 BELOW, THE CONTRIBUTION IS PROVIDED BY THE CONTRIBUTOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE CONTRIBUTION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.</p> <p>== SECTION 3: Representations ==</p> <p>* You represent that You are legally entitled to grant the above license. If your employer(s) has rights to intellectual property that You create that includes Your Contributions, You represent that You have received permission to make Contributions on behalf of that employer, that Your employer has waived such rights for Your Contributions.</p> <p>* You represent that each of Your Contributions is Your original creation (see Section 4 for submissions on behalf of others). You represent that Your Contribution submissions include complete details of any third-party license or other restriction (including, but not limited to, related patents and trademarks) of which You are personally aware and which are associated with any part of Your Contributions.</p> <p>== SECTION 4: Third Party Contributions ==</p> <p>* Should You wish to submit work that is not Your original creation, You may submit it to TianoCore site separately from any Contribution, identifying the complete details of its source and of any license or other restriction (including, but not limited to, related patents, trademarks, and license agreements) of which You are personally aware, and conspicuously marking the work as "Submitted on behalf of a third-party: [named here]".</p> <p>== SECTION 5: Miscellaneous ==</p> <p>* Applicable Laws. Any claims arising under or relating to this Agreement shall be governed by the internal substantive laws of the State of Delaware or federal courts located in Delaware, without regard to principles of conflict of laws.</p> <p>* Language. This Agreement is in the English language only, which language shall be controlling in all respects, and all versions of this Agreement in any other language shall be for accommodation only and shall not be binding. All communications and notices</p>

Software	Related software use agreement contract
	<p>made or given pursuant to this Agreement, and all documentation and support to be provided, unless otherwise noted, shall be in the English language.</p> <p>BSD License Visit the following URL. http://opensource.org/licenses/bsd-license.php</p> <p>Eclipse License Visit the following URL. http://opensource.org/licenses/EPL-1.0</p>
zlib	<p>zlib license Visit the following URL. http://www.zlib.net/zlib_license.html</p>
Others: software contained in Redhat Enterprise Linux 6 server	<p>GNU General Public License version2, and license agreement of each software Visit the following URL. http://www.gnu.org/licenses/gpl.html</p>

Functionality Supported by LPAR manager

This appendix describes PCI devices, their functionality, and the SR-IOV functionality supported by LPAR manager.

- ☐ [List of PCI devices supported by LPAR manager](#)
- ☐ [List of functionality supported by LPAR manager](#)
- ☐ [SR-IOV functionality supported by LPAR manager](#)
- ☐ [Dedicated port functionality supported by LPAR manager](#)
- ☐ [LPAR manager licenses](#)
- ☐ [Differences in supported items depending on the guest OSs](#)

List of PCI devices supported by LPAR manager

The following table describes PCI devices supported by LPAR manager and whether they are supported for each logical partition type.

Table B-1 PCI devices supported by LPAR manager

PCI device				Support specification		
				Dedicated	Shared	Exclusively shared
NIC	Onboard LAN	Onboard LAN ^{1, 2, 3, 4}		Y	Y	N
	Mezzanine card	Broadcom 1Gb 4-port LAN mezzanine card ³		N	Y	N
	I/O adapter	1000BASE-T 4-port LAN adapter ³		Y ¹⁰	Y	N
		10GBASE-SR 2-port LAN adapter		Y	Y ⁵	N
		10GBASE-T 2-port LAN adapter ⁶		Y	N	N
		Emulex 10Gb 2-port converged network adapter ^{1, 3, 4, 7}		Y	Y	N
FC	I/O adapter	Hitachi 8Gb 2-port fibre channel adapter		Y	Y	N
		Hitachi 16Gb 2-port fibre channel adapter ^{8, 9}		Y	Y	N
Flash drive	I/O adapter	HGST 1.1TB PCIe MLC Flash drive adapter (FlashMAX3) ⁸		Y	N	N
		HGST 2.2TB PCIe MLC Flash drive adapter (FlashMAX3) ⁸		Y	N	N
USB device connected to front USB port		CD/DVD drive	CB 520X B1/B2/B 3	Y	N	N
			CB 520H B3/B4	N	N	Y
		USB memory	CB 520X B1/B2/B 3	Y	N	N
			CB 520H B3/B4	N	N	Y
		Keyboard		N	N	N

PCI device		Support specification		
		Dedicated	Shared	Exclusively shared
	Mouse	N	N	N
Device connected via KVM connector	CD/DVD drive	N	N	Y
	USB memory	N	N	Y
	Keyboard	N	N	Y
	Mouse	N	N	Y
Remote console	CD/DVD drive	N	N	Y
	USB memory	N	N	Y
	Keyboard	N	N	Y
	Mouse	N	N	Y
<p>Legend:</p> <p>Y: Can be used</p> <p>N: Cannot be used</p> <p>Notes:</p> <ol style="list-style-type: none"> Multichannel is not supported. Set MultiChannel Support to Disabled. For details about how to configure this setting, see the manual <i>Hitachi Compute Blade Emulex Adapter User's Guide for Hardware</i>. Note, however, that you cannot change the setting in LP mode. If necessary, change it in Basic mode. Modes other than NIC and FCoE are not supported. Set Personality to NIC or FCoE. For details about how to configure this setting, see the manual <i>Hitachi Compute Blade Emulex Adapter User's Guide for Hardware</i>. Note, however, that you cannot change the setting in LP mode. If necessary, change it in Basic mode. In LPARs to which a shared NIC and virtual NIC are assigned, the NIC is recognized as a 1-GB LAN (Intel 82576 specification) on a guest OS. In LPARs to which a shared NIC and virtual NIC are assigned, the total throughput is about 3 Gbps per LPAR manager. Supported by LPAR manager firmware versions 02-40 or later. Supported by LPAR manager firmware versions 02-25 or later. iSCSI mode and FCoE mode are not supported. Make sure that you use the device in NIC mode. Set Personality to NIC. For details about how to configure this setting, see the manual <i>Hitachi Compute Blade Emulex Adapter User's Guide for Hardware</i>. Note, however, that you cannot change the setting in LP mode. If necessary, change it in Basic mode. Supported by LPAR manager firmware versions 02-20 or later. For details about the supported fibre channel adapter versions, see the manual <i>HITACHI Gigabit Fibre Channel adapter user's guide (Support Matrix Edition)</i>. If the dedicated port functionality is enabled, this can be assigned to each port. 				

List of functionality supported by LPAR manager

The following table describes functionality supported by LPAR manager and their support conditions.

Table B-2 SMPs supported by LPAR manager

Item	Support condition
2-blade SMP	Y
4-blade SMP ¹	Y
Legend: Y: Can be used N: Cannot be used Notes: 1. The CB 520X B2 are supported by LPAR manager firmware version 02-27 or later.	

Table B-3 Maximum number of LPARs supported by LPAR manager

Item		Support condition
Maximum number of LPARs that can be defined		60
Maximum number of LPARs that can be activated	Essential	4
	Advanced	30
	Enterprise	60

Table B-4 Processors supported by LPAR manager

Item		Support condition
Minimum unit of division		Thread
Maximum number of logical processors	CB 520X B1/B2/B3	64 [02-0X or later] 72 [02-28 or later] ¹ 240 [02-40 or later] ^{1, 2}
	CB 520H B3	64 [02-05 or later] 72 [02-50 or later] ¹
	CB 520H B4	88 [02-50 or later] ¹
Processor in dedicated mode	Specifying a physical processor number	Y
Processor in shared mode	Specifying a physical processor number	Y
	Service rate	Y
	Idle detection	Y
	Processor capping	Y

Item		Support condition
Maximum number of processor groups that can be defined	Essential	4
	Advanced	30
	Enterprise	60
Hyper-threading		Y
Scheduling mode dynamic change		Y
Partition Reference Time Enlightenment (PRTE)		Y [02-25 or later]
Legend: Y: Can be used Notes: 1. If the PRTE functionality is enabled, do not allocate more than 64 logical processors to an LPAR. 2. Only dedicated mode is supported.		

Table B-5 Memory supported by LPAR manager

Item			Support condition
Minimum unit of division			256 MB
Minimum amount of memory that can be allocated to one LPAR			256 MB
Maximum amount of memory that can be allocated to one LPAR			4,092 GB ²
Maximum amount of memory that can be installed	CB 520X B1/B2/B3	1-blade	1,536 GB
		2-blade SMP	3,072 GB
		4-blade SMP	6,144 GB
	CB 520H B3/B4		768 GB
Memory amount that LPAR manager uses ¹	CB 520X B1/B2		3 GB
	CB 520X B3		6 GB
	CB 520H B3		2.5 GB
	CB 520H B4		4 GB (when MM Config Base is set to 2 GB)
			6 GB (when MM Config Base is set to 3 GB)
Non-NUMA			Y
NUMA			Y
L3 cache allocation ³	CB 520X B1/B2		N
	CB 520X B3		Y [02-55 or later]
	CB 520H B3		N

Item		Support condition
	CB 520H B4	Y [02-55 or later]
<p>Legend:</p> <p>Y: Can be used</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. The maximum amount of memory that can be allocated to LPAR is calculated by the following formula: (maximum-amount-of-memory-installed) - (amount-of-memory-used-by-LPAR-manager) 2. The smaller of the two values, 4,092GB and the maximum amount of memory that can be allocated to LPAR (Note 1), is the maximum amount of memory that can be allocated to one LPAR. 3. Only Enterprise models are supported. 		

Table B-6 NICs supported by LPAR manager

Item		Support condition
Dedicated NIC ^{4,6}	Minimum unit of division	Controller (Device)
		Port [02-50 or later] ³
	Maximum number of NIC ports that can be assigned per LPAR	Same as the number of physical NICs
	VLAN	Y
	WoL	N
	Teaming	Y
	TSO	Y
	Promiscuous mode	Y
	Inter-LPAR communication packet filtering	N
	PXE boot	N
	iSCSI boot	N
	FCoE boot ⁵	Y [02-50 or later]
Shared NIC	Minimum unit of division	Port
	Maximum number of physical LAN controllers that can be assigned per LPAR manager	8
	Maximum number of physical ports that can be assigned per LPAR manager	16
	Maximum number of shared NICs that can be assigned per LPAR	16
	Port Multiple Assignment	Y
	Port Separate Assignment	Y

Item		Support condition
	VLAN	Y
	WoL ^{1, 2}	Y
	Teaming	Y
	TSO	Y
	Promiscuous mode	Y
	Inter-LPAR communication packet filtering	Y
	PXE boot ¹	Y
	iSCSI boot	N
	FCoE boot	N
VF NIC ⁶	Minimum unit of division	Port
	Maximum number of LAN controllers that can be assigned per LPAR manager	8
	Maximum number of physical ports that can be assigned per LPAR manager	16
	Maximum number of VF NICs that can be assigned per LPAR	16
	Port Multiple Assignment	Y
	Port Separate Assignment	Y
	VLAN	Y
	WoL	N
	Teaming	Y
	TSO	Y
	Promiscuous mode	N
	Inter-LPAR communication packet filtering	N
	PXE boot	N
	iSCSI boot	N
	FCoE boot	N
Virtual NIC	Maximum number of network segments per LPAR manager	4
	Maximum number of virtual NICs that can be assigned per LPAR	16
	VLAN	Y
	WoL	N

Item		Support condition
	Teaming	Y
	TSO	Y
	Promiscuous mode	Y
	Inter-LPAR communication packet filtering	N
	PXE boot	N
	iSCSI boot	N
	FCoE boot	N
Multichannel		N
SR-IOV		Y
<p>Legend:</p> <p>Y: Can be used</p> <p>N: Cannot be used</p> <p>Notes:</p> <ol style="list-style-type: none"> Supported by onboard LANs and mezzanine cards mounted on server blades only. Not supported by I/O adapters. Only when the management tool is the deployment manager of HCSM. Supported by only HCSM power control through WoL. If the dedicated port functionality is enabled, this can be assigned to each port. If SR-IOV is enabled, the NIC does not run in multi-queue mode even in dedicated mode. As a result, performance might be reduced. To use an NIC in dedicated mode, set the SR-IOV setting to disabled (default setting). The FCoE functionality is supported only by the onboard LANs (Onboard LAN) mounted on server blades. There are some restrictions on guest OSs. For details, see Differences in supported items depending on the guest OSs on page B-22. 		

Table B-7 FCs supported by LPAR manager

Item		Support condition
Dedicated FC	Minimum unit of division	Controller (Device)
	Maximum number of dedicated FC ports per port	Same as the number of physical FC ports
	SAN boot	Y
	NPIV-compatible fibre channel switch connection configuration	Y
	SAN storage direct connection configuration	Y
	N+M cold standby (LUID mode)	Y (02-40 or later)
Shared FC	Minimum unit of division	Port

Item		Support condition
	Maximum number of dedicated FC ports per port	8Gb fibre channel adapter: 15 16Gb fibre channel adapter: 30
	SAN boot	Y
	NPIV-compatible fibre channel switch connection configuration	Y
	SAN storage direct connection configuration	Y
	HBA-core dedicated mode ¹	Y ²
	N+M cold standby (LUID mode)	Y (02-40 or later)
Legend: Y: Can be used N: Cannot be used Notes: 1. Only Enterprise models are supported. 2. Supported by LPAR manager firmware version 02-27 or later.		

Table B-8 USB and KVM ports supported by LPAR manager

Item		Support condition
Front side of management module	USB port	N
Front side of server blade	USB port	Y
	KVM port	Y
Legend: Y: Can be used N: Cannot be used		

Table B-9 User interfaces supported by LPAR manager

Item		Support condition
GUI	Web console	Y
	HCSM ¹	Y
	HVM Navigator ²	Y
CUI	LPAR manager screen	Y
	Guest screen	Y
CLI	HvmSh	Y
Legend: Y: Can be used Notes:		

Item	Support condition
1. For details about the support status, see the manual <i>Hitachi Command Suite Compute Systems Manager User Guide</i> .	
2. There are restrictions on guest OSs. For details, see Differences in supported items depending on the guest OSs on page B-22 .	

Table B-10 System operation functionality supported by LPAR manager

Item		Support condition
Web console		Y
HCSM linkage ¹		Y
HVM Navigator ³	LPAR configuration	Y
	Monitoring	Y
	Configuration viewer	Y
	LPAR migration	Y
Remote console		Y
Virtual COM Console	Maximum number of simultaneous connections	16
Logical VGA snapshot		Y
LPAR manager system time	Local time	Y
	UTC	Y
NTP	LPAR time	Y
	LPAR manager system time	Y
Power saving	Power-capping	N
	C3/C6	Y
	P-State	N
LP IP address	IPv4	Y
	IPv6	Y [02-25 or later]
LP communication settings		Y [02-25 or later]
Maximum number of settable VNIC systems		1024
Performance tuning options ²		Y [02-27 or later]
DNS		Y [02-40 or later]
Legend: Y: Can be used N: Cannot be used Notes: 1. For details about the support status, see the manual <i>Hitachi Command Suite Compute Systems Manager User Guide</i> . 2. Only Enterprise models are supported.		

Item	Support condition
3. There are restrictions on guest OSs. For details, see Differences in supported items depending on the guest OSs on page B-22 .	

Table B-11 High-reliability functionality supported by LPAR manager

Item		Support condition
N+M cold standby ¹		Y
HA monitor		Y
UPS		Y
Access control		Y (02-45 or later)
User authentication	Local authentication	Y (02-05 or later)
	LDAP authentication	Y (02-40 or later)
	RADIUS authentication	Y (02-45 or later)
	User authentication log	Y (02-05 or later)
Audit log		Y (02-40 or later)
LPAR manager security		Y
Legend: Y: Can be used		
Notes:		
1. Active blades and their corresponding standby blades must be configured on server blades of the same model.		

Table B-12 Maintenance functionality supported by LPAR manager

Item	Support condition
LPAR manager dump	Y
Guest OS dump	Y
Console log data	Y
Guest memory dump	Y
Linux Tough Dump	Y
LPAR manager firmware version upgrade/revision update	Y
Legend: Y: Can be used	

Table B-13 Software supported by LPAR manager

	Item	Support condition
Virtualization software	VMware	N

	Item	Support condition
	Hyper-V	N
Database	HiRDB	Y
	Oracle Database ¹	Y
Legend: Y: Can be used N: Cannot be used Notes: 1. The support status differs depending on the version of Oracle Database.		

SR-IOV functionality supported by LPAR manager

The following table describes SR-IOV functionality supported by LPAR manager and their support conditions.

Table B-14 List of configurations supported by the SR-IOV functionality

	Item	Support condition
Prerequisite configuration	Switch	Only 10Gb switch connections are supported. Switches can be used only for 10Gb connections. If the communication speed of a switch is fixed to 1Gb, the switch is not linked up.
	NIC ⁸	Emulex 10Gb NIC ^{1, 2, 3} 10GBASE-SR 2-port LAN adapter (supported only when the version is 02-40 or later and the adapter is used together with Enterprise models)
	OS ^{4, 5, 6, 7}	Emulex 10Gb 2-port converged network adapter Windows Server 2012 (02-55 or later) Windows Server 2012 R2 (02-55 or later) Red Hat Enterprise Linux 6.5 (02-00 or later) Red Hat Enterprise Linux 6.6 (02-06 or later) Red Hat Enterprise Linux 6.7 (02-45 or later) Red Hat Enterprise Linux 7.1 (02-45 or later)

Item		Support condition
		Red Hat Enterprise Linux 7.2 (02-50 or later)
		Onboard LAN Red Hat Enterprise Linux 6.5 (02-00 or later) Red Hat Enterprise Linux 6.6 (02-06 or later) Red Hat Enterprise Linux 6.7 (02-45 or later) Red Hat Enterprise Linux 7.1 (02-45 or later) Red Hat Enterprise Linux 7.2 (02-50 or later)
		Intel 10GBASE-SR 2-Port LAN adapter Windows Server 2012 (02-50 or later) Windows Server 2012 R2 (02-50 or later) Windows Server 2016 (02-56 or later) Red Hat Enterprise Linux 6.5 (02-40 or later) Red Hat Enterprise Linux 6.6 (02-40 or later) Red Hat Enterprise Linux 6.7 (02-45 or later) Red Hat Enterprise Linux 6.8 (02-55 or later) Red Hat Enterprise Linux 6.9 (02-59 or later) Red Hat Enterprise Linux 6.10 (02-66 or later) Red Hat Enterprise Linux 7.1 (02-40 or later) Red Hat Enterprise Linux 7.2 (02-45 or later) Red Hat Enterprise Linux 7.3 (02-58 or later) Red Hat Enterprise Linux 7.4 (02-62 or later) Red Hat Enterprise Linux 7.5 (02-64 or later) Red Hat Enterprise Linux 7.6 (02-67 or later) Red Hat Enterprise Linux 7.7 (02-69 or later)

Item			Support condition	
Settings with SR-IOV	SR-IOV settings for NIC ⁹		Enabled	
	NIC scheduling mode		Shared mode	
Performance	Maximum throughput per port ^{10, 11}		About 7 Gbps	
	Physical processor load		Low	
NIC functions	RSS (multi-queue)		N	
	Flow control		Y	
	Transmission band control ^{12, 21}		Only transmission is supported. Unit: 100 Mbps Range: 100 Mbps to 10,000 Mbps	
	Virtual port (VF)	Number of shares per port	Emulex 10Gb 2-port converged network adapter 16 Onboard LAN 15 Intel 10GBASE-SR 2-Port LAN adapter 63 ¹³	
			Multicast packet	Y
			Broadcast packet	Y
			Promiscuous mode	N
	Redundant configuration (Windows)	Mode	No dependency on the switch: Y Static teaming: Y LACP: N	
	Redundant configuration (Linux) ¹⁴	Monitoring method	Emulex 10Gb 2-port converged network adapter ARP monitoring/MII monitoring Onboard LAN MII monitoring Intel 10GBASE-SR 2-Port LAN adapter ARP monitoring/MII monitoring	
		Mode	balance-rr: N active-backup: Y balance-xor: N broadcast: N	

Item			Support condition
			802.3ad: N balance-tlb: N balance-alb: N
		MAC failover	Emulex 10Gb 2-port converged network adapter Y Onboard LAN Y Intel 10GBASE-SR 2-Port LAN adapter Y
	VLAN ^{14, 15, 23}	Undef	Emulex 10Gb 2-port converged network adapter N Onboard LAN N Intel 10GBASE-SR 2-Port LAN adapter Y ¹⁶
		Port VLAN (Untagged setting)	Emulex 10Gb 2-port converged network adapter Y (Only one VLAN is available for one port.) ¹⁷ Onboard LAN Y (Only one VLAN is available for one port.) ¹⁷ Intel 10GBASE-SR 2-Port LAN adapter Y (Only one VLAN is available for one port.) ¹⁸
		Tag VLAN (Tagged setting)	Emulex 10Gb 2-port converged network adapter Y (All VLANs are permitted only.) Onboard LAN Y (All VLANs are permitted only.) Intel 10GBASE-SR 2-Port LAN adapter N
	Inter-LPAR communication ^{19, 20}		Y
LPAR manager functions	User interface	HVM Navigator	Y
		LPAR manager screen	Y

Item			Support condition
		HvmSh	Y
	LPAR migration	Shutdown	Y
		Concurrent maintenance	N
	Force Recovery ²²		Y
Middleware	HCSM		Y (Display only)
	Log Monitor (hardware maintenance agent)		Y
	Linux high-reliability option	Linux Tough Dump	Y
		HA Network Driver for Linux	N
		HA Logger Kit for Linux	Y
	N+M cold standby		Y

Legend:
Y: Can be used
N: Cannot be used

Notes:
1. Use the same setting according to whether you enable or disable SR-IOV for the ports in the controller.
2. Emulex 10Gb NIC with different firmware cannot be mounted in the same server blade.
3. For details about the combinations of firmware versions and drivers, see the manual *Hitachi Compute Blade Emulex Adapter User's Guide for Driver*.
To perform a forced recovery operation, first shut down the OS running on the LPARs, and deactivate the LPARs.
4. When a guest OS to which a VF NIC is assigned starts up, the following messages are collected in /var/log/messages and the system event log (if Log Monitor (hardware maintenance agent) is running)). However, operation of the guest OS is not affected.
o /var/log/messages
be2net 0000:XX:XX.X: Could not use PCIe error reporting
XX:XX.X is Bus:Dev.Func
o System event log
Timestamp Module Level System event log
Message

yyyy-mm-dd hh:mm:ss PX/BX Info XXXX D2 7400 00 37XX 39FFFFFF
576481 Could not use PCIe error reporting
Applicable only when 37XX 39FFFFFF (XX depends on the LPAR number) is output to the system event log.
5. When a guest OS tries to enable the promiscuous mode of a VF NIC (for example, when tcpdump is activated), the following messages are collected in /var/log/

Item	Support condition
<p>messages and the system event log (if Log Monitor (hardware maintenance agent) is running)). However, operation of the guest OS is not affected.</p> <ul style="list-style-type: none"> <code>/var/log/messages</code> <code>be2net 0000:XX:XX.X: opcode 34-1 failed:status 3-8</code> <code>XX:XX.X is Bus:Dev.Func</code> System event log Timestamp Module Level System event log Message ----- yyyy-mm-dd hh:mm:ss PX/BX FAIL XXXX D2 7400 32 37XX 34FFFFFF 576525 opcode <u>number-number</u> failed:status <u>number-number</u> Applicable only when 37XX 34FFFFFF (XX depends on the LPAR number) is output to the system event log. 	
6. When a VF NIC device is blocked, the following message might be collected in /var/log/messages. To recover the blocked VF NIC device, immediately reboot the guest OS to which it is assigned.	
<ul style="list-style-type: none"> <code>/var/log/messages</code> <code>clocksource tsc unstable (delta = -8589944970 ns)</code> 	
7. In the output results of the <code>netstat -i</code> command, the value of a physical port (PF) is output to RX-ERR RX-DRP RX-OVR and TX-ERR TX-DRP TX-OVR.	
8. When you add or remove VF NICs to a guest OS, the PCI config addresses of some VF NICs are changed.	
<p>In this case, when the following conditions are met, the values of the network settings, such as the MAC address, the IP address, and so on, for VF NICs are also changed.</p> <ul style="list-style-type: none"> A VF NIC of the same controller is added or removed. A VF NIC with the same alphabetical character or an alphabetical character prior in alphabetical order, is added or removed. (For example, adding 1av affects the network settings of 1av and 1bv.) The guest OS is Red Hat Enterprise Linux 7 or Windows. 	
9. If the SR-IOV functionality for 10GBASE-SR 2-port LAN adapters is used, you do not need to enable the SR-IOV functionality because it is always enabled.	
10. This value is a guideline based on the measurement result in our environment. The actual network throughput value varies depending on the measurement environment and measurement method.	
11. In the following conditions, VF NIC network throughput might not be sufficient.	
<ul style="list-style-type: none"> Network traffic for a VF NIC is high. A large amount of interruption processing occurs in a short time, and CPU utilization is high. <p>In such a case, add the following codes to the <code>/etc/rc.d/rc.local</code> file, and then restart the OS. (When the OS restarts, it is automatically set.)</p> <pre>/sbin/ethtool -C eth<N> adaptive-rx off /sbin/ethtool -C eth<N> rx-usecs 128</pre> <p>Specify the name of the VF NIC network device to be set for <code>eth<N></code> (for example, <code>eth0</code>).</p>	
12. For 10GBASE-SR 2-port LAN adapters, the throughput performance obtained is a value in the range from the setting value to two times the setting value.	

Item	Support condition
<p>13. For 10GBASE-SR 2-port LAN adapters, the maximum number of shares per port varies depending on the system configuration.</p> <ul style="list-style-type: none"> ◦ The number of cores per CPU ◦ Whether the SR-IOV functionality is enabled or disabled on the network device where the Onboard LAN controller is mounted ◦ Whether hyper threading is enabled or disabled <p>For details about the relationship between system configuration conditions and the maximum number of shares per port, see Table B-15 Maximum number of shares per port of a 10GBASE-SR 2-port LAN adapter on page B-19.</p> <p>14. When you use path redundancy and VLAN, perform the following settings as Table B-16 VLAN settings (Emulex 10Gb 2-port converged network adapter/Onboard LAN) on page B-19, or Table B-17 VLAN settings (Intel 10GBASE-SR 2-Port LAN adapter) on page B-19.</p> <p>If you want to set fail_over_mac=0 to VF NICs of several LPARs and the VF NICs are in the same network segment, set the VF NIC in each LPAR as primary device.</p> <p>15. On the OS, do not specify tagged VLAN settings for VF NICs that are set to Untagged mode.</p> <p>16. Tagged packets can be sent and received.</p> <p>17. Untagged cannot be used in a VF NIC configuration where guest OSs are Red Hat Enterprise Linux 6.7/7.1/7.2.</p> <p>18. When the guest OS on an LPAR is Red Hat Enterprise Linux 7.2/7.3/7.4/7.5/7.6/7.7 and is using bonding, note the following:</p> <ul style="list-style-type: none"> ◦ Do not configure any VLAN settings for all NIC ports through NetworkManager in guest OSs. ◦ Do not configure any VLAN settings for all NIC ports with "ifcfg-eth" files in /etc/sysconfig/network-scripts in guest OSs. ◦ Register the 8021q module in the blacklist of the guest OS by adding <code>blacklist 8021q</code> to the <code>/etc/modprobe.d/blacklist-LPAR.conf</code> file. <p>19. If you are using inter-LPAR communication that uses a VF NIC, set "fail_over_mac=1" for the bonding option. If you do not specify the setting as above, you might not be able to use inter-LPAR communication when switching bonding.</p> <p>20. Inter-LPAR communication cannot be established on VF NICs and shared NICs that use the same physical port.</p> <p>21. There is a difference of, at the most, approximately 100 Mbps between the actual throughput and the value set for TxRate.</p> <p>22. If a forced recovery operation is performed while an LPAR is running, a VF NIC cannot be used from the OS on the LPAR. To recover the VF NIC, reboot the OS on the LPAR after the forced recovery operation is completed.</p> <p>Before performing a forced recovery operation, shut down the OS on the LPAR to deactivate the LPAR.</p> <p>23. When an Emulex adapter is used in your Windows environment, VLAN communications cannot be accomplished if the teaming window of Windows is used for VLAN configuration. You must use Device Manager to configure the VLAN.</p> <ol style="list-style-type: none"> 1. Start Device Manager. 2. Open the properties of the Emulex NIC device below Network adapters. 3. In the Advanced tab, select VLAN Identifier (802.1q) and configure the VLAN ID. 	

Table B-15 Maximum number of shares per port of a 10GBASE-SR 2-port LAN adapter

System configuration	Number of CPU cores per socket						
	4	6	8	10	12 to 18	20	22 or later
<ul style="list-style-type: none"> SR-IOV: disable Hyper threading: enable 	16	16	16	63	63	63	63
<ul style="list-style-type: none"> SR-IOV: disable Hyper threading: disable 	4	4	16	16	16	63	63
<ul style="list-style-type: none"> SR-IOV: enable Hyper threading: enable 	4	16	16	16	63	63	63
<ul style="list-style-type: none"> SR-IOV: enable Hyper threading: disable 	0	0	4	16	16	16	63

Table B-16 VLAN settings (Emulex 10Gb 2-port converged network adapter/Onboard LAN)

Item	LPAR manager VLAN mode	fail_over_mac setting
ARP monitoring	Untagged	fail_over_mac=1
MII monitoring	Untagged	<ul style="list-style-type: none"> For Emulex 10Gb 2-port converged network adapter/Onboard LAN firmware version 10.2 fail_over_mac=1 (recommended) or fail_over_mac=0 For Emulex 10Gb 2-port converged network adapter/Onboard LAN firmware version 10.6 fail_over_mac=1
	Tagged (All permitted only)	fail_over_mac=0

Table B-17 VLAN settings (Intel 10GBASE-SR 2-Port LAN adapter)

Item	LPAR manager VLAN mode	fail_over_mac setting
ARP monitoring	Undef	fail_over_mac=1
MII monitoring	Untagged	

Dedicated port functionality supported by LPAR manager

The following table describes the dedicated port functionality supported by LPAR manager and their support conditions. The table also describes the differences from the dedicated device functionality.

Table B-18 Dedicated port functionality and their supported conditions

Item		Support condition
LPAR manager license	Essential	N
	Advanced	Y
	Enterprise	Y
NIC type	1000BASE-T 4-port LAN adapter	Y
	Other than the above	N
Coexistence of dedicated mode and shared mode		Y
Maximum number of divisions		Same as the number of physical NIC ports
Performance	Response and throughput of port dedicated NICs	90% of device dedicated NICs
Force Recovery	Port dedicated NICs are not linked down.	Y
N+M cold standby	The definitions of port dedicated NICs are moved.	Y
LPAR migration	LPAR migration of an LPAR to which a port dedicated NIC is assigned	N
	LPAR migration of an LPAR to which a shared NIC is assigned	Y
Startup of LPAR manager	Startup of LPAR manager by using the NIC for which the dedicated port functionality is enabled (including a startup of LPAR manager in safe mode)	Y
Upgrade of LPAR manager	Inheriting the configuration information of LPAR manager when it is upgraded	Y
	Inheriting the configuration information of LPAR manager when it is downgraded	N
Legend: Y: Can be used N: Cannot be used		

Table B-19 Management tools and their support conditions

Operation	1	2	3	4	5
Enable or disable the dedicated port functionality	N	N	N	N	Y
Switch dedicated and shared modes	N	N	N	Y	Y
Legend: Y: Can be used N: Cannot be used					

Operation	1	2	3	4	5
1. Web console					
2. HCSM console					
3. HVM Navigator console					
4. LPAR manager screen					
5. HvmSh					

LPAR manager licenses

There are three types of licenses for LPAR manager: Essential, Advanced, and Enterprise. In addition, there are two types of licenses for the Advanced and Enterprise licenses: a permanent LPAR manager license (with no expiration date) and a temporary LPAR manager license (with an expiration date).

Types of LPAR manager licenses

The following table describes the types of LPAR manager licenses:

Table B-20 Types of LPAR manager licenses

LPAR manager license		Supported versions		Supported blades
		Management module	LPAR manager	
Essential license(Essential model)	permanent LPAR manager license	All versions	All versions	All blades
	temporary LPAR manager license	--	--	--
Advanced license(Advanced model)	permanent LPAR manager license	All versions	All versions	All blades
	temporary LPAR manager license	A0135 or later	02-27 or later	CB 520X B2
		A0155 or later	02-46 or later	CB 520X B3
		A0160 or later	02-50 or later	CB 520H B4
Enterprise license(Enterprise model)	permanent LPAR manager license	A0135 or later	02-27 or later	CB 520X B2
		A0155 or later	02-46 or later	CB 520X B3
		A0160 or later	02-50 or later	CB 520H B4

LPAR manager license		Supported versions		Supported blades
		Management module	LPAR manager	
	temporary LPAR manager license	A0135 or later	02-27 or later	CB 520X B2
		A0155 or later	02-46 or later	CB 520X B3
		A0160 or later	02-50 or later	CB 520H B4

Functional differences depending on the LPAR manager license

The following table describes functional differences depending on the type of LPAR manager license:

Table B-21 Functional differences depending on the LPAR manager license

Function	Essential	Advanced	Enterprise
Maximum number of LPARs that can be activated	4	30	60
LPAR migration (Concurrent maintenance)	N	Y	Y
HBA-core dedicated mode	N	N	Y
10GBASE-SR 2-port LAN adapter (SR-IOV)	N	N	Y
L3 cache allocation	N	N	Y
Performance tuning options	N	N	Y
Dedicated port functionality	N	Y	Y
Legend: Y: Supported N: Not supported			

Differences in supported items depending on the guest OSs

The following table describes the differences in supported items depending on the guest OSs.

Table B-22 Differences in supported items depending on the guest OSs

Items		Guest OSs		
		Other than Windows Server 2016 or RHEL6.8/6.9 / 6.10/7.3/7.4/7.5/7.6/7.7	Windows Server 2016, RHEL6.8	RHEL6.9/6.10/7.3/7.4/7.5/7.6/7.7
Hardware configuration/ functionality	FCoE mode (Emulex CNA)	Y	Y	N
LPAR manager functionality	Dedicated NIC(Emulex NIC)	Y	N	N
	VF NIC(Emulex NIC)	Y	N	N
	LPAR migration in concurrent maintenance mode	Y	Y	N
Middleware	HVM Navigator	Y	Y	N
Legend: Y: Supported N: Not supported				



LPAR manager Setting Items List

This appendix describes the list of LPAR manager setting items.

- ☐ [LPAR manager setting items](#)
- ☐ [EFI driver setting items](#)

LPAR manager setting items

The following table describes LPAR manager system setting items required to configure LPAR manager.

Table C-1 LPAR manager setting items (Web console)

Item		Description	Default ¹
EFI		Set EFI on the server blade. Setting values of each item are the same as when the server blade operates in Basic mode. For details, see the manual <i>Hitachi Compute Blade 2500 Series UEFI Setup Guide</i> .	Depends on the initial setting (the setting at shipping time)
LPAR manager Firmware Bank		Select a value in the range from 0 to 3.	0
Logical partitioning		Set the LP mode.	Depends on the initial setting (the setting at shipping time)
IPv4	IP address	Set the LP IP address for IPv4 and other items.	0.0.0.0
	Subnet mask		0.0.0.0
	Default gateway		0.0.0.0
IPv6	Static address	Set the LP IP address for IPv6 and other items.	Disable [A0130 or later]
	IP address		-- [A0130 or later]
	Prefix len		-- [A0130 or later]
	Default gateway		Not use [A0130 or later]
	Address		-- [A0130 or later]
	Stateless address	To use a stateless address, set Enable.	Disable [A0130 or later]
LP communication settings		Set the protocol that is used for communication between LPAR manager and the management module.	IPv4 [A0130 or later]
VNIC System No		Set VNIC system numbers. Set a value which does not overlap with other LPAR manager(s), for example Compute Blade Series.	0
Time zone		Set LPAR manager system time zone.	Depends on the initial setting (the

Item	Description	Default ¹
		setting at shipping time)
Performance tuning options	To enable Performance tuning options, set Enable.	Disabled [A0135 or later]
Management path	Set NICs and ports to be used for connecting LPAR manager to management paths.	Disabled [A0120 or later]
User authentication	Set up user authentication for connecting via the LP CLI.	Disabled [A0110 or later]
CLI IP address (IPv4)	Set the IP address of the server running the HvmSh command, etc.	0.0.0.0
CLI IP address (IPv6)		:: [A0130 or later]
Connection mode	Set the connection method for the virtual COM console.	Telnet [A0110 or later]
Telnet user authentication	Set up user authentication for connecting to the guest screen.	Disabled [A0110 or later]
Virtual COM console port	Set a TCP port of a virtual COM console.	20801 [A0110 or later]
Password expiry period (day)	Set the validity period of the password.	0 [A0110 or later]
LP options	Set up periodical diagnosis of management paths.	Disabled [A0120 or later]
Notes:		
1. [] is supported management module firmware version.		

Table C-2 LPAR manager setting items (LPAR manager screen)

Item		Description	Default ¹
System Configuration	LP ID	Set the LPAR manager ID.	LP_0000
	VNIC System No	Set VNIC system numbers. Set a value which does not overlap with other LPAR manager(s), for example Compute Blade Series.	0
	Virtual Console Port	Set a TCP port of a virtual COM console.	20801
	LP CLI IP Address (IPv4)	Set the IP address of the server running the HvmSh command, etc.	0.0.0.0
	LP CLI IP Address		::

Item		Description	Default ¹
	(IPv6)		[02-25 or later]
	VC	Set up user authentication for connecting to the guest screen.	Disable [02-05 or later]
	LP CLI	Set up user authentication for connecting via the LP CLI.	Disable [02-05 or later]
	Expiry	Set the validity period of the password.	0 [02-05 or later]
	Type	Set the connection method for the virtual COM console.	Telnet [02-05 or later]
	SYS2 Processors	Set the upper limit of the number of the physical processors used by SYS2.	2 [02-62 or later]
Date and Time	Select Display	Select the time to display.	LPAR RTC
	System Time Zone	Set LPAR manager system time zone.	+ 0:00
	TimeSync	Select a time synchronous setup by an NTP server. We recommend a setup that performs synchronizing of the time by a management module.	Disable
LP Options	Pre-state auto activation	Set Yes for restoring LPAR to the same condition as previous LPAR before rebooting LPAR manager by accident.	No
	LP Auto Shutdown	Set Yes for shutting down LPAR manager when all LPARs are deactivated.	No
	LP ErrorWatching	Set Yes for detecting a hung-up state.	Yes
	PhyCPU C-State (>= C3)	Set Enable for enabling the save electric power functionality.	Enable
	USB Auto Allocation to LPAR	Set Enable so that USB devices are automatically attached to all LPARs when the LPARs are activated or reactivated. Set Disable so that USB devices are automatically attached to only the specified LPAR.	Enable
	Save Changed Config Format	Set Enable for enabling the configuration information auto save functionality.	Disable

Item		Description	Default ¹
	Save Time Config	Set Enable for enabling the time information auto save functionality.	Disable
	Activation	Set Yes for displaying a confirmation sub-screen at activation.	Yes
	Deactivation and Reactivation	Set Yes for displaying a confirmation sub-screen when deactivation or reactivation is performed.	Yes
	Screen Switching Character	Set a character used to switch from the guest screen to the LPAR manager screen.	I (el)
Logical Partition Configuration	LPAR Name	Sets the LPAR name.	NO_NAME
	Scheduling Mode (Scd)	Set a shared mode or a dedicated mode.	D
	Logical Processor Number (Pro)	Sets the number of logical processors.	1
	Processor Group Number (Grp)	Sets the processor group number.	0
	Service rate (Srv)	Set a service ratio of physical processor. You can only set this option for an LPAR in shared mode.	100
	Memory Size (Mem)	Set a memory size.	1024
	Memory Node Number (MN)	Set a memory node number to be assigned to an LPAR. MN is available only when the EFI NUMA setting is enabled.	A
	Idle Detection (ID)	Set Y for detecting a logical processor idle state. Set this item to Y to use CPU resources efficiently.	If Performance tuning options are disabled: Y
			If Performance tuning options are enabled: N
	Guest Idle Mode	Indicates a mode to process instructions when logical processors are idle. You can change the setting only while Performance tuning options are enabled.	If Performance tuning options are disabled: HALT If Performance tuning options are enabled: MWAIT [02-27 or later]

Item		Description	Default ¹
	Low Latency	Indicates a method in which logical processors work in I/O access. You can change the setting only while Performance tuning options are enabled.	If Performance tuning options are disabled: N If Performance tuning options are enabled: Y [02-27 or later]
	EPT1GB	Indicates the size of a memory unit for memory control and operation. You can change the setting only while Performance tuning options are enabled.	Performance tuning options are disabled: N Performance tuning options are enabled: Y [02-27 or later]
	Automatic Activate (AA)	Set the order in which LPARs are activated automatically when LPAR manager boots up.	* (Unassigned)
	Automatic Clear (AC)	Set Y for automatic clearance of a logical SEL.	N
	Processor Capping (PC)	Set Y for performing a processor-capping. You can only set this option for an LPAR in shared mode.	* (Unassigned)
	Virtual COM Console (VC)	Set Y for using a virtual COM console.	N
	Pre-boot Firmware (PB)	Select pre-boot firmware. Use this item with the default value 64UEFI.	64UEFI
	NUMA	To apply NUMA to the LPAR, specify Y.	N
	PRTE	To apply PRTE to LPAR, specify Y.	N [02-25 or later]
Logical Processor Configuration	Logical Processor Assignment	Set an assignment of a physical processor to a logical processor.	A
Physical Processor Configuration	Processor Group Configuration	Sets the processor group number.	0
PCI Device Assignment	Scheduling Mode (Schd)	Set a shared mode or a dedicated mode.	S
	PCI Device Assignment	Sets the PCI device assignment.	--
Virtual NIC Assignment	VNIC Assignment	Set a logical NIC.	* (Unassigned)
	Promiscuous Mode	Sets the promiscuous mode.	T (shared NIC/virtual NIC)

Item		Description	Default ¹
		You can only set this option for shared NICs and virtual NICs.	R (VF NIC)
	VLAN Mode	Sets the VLAN mode. You can only set this option for shared NICs and virtual NICs.	Undef (shared NIC/virtual NIC/VFNIC (Intel 10GBASE-SR 2-Port LAN adapter)) Tag (VF NIC (Emulex 10Gb 2-port converged network adapter/ Onboard LAN))
	Inter-LPAR Packet Filtering	Sets the inter-LPAR communication packet filtering. You can only set this option for shared NICs.	Disable
	TXRATE	Sets the transmission band restrictions for VF NIC.	10,000 Mbps
Shared FC Assignment	Shared FC Assignment	Set an assignment of a shared FC port.	* (Unassigned)
Notes:			
1. [] is supported LPAR manager firmware version.			

EFI driver setting items

The following table describes EFI driver setting items required to configure LPAR manager.

Table C-3 EFI driver setting items

Item	Description	Default
Boot Function	Set Enable for enabling the SAN boot functionality. It is necessary to set an FC port of the boot path to enabled.	Disabled
Connection Type	Set the connection form of an FC interface.	Auto
Data Rate	Set the data transfer speed of an FC interface.	Depends on the initial setting (the setting at shipping time)
Select Boot Device Enable	Set Enable for searching for a boot device that is registered to the boot device list.	Disabled
Boot Device List	Register the boot device to be used when the Select Boot Device Enable option is set to Enable.	(All zero)



Available Consoles in LPAR manager

This appendix describes the functionality of LPAR manager for each console that can be used in LPAR manager.

- ☐ [Relationship between consoles and the functionality of LPAR manager](#)

Relationship between consoles and the functionality of LPAR manager

You can use the following consoles in LPAR manager:

1. Web console
2. HCSM console
3. HVM Navigator console
4. LPAR manager screen
5. Guest screen
6. Remote console
7. Virtual COM console
8. Remote desktop
9. LP Web system console

Item	1	2 ¹	3 ²	4	5	6	7	8	9
EFI settings	Y	N	N	N	N	N	N	N	N
Selecting the LPAR manager firmware	Y	N	N	N	N	N	N	N	N
Initializing LPAR manager	Y	Y	Y	Y	N	N	N	N	N
LP Mode setting	Y	Y	N	N	N	N	N	N	N
LPAR manager boot up	Y	Y	N	N	N	N	N	N	N
Creating an LPAR	Y	Y	Y	Y	N	N	N	N	N
Setting the boot order	Y	N	Y	N	Y	Y	Y	N	N
LPAR activation	Y	Y	Y	Y	N	N	N	N	N
Guest OS installation	N	N	N	N	N	Y	N	N	N
Guest OS operation	N	N	N	N	Y	Y	Y	Y	N
Guest OS failure detection	N	N	N	N	Y	Y	Y	N	Y
Collecting dumps of	N	N	Y	Y	N	N	N	N	N

Item	1	2 ¹	3 ²	4	5	6	7	8	9
a guest OS									
Guest OS shutdown	N	Y	N	N	Y	Y	Y	Y	N
Stopping an LPAR	Y	Y	Y	Y	N	N	N	N	N
LPAR manager shutdown	Y	Y	Y	Y	N	N	N	N	N
LPAR manager firmware version upgrade/revision update	Y	N	N	N	N	N	N	N	N
Model upgrade	Y	N	N	N	N	N	N	N	N
Using each LPAR manager or LPAR	LPAR manager	LPAR manager	LPAR manager	LPAR manager	LPAR manager	LPAR manager	LPAR	LPAR	LPAR manager
Legend: Y: Available N: Not available Notes: 1. For the latest support status, see the manual <i>Hitachi Command Suite Compute Systems Manager User Guide</i> . 2. For the latest support status, see the manual <i>Hitachi Compute Blade HVM Navigator User's Guide - Getting Started</i> .									



Port numbers used by LPAR manager

This appendix describes the port numbers that LPAR manager uses to communicate with modules and external programs.

- ☐ [Port numbers used for communication with the management server](#)
- ☐ [Port numbers used for communication with a management module](#)
- ☐ [Port numbers used for LPAR migration](#)

Port numbers used for communication with the management server

The following table describes the port numbers (the setting at shipping time) that LPAR manager uses to communicate with the management server.

For each of the following items, you can change the default port number to any port number in the range of specifiable values.

Table E-1 Port numbers used for communication with the management server

Item	Protocol	Port number	Direction of communication	Remarks	Communication protocol
HCSM	TCP	22611	From LPAR manager to the management server	Communication with HCSM	--
LPAR migration	TCP	23401, 20671, 20650	Bidirectional	LPAR migration	--
NTP	UDP	123	From LPAR manager to the management server	Time synchronization	NTP
Virtual COM console	TCP	[LPAR manager firmware version 02-02 or earlier] 20801 to 20816 (specifiable values: 1024 to 65520)	From the management server to LPAR manager	Virtual COM console	--
		[LPAR manager firmware version 02-05 or later] 20801 to 20832 (specifiable values: 1024 to 65520 ¹)			
Virtual COM console (LPAR manager internal use only)	TCP	22450	From the management server to LPAR manager	Virtual COM console	--
LP web system	TCP	443	From the management server to LPAR manager	Logical VGA snapshot	HTTPS
HvmSh	UDP	623	From the management server to LPAR manager	HvmSh command, HVM Navigator, etc.	RMCP

Item	Protocol	Port number	Direction of communication	Remarks	Communication protocol
	TCP	23250, 20670	From the management server to LPAR manager		--
Guest memory dump collection command and LPAR manager dump collection command	TCP	20, 21	From LPAR manager to the management server	Dump collection	FTP
DNS	UDP	53	From LPAR manager to the management server	Name retrieval	--
Syslog	UDP	6514 (specifiable values: 1 to 65535)	From LPAR manager to the management server	Audit log collection	--
	TCP				
	TLS				
LDAP	TCP	389 (specifiable values: 1 to 65535)	From LPAR manager to the management server	LDAP authentication	--
RADIUS	UDP	1812 (specifiable values: 1 to 65535)	From LPAR manager to the management server	RADIUS authentication	--
Notes: 1. If the connection method of the Virtual COM console is "user authentication-enabled Telnet" or "SSH", a value from 1024 to 65504 can be set.					

Port numbers used for communication with a management module

The following table describes the port numbers (the setting at shipping time) that LPAR manager uses to communicate with a management module.

For each of the following items, you can change the default port number to any port number in the range of specifiable values.

Table E-2 Port numbers used for communication with a management module

Item	Protocol	Port number	Direction of communication	Remarks
Communication between management modules	TCP	[LPAR manager firmware version 02-20 or earlier] 25101, 25102	From LPAR manager to the management module	Heartbeat between management modules, N+M cold standby, saving configuration information, LPAR dump transfer
		[LPAR manager firmware version 02-25 or later] 25101, 25102 (specifiable values: 1024 to 32767)		
HA monitor	TCP	[LPAR manager firmware version 02-20 or earlier] 25201	From the management module to LPAR manager	HA monitor
		[LPAR manager firmware version 02-25 or later] 20672 (specifiable values: 1024 to 32767)		
Boot notification for a management module	UDP	[LPAR manager firmware version 02-20 or earlier] 25202	From the management module to LPAR manager	Boot notification for a management module
		[LPAR manager firmware version 02-25 or later] 25202 (specifiable values: 1024 to 32767)		
HvmSh	TCP	[LPAR manager firmware version 02-20 or earlier] 23250	From the management module to LPAR manager	Communication from the Web console or HCSM
		[LPAR manager firmware version 02-25 or later] 20670 (specifiable values: 1024 to 32767)		

Port numbers used for LPAR migration

The following table describes the port numbers that LPAR manager uses to perform LPAR migration.

Table E-3 Port numbers used for LPAR migration

Item	Protocol	Port number	Programs and hardware that use the ports
LPAR migration	TCP	23402	Within LPAR manager
		23400	Between management servers



Glossary

This section explains the terminology you need to know when using the CB 2500.

A

active blade

When using the N+M cold standby function, the active blade is the server blade that is actively running your applications.

APC (Accurate Power Control)

A function that uses power capping to limit the power consumption of the system unit. The APC function reduces power consumption by controlling the CPU clock rate of the system unit when power consumption exceeds a predetermined level.

B

BMC

Baseboard management controller

A controller that monitors and controls the status of server blades. The BMC monitors and controls server blades by connecting to the system console and the management module.

C

CLI

Command Line Interface

CSV

Comma-Separated Values

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

D

DDE

Dynamic Data Exchange

Deployment Manager

Software provided as part of Compute Systems Manager. Deployment Manager is a function that allows you to back up and restore the disk data of a server blade as an image file. You can also use a backed up image file to replicate the environment of a managed resource on another managed resource.

F

FC

Fibre Channel

G

GUI

Graphical User Interface

I

I/O

Input/Output

IPMI

Intelligent Platform Management Interface

L

LDAP

Lightweight Directory Access Protocol

LID (Location Identifier lamp)

An LED lamp that you can use to identify the location of server chassis and modules. By controlling the LIDs of a server blade or server chassis remotely from the system console or Hitachi Compute Systems Manager, you can easily identify a managed resource in the system unit.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

logical partitioning

A function that uses Hitachi's server logical partitioning framework to logically partition a blade server composed of one or several server blades. Each logical partition can then be used to create a discrete server environment.

LPAR (Logical PARTition)

When using logical partitioning, an LPAR is the term for each logical partition that can accommodate a discrete server environment.

LPAR manager (Logical PARTitioning manager)

A function of logical partitioning. A component that manages LPARs on a blade server.

M

management module

A module that monitors and configures the system unit as a whole. The management module allows you to centrally manage the server blades and modules in the system unit.

memory dump

A file containing the memory contents of a server at a particular time. When a failure occurs in the OS, you can use a memory dump to diagnose the nature of the failure.

MIB

Management Information Base

N

N+M cold standby

When a failure occurs in a server, the N+M cold standby function allows the server to failover to a machine that is in standby with power off. When a failure occurs in an active blade, failover to the standby blade takes place automatically. The server that is actively running applications is called the "active blade". The server blade that is in standby is called the "standby blade".

NIC

Network Interface Card

NMI (Non-Maskable Interrupt)

A hardware interrupt issued to the CPU from an external device. An NMI can be used, for example, to collect OS dump files.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

O

OID

Object Identifier

P

PXE

Preboot eXecution Environment

R

remote console

Software provided with the CB 2500. You can use the remote console to remotely control the server OS and LPARs on a server blade.

S

server chassis

A frame in which server blades and modules are mounted.

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SR-IOV

Single Root IO Virtualization

SSH

Secure SHell

SSL

Secure Sockets Layer

standby blade

When using the N+M cold standby function, the standby blade remains in standby with its power off until a failover occurs from a failed active blade.

system console

A computer from which a user monitors and configures the CB 2500 system unit.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

switch module

A module that connects the system unit to LANs, SANs, and other networks.

T**terminal software**

Software that allows a user to operate a remote host computer from a terminal computer. The CB 2500 remote console can be operated using generic terminal software.

V**VF NIC**

Virtual Function Network Interface Card

virtual media

An image file that contains the data recorded on media such as a CD or DVD. By converting the installation media for the OS and other software to virtual media, you can make the software available for installation on a server blade.

W**Web console**

A console that runs in a Web browser. You can use the Web console to view hardware information for a server chassis or server blade, or to control the hardware remotely.

WMI

Windows Management Instrumentation

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	---	-------------------	-------------------	---	-------------------	---	---	-------------------	-------------------	-------------------	-------------------	-------------------	---	-------------------	-------------------	-------------------	---	-------------------	-------------------	---	---	---

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------



Index

A

Allocated FC Information screen 10-45
 checking configuration information of fibre
 channel adapter 10-46
audit log messages 11-34

B

basic environments 9-2
Basic mode 1-4

C

changing LPAR manager system time 10-65
changing LPAR manager system time zone 10-65
changing LPAR time 10-64
changing LPAR time zone 10-64
changing time mode of LPARs 10-64
checking BMC firmware version 10-92
checking EFI firmware version 10-92
checking fibre channel adapter firmware version
10-92
checking firmware 2-3
checking internal version of LPAR manager
firmware 10-92
checking LPAR manager firmware version 10-92
checking LPAR manager model 10-92
checking serial number of LPAR manager 10-92
checking system status of LPAR 10-87
checking the validity period of an LPAR manager
license 10-92
collecting console log data 10-87
collecting guest OS dump 10-87

collecting guest screen data 10-87
creating LPARs 3-2

D

Date and Time screen 10-63
 changing LPAR manager system time 10-65
 changing LPAR manager system time zone 10-65
 changing LPAR time 10-64
 changing LPAR time zone 10-64
 changing time mode of LPARs 10-64
 displaying RTC, or SEL time of LPARs 10-64
 importing synchronization settings of time from
 management module or BMC 10-65
 setting IP address of NTP server 10-65
 specifying time adjustment settings for NTP
 10-65
 synchronizing LPAR time with LPAR manager
 system time 10-65
dedicated mode 1-2
deleting LPARs 3-14
displaying RTC, or SEL time of LPARs 10-64

E

example of using promiscuous mode 6-19
example of using VLAN functionality 6-9
exclusively shared mode 1-3
exiting safe mode 9-22

F

FCoE 6-4

- Firmware Version Information screen 10-91
 - checking BMC firmware version 10-92
 - checking EFI firmware version 10-92
 - checking fibre channel adapter firmware version 10-92
 - checking internal version of LPAR manager firmware 10-92
 - checking LPAR manager firmware version 10-92
 - checking LPAR manager model 10-92
 - checking serial number of LPAR manager 10-92
 - checking the validity period of an LPAR manager license 10-92
- Front Panel screen 10-86
 - checking system status of LPAR 10-87
 - collecting console log data 10-87
 - collecting guest OS dump 10-87
 - collecting guest screen data 10-87
 - removing console log data 10-87
 - removing guest screen data 10-87
 - restoring Migration Failed LPAR 10-87

G

- guest OS 1-4

H

- HCSM alert messages
 - information level 11-73
 - warning level 11-74

I

- idle-detection functionality 1-5
- image of shared NIC switch 6-10
- image of VF NIC switch 6-12
- importing synchronization settings of time from management module or BMC 10-65
- installing LPAR manager firmware 8-20

L

- Logical Partition Configuration screen 10-8
 - adding LPAR 10-9
 - applying NUMA configuration to LPAR 10-9
 - applying PRTE to LPAR 10-9

- changing automatic clear functionality of logical SEL 10-9
- changing idle detection functionality 10-9
- changing LPAR name 10-9
- changing memory capacity 10-9
- changing memory node number which is assigned to LPAR 10-9
- changing number of logical processors 10-9
- changing processor capping functionality 10-9
- changing processor group number 10-9
- changing scheduling mode 10-9
- changing service ratio of service time 10-9
- changing service time distribution 10-9
- checking processor and memory number assigned to LPAR 10-9
- deleting LPAR 10-9
- displaying guest screen 10-9
- displaying memory allocation 10-9
- enabling virtual COM console functionality 10-9
- restarting LPAR 10-9
- saving configuration information 10-9
- starting LPAR automatically 10-9
- turning off LPAR 10-9
- turning on LPAR 10-9
- logical partitioning of hardware resources 1-2
- Logical Processor Configuration screen 10-20
 - assigning logical processor to physical processor 10-21
- logical RTC time 8-26
- LP mode 1-4
 - checking firmware 2-3
- LP Options screen 10-74
 - changing functionality for automatically saving configuration information 10-75
 - changing functionality for saving time information automatically 10-75
 - changing method for shutting down LPAR manager automatically 10-75
 - changing power saving functionality 10-75
 - Changing Safe Mode to OFF 10-75
 - changing setting to restore setting before restarting LPAR 10-75
 - changing the target LPARs for the USB Auto Attach functionality 10-75
 - collecting LPAR manager dumps 10-75
 - detecting LPAR manager hang up 10-75
 - restoring status before restarting LPAR 10-75
- LP System Logs screen 10-89
 - failure (Error) log 10-90

- information (Info) log 10-90
- warning (Warn) log 10-90
- LPAR manager boot messages 11-2
- LPAR manager environments 9-2
- LPAR manager firmware 2-3
- LPAR manager licenses B-21
- LPAR manager Menu screen 10-5
 - adding LPAR 10-6
 - deleting LPAR 10-6
 - displaying guest screen 10-6
 - restarting LPAR 10-6
 - saving configuration information 10-6
 - turning off LPAR 10-6
 - turning on LPAR 10-6
- LPAR manager model 10-92
- LPAR manager screen 10-1
 - Allocated FC Information screen 10-45
 - Date and Time screen 10-63
 - Firmware Version Information screen 10-91
 - Front Panel screen 10-86
 - Logical Partition Configuration screen 10-8
 - Logical Processor Configuration screen 10-20
 - LP Options screen 10-74
 - LP System Logs screen 10-89
 - LPAR manager Menu screen 10-5
 - LPAR Usage screen 10-81
 - operation keys 10-3
 - PCI Device Assignment screen 10-30
 - PCI Device Information screen 10-26
 - Physical Processor Configuration screen 10-23
 - Shared FC Assignment screen 10-42
 - System Configuration screen 10-47
 - System Service State screen 10-58
 - Virtual NIC Assignment screen 10-34
- LPAR manager sub-screens 10-92
- LPAR manager system log messages
 - Error log messages 11-17
 - Information log messages 11-28
 - Warning log messages 11-23
- LPAR manager system time 8-26
- LPAR Usage screen 10-81
 - displaying use status of LPAR manager or each LPAR 10-82
- LPARs 1-2
- LUID mode
 - N+M cold standby 6-22

M

- maintaining the I/O performance by using HBA dedicated core mode 6-20
- management paths 8-3, 8-4, 8-5, 8-6
- memory allocation
 - automatic allocation 5-18
 - by specified memory node 5-18
- Memory Allocation Display sub-screen 10-93
- messages
 - audit logs 11-34
 - HCSM alert 11-72
 - LPAR manager boot messages 11-2
 - LPAR manager screen operation messages 11-7
 - LPAR manager system log messages 11-17

N

- N+M cold standby (LUID mode) 6-22
- names and usages of LPAR manager screen 10-4
- NIC scheduling mode
 - shared NIC 1-7
 - VF NIC 1-7
 - virtual NIC 1-7
- NTP time synchronization 8-29

O

- operating mode 1-4
- OS system time 8-26

P

- packet capturing 6-19
- PCI Device Assignment screen 10-30
 - assigning PCI device to LPAR 10-30
 - changing the USB Auto Attach setting for a specified LPAR 10-30
 - changing scheduling mode of PCI device 10-30
 - switching the LPAR to which the PCI device in exclusively shared mode is attached 10-30
- PCI Device Information screen 10-26
 - checking mapping information about physical PCI device and PCI device on LPAR 10-27
- Physical Processor Configuration screen 10-23
 - adding processor group 10-24
 - changing processor group name 10-24
 - changing processor group number 10-24

- deleting processor group 10-24
- physical RTC time 8-26
- port number
 - LPAR migration E-5
 - management module E-3
 - management server E-2
- promiscuous mode 6-18

R

- reactivating LPAR 4-2
- removing console log data 10-87
- removing guest screen data 10-87
- restoring Migration Failed LPAR 10-87

S

- safe mode 9-21
- scheduling mode 1-4, 8-4
- security 9-5
- SEL time 8-26
- service ratio 1-5
- setting IP address of NTP server 10-65
- Shared FC Assignment screen 10-42
 - changing shared FC assignment 10-42
 - checking shared FC port status 10-42
 - checking WWN of shared FC 10-42
- shared mode 1-3
- specifiable NICs 8-3
- specifying time adjustment settings for NTP 10-65
- SR-IOV 6-2
- synchronizing LPAR time with LPAR manager
- system time 10-65
- System Configuration screen 10-47
 - applying changes to LPAR manager 10-49
 - changing LP ID 10-49
 - changing LPAR manager CLI IP address 10-49
 - changing virtual console port 10-49
 - changing VNIC system number 10-49
- System Service State screen 10-58
 - displaying LPAR manager service status 10-59
 - restoring normal state of LPAR manager system service 10-59
- system unit time 8-26

U

- uninstalling LPAR manager firmware 8-21

- updating LPAR manager firmware 8-21
- Using inter-LPAR communication 6-15

V

- Virtual NIC Assignment screen 10-34
 - changing assignment to LPAR of shared NIC and virtual NIC 10-35
 - changing inter-LPAR communication packet filtering 10-35
 - changing MAC address 10-35
 - changing promiscuous mode 10-35
 - displaying list of VLAN ID assignments and promiscuous mode settings 10-35
- virtual switch images 6-9
- VLAN functionality 6-6
 - Tagged 6-7
 - Undef 6-7
 - Untagged 6-7
- VLAN handling 6-7

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-99CB2500006-26