

ServerView Resource Orchestrator Virtual Edition V3.0.0



Operation Guide

Windows/Linux

J2X1-7605-01ENZ0(05)
April 2012

Preface

Purpose

This manual explains how to operate ServerView Resource Orchestrator (hereinafter Resource Orchestrator).

Target Readers

This manual is written for people who will operate Resource Orchestrator.

An overview of the functions provided in Resource Orchestrator can be found in "Chapter 1 Overview" of the "Setup Guide VE". It is strongly recommended that you read this chapter before using this manual.

Resource Orchestrator allows administrators to choose between two different views according to their level of authority or the kinds of operations that need to be performed. For details, refer to "[Chapter 2 Switching between Views](#)".

Organization

This manual is composed as follows:

Title	Description
Chapter 1 Starting and Stopping	Explains how to start and stop Resource Orchestrator.
Chapter 2 Switching between Views	Provides an overview of the views available in Resource Orchestrator (ROR console and BladeViewer) and explains how to switch between them.
Chapter 3 BladeViewer	Provides an overview of BladeViewer and explains its features.
Chapter 4 User Accounts	Explains the user accounts used in Resource Orchestrator.
Chapter 5 Monitoring	Explains how to monitor the configuration and status of managed resources.
Chapter 6 Power Control	Explains how to remotely control the power state of managed resources.
Chapter 7 Control of VM Environments	Explains the features specific to VM guests and VM hosts.
Chapter 8 Backup and Restore	Explains how to use the backup and restore functions provided in Resource Orchestrator.
Chapter 9 Hardware Maintenance	Explains how to replace hardware and perform maintenance tasks using Resource Orchestrator.
Chapter 10 Server Switchover	Explains how to use the server switchover function.
Chapter 11 Maintaining Software with Cloning [Windows/Linux]	Explains how to perform software maintenance using the cloning function.
Chapter 12 Network Map	Provides an overview of the Network Map and explains its features.
Chapter 13 Collecting Power Consumption Data and Displaying Graphs	Describes the power consumption data collected from power monitoring targets and explains how to export it.
Chapter 14 Customizing the ROR Console	Explains how to customize the ROR console.
Chapter 15 Troubleshooting	Explains how to solve problems and gather troubleshooting data for a technical investigation.
Appendix A Notes on Operating ServerView Resource Orchestrator	Gives important reminders for the operation of Resource Orchestrator.
Appendix B Admin Server Backup and Restore	Explains how to back up and restore the admin server.
Appendix C Event Handling	Explains how to connect events from monitored devices with external applications.

Title	Description
Appendix D Backing Up and Restoring Image Files	Explains how to back up and restore system images and cloning images.
Glossary	Explains the terms used in this manual. Please refer to it when necessary.

Notational Conventions

The notation in this manual conforms to the following conventions.

- When using Resource Orchestrator and the functions necessary differ due to the necessary basic software (OS), it is indicated as follows:

[Windows]	Sections related to Windows (When not using Hyper-V)
[Linux]	Sections related to Linux
[Red Hat Enterprise Linux]	Sections related to Red Hat Enterprise Linux
[Solaris]	Sections related to Solaris
[VMware]	Sections related to VMware
[Hyper-V]	Sections related to Hyper-V
[Xen]	Sections related to Xen
[KVM]	Sections related to RHEL-KVM
[Solaris Containers]	Sections related to Solaris containers
[Windows/Hyper-V]	Sections related to Windows and Hyper-V
[Windows/Linux]	Sections related to Windows and Linux
[Linux/VMware]	Sections related to Linux and VMware
[Linux/Xen]	Sections related to Linux and Xen
[Xen/KVM]	Sections related to Xen and RHEL-KVM
[Linux/Solaris/VMware]	Sections related to Linux, Solaris, and VMware
[Linux/VMware/Xen]	Sections related to Linux, VMware, and Xen
[Linux/Xen/KVM]	Sections related to Linux, Xen, and RHEL-KVM
[VMware/Hyper-V/Xen]	Sections related to VMware, Hyper-V, and Xen
[Linux/Solaris/VMware/Xen]	Sections related to Linux, Solaris, VMware, and Xen
[Linux/VMware/Xen/KVM]	Sections related to Linux, VMware, Xen, and RHEL-KVM
[VMware/Hyper-V/Xen/KVM]	Sections related to VMware, Hyper-V, Xen, and RHEL-KVM
[Linux/Solaris/VMware/Xen/KVM]	Sections related to Linux, Solaris, VMware, Xen, and RHEL-KVM
[VM host]	Sections related to VMware, Windows Server 2008 with Hyper-V enabled, Xen, RHEL-KVM, and Solaris containers

- Unless specified otherwise, the blade servers mentioned in this manual refer to PRIMERGY BX servers.
- Oracle Solaris may also be indicated as Solaris, Solaris Operating System, or Solaris OS.
- References and character strings or values requiring emphasis are indicated using double quotes (").
- Window names, dialog names, menu names, and tab names are shown enclosed by brackets ([]).
- Button names are shown enclosed by angle brackets (< >) or square brackets ([]).
- The order of selecting menus is indicated using []-[] .
- Text to be entered by the user is indicated using bold text.

- Variables are indicated using italic text and underscores.
- The ellipses ("...") in menu names, indicating settings and operation window startup, are not shown.

Menus in the ROR console

Operations on the ROR console can be performed using either the menu bar or pop-up menus. By convention, procedures described in this manual only refer to pop-up menus.

Documentation Road Map

The following manuals are provided with Resource Orchestrator. Please refer to them when necessary:

Manual Name	Abbreviated Form	Purpose
ServerView Resource Orchestrator Virtual Edition V3.0.0 Setup Guide	Setup Guide VE	Please read this first. Read this when you want information about the purposes and uses of basic functions, and how to install Resource Orchestrator.
ServerView Resource Orchestrator Virtual Edition V3.0.0 Installation Guide	Installation Guide VE	Read this when you want information about how to install Resource Orchestrator.
ServerView Resource Orchestrator Virtual Edition V3.0.0 Operation Guide	Operation Guide VE	Read this when you want information about how to operate systems that you have configured.
ServerView Resource Orchestrator Virtual Edition V3.0.0 User's Guide	User's Guide VE	Read this when you want information about how to operate the GUI.
ServerView Resource Orchestrator Virtual Edition V3.0.0 Command Reference	Command Reference	Read this when you want information about how to use commands.
ServerView Resource Orchestrator Virtual Edition V3.0.0 Messages	Messages VE	Read this when you want detailed information about the corrective actions for displayed messages.

Related Documentation

Please refer to these manuals when necessary.

- ETERNUS SF Storage Cruiser User's Guide

Abbreviations

The following abbreviations are used in this manual:

Abbreviation	Products
Windows	Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Windows(R) 7 Professional Windows(R) 7 Ultimate Windows Vista(R) Business

Abbreviation	Products
	Windows Vista(R) Enterprise Windows Vista(R) Ultimate Microsoft(R) Windows(R) XP Professional operating system
Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter
Windows 2008 x86 Edition	Microsoft(R) Windows Server(R) 2008 Standard (x86) Microsoft(R) Windows Server(R) 2008 Enterprise (x86)
Windows 2008 x64 Edition	Microsoft(R) Windows Server(R) 2008 Standard (x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x64)
Windows Server 2003	Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
Windows 2003 x64 Edition	Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
Windows 7	Windows(R) 7 Professional Windows(R) 7 Ultimate
Windows Vista	Windows Vista(R) Business Windows Vista(R) Enterprise Windows Vista(R) Ultimate
Windows XP	Microsoft(R) Windows(R) XP Professional operating system
Windows PE	Microsoft(R) Windows(R) Preinstallation Environment
Linux	Red Hat(R) Enterprise Linux(R) AS (v.4 for x86) Red Hat(R) Enterprise Linux(R) ES (v.4 for x86) Red Hat(R) Enterprise Linux(R) AS (v.4 for EM64T) Red Hat(R) Enterprise Linux(R) ES (v.4 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.5 for x86) Red Hat(R) Enterprise Linux(R) ES (4.5 for x86) Red Hat(R) Enterprise Linux(R) AS (4.5 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.5 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.6 for x86) Red Hat(R) Enterprise Linux(R) ES (4.6 for x86) Red Hat(R) Enterprise Linux(R) AS (4.6 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.6 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.7 for x86) Red Hat(R) Enterprise Linux(R) ES (4.7 for x86) Red Hat(R) Enterprise Linux(R) AS (4.7 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.7 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.8 for x86) Red Hat(R) Enterprise Linux(R) ES (4.8 for x86) Red Hat(R) Enterprise Linux(R) AS (4.8 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.8 for EM64T) Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86)

Abbreviation	Products
	<p>Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 6 (for x86) Red Hat(R) Enterprise Linux(R) 6 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.1 (for x86) Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64) SUSE(R) Linux Enterprise Server 10 Service Pack2 for x86 SUSE(R) Linux Enterprise Server 10 Service Pack2 for EM64T SUSE(R) Linux Enterprise Server 10 Service Pack3 for x86 SUSE(R) Linux Enterprise Server 10 Service Pack3 for EM64T SUSE(R) Linux Enterprise Server 11 for x86 SUSE(R) Linux Enterprise Server 11 for EM64T SUSE(R) Linux Enterprise Server 11 Service Pack1 for x86 SUSE(R) Linux Enterprise Server 11 Service Pack1 for EM64T Oracle Enterprise Linux Release 5 Update 4 for x86 (32 Bit) Oracle Enterprise Linux Release 5 Update 4 for x86_64 (64 Bit) Oracle Enterprise Linux Release 5 Update 5 for x86 (32 Bit) Oracle Enterprise Linux Release 5 Update 5 for x86_64 (64 Bit)</p>
Red Hat Enterprise Linux	<p>Red Hat(R) Enterprise Linux(R) AS (v.4 for x86) Red Hat(R) Enterprise Linux(R) ES (v.4 for x86) Red Hat(R) Enterprise Linux(R) AS (v.4 for EM64T) Red Hat(R) Enterprise Linux(R) ES (v.4 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.5 for x86) Red Hat(R) Enterprise Linux(R) ES (4.5 for x86) Red Hat(R) Enterprise Linux(R) AS (4.5 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.5 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.6 for x86) Red Hat(R) Enterprise Linux(R) ES (4.6 for x86) Red Hat(R) Enterprise Linux(R) AS (4.6 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.6 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.7 for x86) Red Hat(R) Enterprise Linux(R) ES (4.7 for x86) Red Hat(R) Enterprise Linux(R) AS (4.7 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.7 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.8 for x86) Red Hat(R) Enterprise Linux(R) ES (4.8 for x86) Red Hat(R) Enterprise Linux(R) AS (4.8 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.8 for EM64T) Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86)</p>

Abbreviation	Products
	Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 6 (for x86) Red Hat(R) Enterprise Linux(R) 6 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.1 (for x86) Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)
Red Hat Enterprise Linux 5	Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64)
Red Hat Enterprise Linux 6	Red Hat(R) Enterprise Linux(R) 6 (for x86) Red Hat(R) Enterprise Linux(R) 6 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.1 (for x86) Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)
RHEL-KVM	Red Hat(R) Enterprise Linux(R) 6.1 (for x86) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64) Virtual Machine Function
Xen	Citrix XenServer(TM) 5.5 Citrix Essentials(TM) for XenServer 5.5, Enterprise Edition Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Linux Virtual Machine Function
DOS	Microsoft(R) MS-DOS(R) operating system, DR DOS(R)
SUSE Linux Enterprise Server	SUSE(R) Linux Enterprise Server 10 Service Pack2 for x86 SUSE(R) Linux Enterprise Server 10 Service Pack2 for EM64T

Abbreviation	Products
	SUSE(R) Linux Enterprise Server 10 Service Pack3 for x86 SUSE(R) Linux Enterprise Server 10 Service Pack3 for EM64T SUSE(R) Linux Enterprise Server 11 for x86 SUSE(R) Linux Enterprise Server 11 for EM64T SUSE(R) Linux Enterprise Server 11 Service Pack1 for x86 SUSE(R) Linux Enterprise Server 11 Service Pack1 for EM64T
Oracle Enterprise Linux	Oracle Enterprise Linux Release 5 Update 4 for x86 (32 Bit) Oracle Enterprise Linux Release 5 Update 4 for x86_64 (64 Bit) Oracle Enterprise Linux Release 5 Update 5 for x86 (32 Bit) Oracle Enterprise Linux Release 5 Update 5 for x86_64 (64 Bit)
Solaris	Solaris(TM) 10 Operating System
VMware	VMware(R) Infrastructure 3 VMware vSphere(R) 4 VMware vSphere(R) 4.1 VMware vSphere(R) 5
VIOM	ServerView Virtual-IO Manager
ServerView Agent	ServerView SNMP Agents for MS Windows (32bit-64bit) ServerView Agents Linux ServerView Agents VMware for VMware ESX Server
Excel	Microsoft(R) Office Excel(R) 2010 Microsoft(R) Office Excel(R) 2007 Microsoft(R) Office Excel(R) 2003
Excel 2010	Microsoft(R) Office Excel(R) 2010
Excel 2007	Microsoft(R) Office Excel(R) 2007
Excel 2003	Microsoft(R) Office Excel(R) 2003
ROR VE	ServerView Resource Orchestrator Virtual Edition
ROR CE	ServerView Resource Orchestrator Cloud Edition
Resource Coordinator	Systemwalker Resource Coordinator
Resource Coordinator VE	ServerView Resource Coordinator VE Systemwalker Resource Coordinator Virtual server Edition
Resource Orchestrator	ServerView Resource Orchestrator

Export Administration Regulation Declaration

Documents produced by FUJITSU may contain technology controlled under the Foreign Exchange and Foreign Trade Control Law of Japan. Documents which contain such technology should not be exported from Japan or transferred to non-residents of Japan without first obtaining authorization from the Ministry of Economy, Trade and Industry of Japan in accordance with the above law.

Trademark Information

- BMC, BMC Software, and the BMC Software logo are trademarks or registered trademarks of BMC Software, Inc. in the United States and other countries.
- Citrix(R), Citrix XenServer(TM), Citrix Essentials(TM), and Citrix StorageLink(TM) are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.
- Dell is a registered trademark of Dell Computer Corp.
- HP is a registered trademark of Hewlett-Packard Company.
- IBM is a registered trademark or trademark of International Business Machines Corporation in the U.S.

- Linux is a trademark or registered trademark of Linus Torvalds in the United States and other countries.
- Microsoft, Windows, MS, MS-DOS, Windows XP, Windows Server, Windows Vista, Windows 7, Excel, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates in the United States and other countries.
- Oracle is a registered trademark of Oracle Corporation and/or its affiliates.
- Red Hat, RPM and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.
- Spectrum is a trademark or registered trademark of Computer Associates International, Inc. and/or its subsidiaries.
- SUSE is a registered trademark of SUSE LINUX AG, a Novell business.
- VMware, the VMware "boxes" logo and design, Virtual SMP, and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
- ServerView and Systemwalker are registered trademarks of FUJITSU LIMITED.
- All other brand and product names are trademarks or registered trademarks of their respective owners.

Notices

- The contents of this manual shall not be reproduced without express written permission from FUJITSU LIMITED.
- The contents of this manual are subject to change without notice.

Month/Year Issued, Edition	Manual Code
November 2011, First Edition	J2X1-7605-01ENZ0(00)
December 2011, 1.1	J2X1-7605-01ENZ0(01)
December 2011, 1.2	J2X1-7605-01ENZ0(02)
February 2012, 1.3	J2X1-7605-01ENZ0(03)
March 2012, 1.4	J2X1-7605-01ENZ0(04)
April 2012, 1.5	J2X1-7605-01ENZ0(05)

Copyright FUJITSU LIMITED 2010-2012

Contents

Chapter 1 Starting and Stopping.....	1
Chapter 2 Switching between Views.....	2
Chapter 3 BladeViewer.....	3
3.1 Overview.....	3
3.2 Login and Logout.....	4
3.3 Screen Layout.....	5
3.4 Resource Status Monitoring.....	6
3.4.1 Status Panel.....	6
3.4.2 Chassis Panel.....	7
3.4.3 Blade Panel.....	8
3.4.3.1 Resource List.....	8
3.4.3.2 VM Guest List.....	11
3.4.4 Resource Details.....	13
3.5 Power Control.....	13
3.5.1 Server Blade.....	13
3.5.2 VM guest.....	15
3.6 Status Panel Operations.....	16
3.6.1 Listing and Editing of Labels and Comments.....	17
3.6.2 Editing Contacts.....	18
3.6.3 Changing Passwords.....	18
Chapter 4 User Accounts.....	20
4.1 Overview.....	20
4.2 Managing User Accounts.....	20
Chapter 5 Monitoring.....	23
5.1 Overview.....	23
5.2 Resource Status.....	24
5.3 Addressing Resource Failures.....	26
Chapter 6 Power Control.....	28
6.1 Server Power Control.....	28
6.2 Chassis Power Control.....	29
Chapter 7 Control of VM Environments.....	30
7.1 Migration of VM Guests between Servers.....	30
7.2 VM Maintenance Mode of VM Hosts.....	31
7.3 VM Home Position.....	31
7.3.1 Setting VM Home Position.....	31
7.3.2 Migrating to VM Home Position.....	32
7.3.3 Clearing VM Home Position.....	32
Chapter 8 Backup and Restore.....	33
8.1 Overview.....	33
8.2 Backup.....	34
8.3 Restoring System Images.....	36
8.4 Viewing System Images.....	38
8.5 Deleting System Images.....	38
Chapter 9 Hardware Maintenance.....	40
9.1 Overview.....	40
9.2 Maintenance LEDs.....	41
9.3 Re-configuring Hardware Properties.....	42
9.4 Replacing Servers.....	44
9.5 Replacing and Adding Server Components.....	50

9.6 Replacing Non-server Hardware.....	51
Chapter 10 Server Switchover.....	54
10.1 Overview.....	54
10.2 Switchover.....	54
10.3 Post-Switchover Operations.....	56
Chapter 11 Maintaining Software with Cloning [Windows/Linux].....	59
11.1 Overview.....	59
11.2 Software Maintenance Procedure.....	59
Chapter 12 Network Map.....	61
12.1 Overview.....	61
12.2 Preparations.....	62
12.3 Screen Layout.....	63
12.3.1 Network Map Layout.....	63
12.3.2 Map Types.....	64
12.4 Resource Icons.....	65
12.4.1 Resource Statuses.....	65
12.4.2 VLAN Display.....	69
12.4.3 Other Icons.....	70
12.5 Network Links.....	71
12.5.1 Link Display.....	71
12.5.2 Link Statuses.....	71
12.5.3 Aggregate Display of Network Links.....	71
12.6 Display Filters.....	72
Chapter 13 Collecting Power Consumption Data and Displaying Graphs.....	74
13.1 Overview.....	74
13.2 Exporting Power Consumption Data.....	74
13.3 Power Consumption Data File (CSV Format).....	76
13.4 Displaying Power Consumption Data Graphs.....	78
Chapter 14 Customizing the ROR Console.....	81
14.1 Dialogs.....	81
14.2 External Software.....	81
Chapter 15 Troubleshooting.....	83
15.1 Types of Troubleshooting Data.....	83
15.1.1 Collecting Initial Troubleshooting Data.....	83
15.1.2 Collecting Exhaustive Troubleshooting Data.....	87
15.2 OS Startup Issues (with I/O Virtualization).....	88
15.3 "unknown" Server Status.....	89
15.4 Image Operation Issues [Windows/Linux] [Hyper-V].....	91
15.5 Public LAN Communication Issues.....	92
15.6 Multipath Configuration Issues.....	92
15.7 Cloning Issues Following Manager Re-installation.....	92
15.8 Server Switchover and Failback Issues.....	95
15.9 HBA Address Rename is Set by Mistake.....	95
15.10 Boot Issues (Boot Order Related).....	96
15.11 Boot Issues (Endless Reboot Cycle).....	96
15.12 When the Display of Resource Information in the [Resource] Tab of the ROR Console Collapses.....	96
Appendix A Notes on Operating ServerView Resource Orchestrator.....	97
Appendix B Admin Server Backup and Restore.....	101
B.1 Overview.....	101
B.1.1 Managed Resources and Update Timing.....	101
B.1.2 Backup.....	102

B.1.3 Restoring the Admin Server.....	102
B.1.4 Backup and Restore Commands.....	103
B.2 Backup.....	103
B.2.1 Backing Up All Management Information.....	105
B.2.2 Backing up Configuration Definition Information.....	107
B.3 Restore.....	107
Appendix C Event Handling.....	112
Appendix D Backing Up and Restoring Image Files.....	116
D.1 Configuration of Folders and Files.....	116
D.2 Backing Up Image Files.....	117
D.3 Restoring Image Files.....	117
Glossary.....	119

Chapter 1 Starting and Stopping

This chapter explains how to start and stop Resource Orchestrator.

To use Resource Orchestrator, first open the ROR console or BladeViewer from an admin client.

Refer to "1.1 ROR Console Layout" of the "User's Guide VE" for details on opening and closing the ROR console.

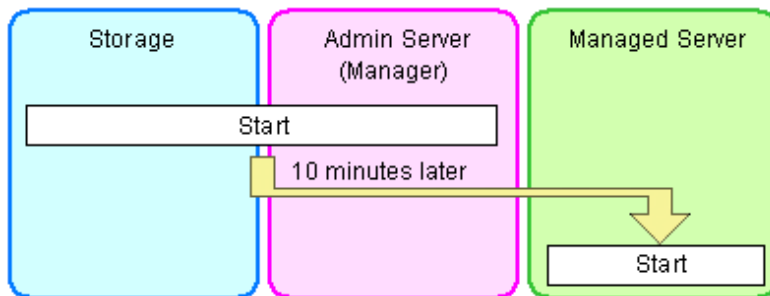
For details on opening and closing BladeViewer, refer to "3.2 Login and Logout".

To use Resource Orchestrator, both the manager and agents must be running. The manager and agent services are configured to start automatically upon startup of their respective servers (admin server, managed server). Normally, there should be no need to manually start or stop either the manager or agents. To start or stop a manager or an agent intentionally, refer to "7.2 Starting and Stopping the Manager" and "7.3 Starting and Stopping the Agent" of the "Setup Guide VE".

Note

When using the HBA address rename function, ensure that the manager is started before starting any managed servers. The power on procedure should be managed as follows: first, start the admin server together with any storage devices, and start the managed servers 10 minutes later.

Managed servers will not boot up properly if they are started before the manager. Make sure that the manager is running before starting managed servers.



Additionally, when using the HBA address rename function, the HBA address rename setup service should be started on a dedicated server (HBA address rename server) and left running continuously. For details on starting, stopping, and confirming the state of the HBA address rename setup service, refer to "8.2.1 Settings for the HBA address rename Setup Service" of the "Setup Guide VE".

Chapter 2 Switching between Views

This chapter provides an overview of the two views available in Resource Orchestrator and explains how to switch between them.

Resource Orchestrator allows administrators to choose between the following two GUIs: the ROR console and BladeViewer. Choosing an appropriate GUI depends on the administrator's authority level, or the kind of operations to be performed.

- ROR console

The ROR console gives access to all functions of Resource Orchestrator.

- BladeViewer

BladeViewer offers a simplified, lifelike representation of blade servers and their statuses. While this enables intuitive operation, it does not include the tree-based navigation or detailed menus available in the ROR console.

BladeViewer makes it easier to monitor blade servers, visualize their hosted applications, and perform power operations. This makes BladeViewer suitable for administrators who only need to monitor blades and perform basic operations.

To switch from the ROR console to BladeViewer, click <BladeViewer>>>. To switch from BladeViewer to the ROR console, click <Advanced>>>.



Information

- For details on the ROR console, refer to "Chapter 1 User Interface" of the "User's Guide VE".
- For details on BladeViewer, refer to "[Chapter 3 BladeViewer](#)". This explains the BladeViewer screen and the functions that it provides.
- When logging in for the first time, the ROR console is displayed.
Otherwise, the last view used before logging out (either the ROR console or BladeViewer) is displayed.

Chapter 3 BladeViewer

This chapter provides an overview of BladeViewer and explains its features.

Please note that BladeViewer is only available for PRIMERGY BX servers.

Note

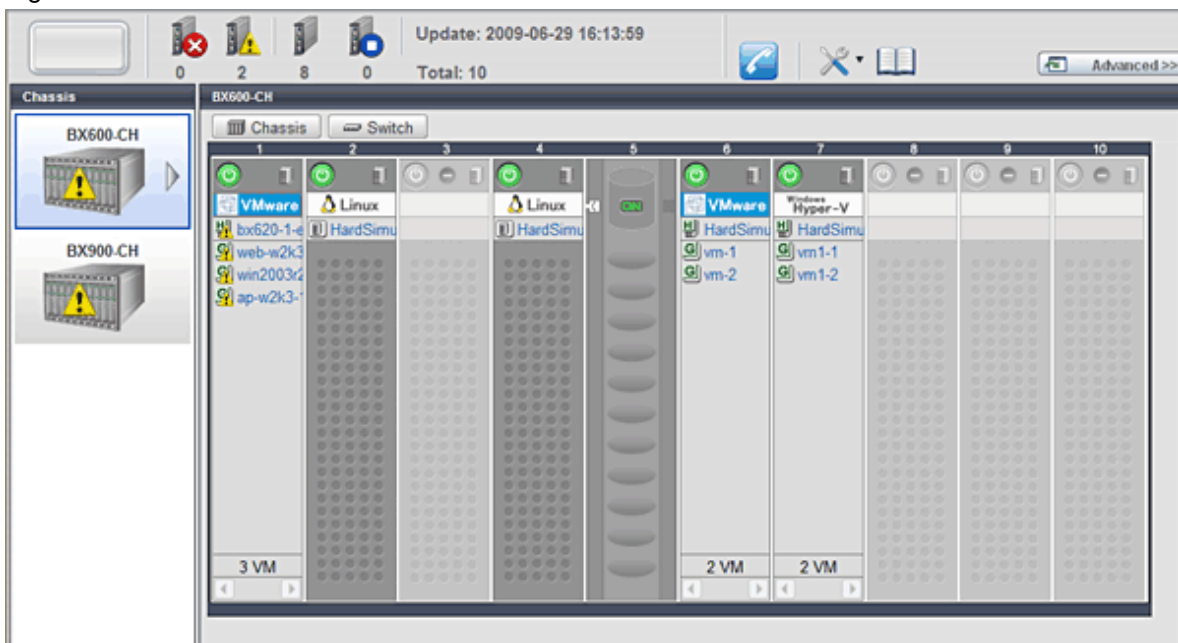
- When accessing the ROR console using Internet Explorer 8 or 9, be sure to enable the Compatibility View in Internet Explorer.
- BladeViewer uses the standard Web browser font, and is optimized for a window size of 1024 by 768 pixels. If the Web browser is resized by a significant amount, the display quality may deteriorate.
- BladeViewer uses JavaScript, Cookies, and IFRAME. Therefore, those features should be enabled beforehand in the Web browser settings.

3.1 Overview

This section provides a functional overview of BladeViewer.

BladeViewer provides an intuitive representation of blade servers and their statuses. This makes it easier to monitor resource states or perform basic operations on blade servers.

Figure 3.1 BladeViewer



BladeViewer allows the following operations:

- Monitoring of resource statuses

The statuses of chassis, servers, LAN switches, and physical OS's can be monitored from a view representative of the actual placement and configuration of physical devices.

When using virtual servers, BladeViewer shows a list of VM guests for each VM host. This helps keeping track of relationships between VM guests and VM hosts.

BladeViewer also makes it easy to confirm which operating systems (physical OS and guest OS) are affected by a hardware failure.

- Display and control of power status

The power status of each server blade, storage blade, and VM guest is represented by an intuitive power button. Clicking this button provides quick access to power control operations (for both server blades and VM guests).

- Display of custom labels and comments

BladeViewer allows users to define custom labels and comments for each physical OS, VM host, and VM guest.

Once defined, labels are shown on top of each displayed physical OS, VM host, and VM guest. Using labels to display application contents makes it easy to visualize what applications are running on each server blade and identify the applications affected by a server failure.

Clicking on a label displays the comment defined for the related resource. Registering troubleshooting and recovery procedures beforehand can speed up the recovery of affected applications when a problem occurs.

- Display of contact information

BladeViewer allows users to define technical (support) contact information for their entire IT system. This contact information can be shown by clicking on the Contact icon.

Registering contact details of technical support staff beforehand can help streamline recovery procedures when problems occur.

3.2 Login and Logout

This section explains how to log in and out of BladeViewer.

Login

Start a Web browser from an admin client and specify the URL of the ROR console for connection. If the port number was changed, specify the new port number.

```
https://Admin_server_IP_address:23461/
```

On a Windows admin server, the ROR console can also be opened by selecting [start]-[All Programs]-[Resource Orchestrator]-[ROR console]. If you are already logged in on a separate Web browser instance, login may be performed automatically without the login screen being displayed.



- If the login screen is not displayed, confirm the following.
 - The correct URL was entered.
 - The proxy settings of the Web browser are correct.
 - The firewall settings on the admin server are correct.
- When opening the ROR console right after launching a Web browser, a warning window concerning the site's security certificate will be displayed.

With Internet Explorer 8, or 9, the following message is displayed: "There is a problem with this web site's security certificate.". This warns the user that Resource Orchestrator uses a self-signed certificate to encrypt its HTTPS (SSL) communication with the Web browser.

Resource Orchestrator generates a unique, self-signed certificate for each admin server during manager installation.

Within a firewall-protected intranet, a network where the risk of identity theft is low, or where all correspondents are trusted, there is no risk in using self-signature certificates for communications. Accept the warning to display the Resource Orchestrator login screen.

With Internet Explorer 8, or 9, the login screen can be displayed by selecting the following option: "Continue to this web site (not recommended).".
- When connecting to the manager from Internet Explorer 8 or 9, the background of the address bar will become red and the words "Certificate Error" will be displayed on the right side of the address bar of the login screen, the ROR console, and BladeViewer. Furthermore, the Phishing Filter may show a warning on the status bar. These warnings are referring to the same self-signed certificate issue discussed in the previous bullet. It is safe to continue with the current browser settings.
- To stop displaying the security certificate warning screen and the certificate error icon, create a certificate associated with the IP address or hostname of the admin server and add it to the Web browser.

Refer to "Appendix B HTTPS Communications" of the "Setup Guide VE" for details.
- If already logged in from another Web browser window, login may be performed automatically (without displaying the login screen).

- When using Internet Explorer, add the URL of the ROR console to the browser's "Trusted sites".

In the login screen, enter the following items, and click <Login>.

If the login is successful, either BladeViewer or the ROR console is displayed.

- User ID
- Password

However, opening multiple Web browsers from an already opened browser window (e.g. using the [File]-[New Window] menu from a Web browser) may disable logging in as a different user.

To log in as a different user, start up a new Web browser from the Windows start menu.

Information

- At installation, enter the name and password of the user account specified in "2.1 Manager Installation" of the "Installation Guide VE".
- When logging in for the first time, the ROR console is displayed. Otherwise, the last view used before logging out (either the ROR console or BladeViewer) is displayed.
- Clicking <BladeViewer>>> on the ROR console will switch over to the BladeViewer view.

Logout

To log out of BladeViewer, click the "Logout" button text link displayed on the upper-right of the BladeViewer screen.

Note

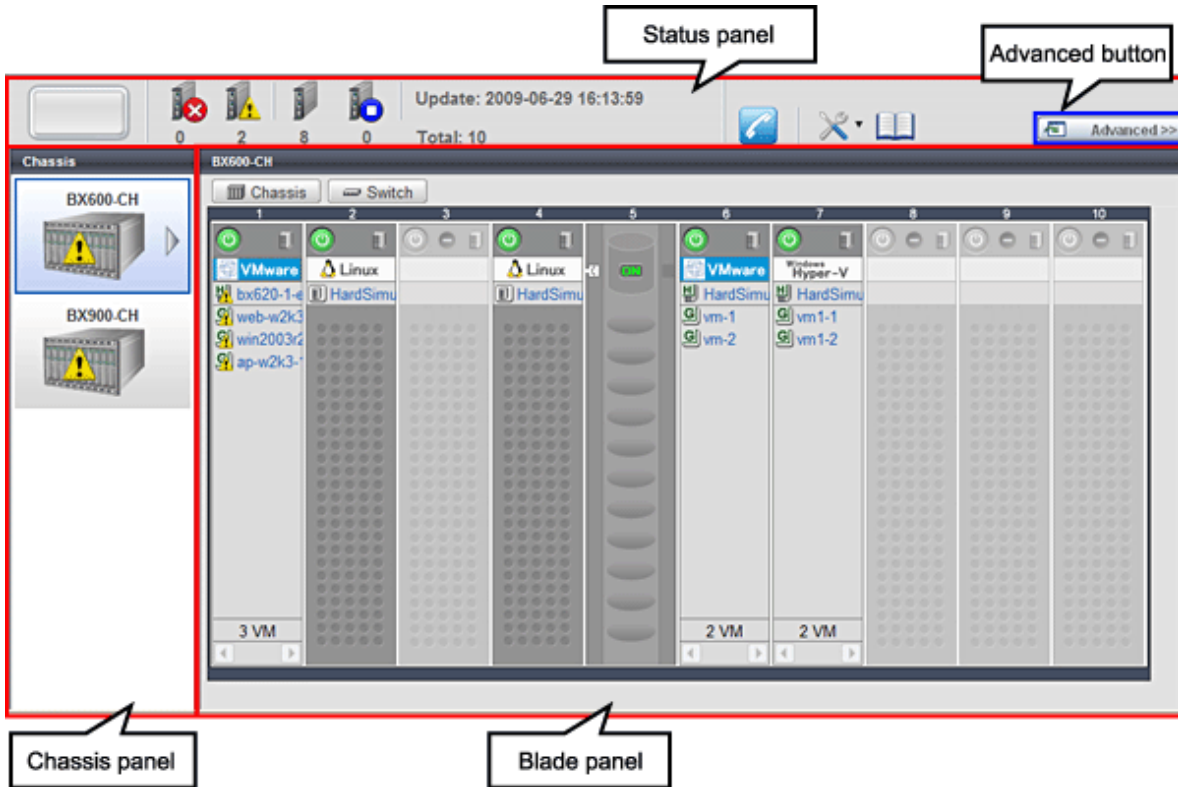
- If the Web browser is closed without logging out first, user authentication may be skipped the next time Resource Orchestrator is accessed. In that case, users will be automatically logged in using the previously used session. It is advised that the users log out properly after using the ROR console or BladeViewer.
- If the ROR console or BladeViewer has been opened simultaneously in several Web browser windows, those login sessions may be terminated.

3.3 Screen Layout

This section explains how the BladeViewer screen is organized.

The BladeViewer screen consists of a status panel, a chassis panel, and a blade panel.

Figure 3.2 BladeViewer: Screen Layout



Status panel

This panel displays a summary of resources statuses.

Chassis panel

This panel displays the statuses of each registered chassis.

Blade panel

This panel displays the status of all resources mounted within the selected chassis.

Information

To switch from BladeViewer to the ROR console, click <Advanced>>>, which is displayed in the upper-right of the BladeViewer screen. Switch to the ROR console when necessary, for example to register servers and change various settings. Otherwise, the last view used before logging out (either the ROR console or BladeViewer) is displayed.

3.4 Resource Status Monitoring

This section explains how to monitor resource statuses using BladeViewer.

3.4.1 Status Panel

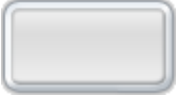


The status panel displays a summary of resources statuses (including resources other than PRIMERGY BX servers).

When a problem occurs in the system, a red or yellow light icon starts blinking on the left side of the status panel.

Clicking the light icon changes its color back to gray.

The table below shows the status and meaning associated with each light icon.

Table 3.1 Light Icons

Icon	Color	Status	Meaning
	Gray (not lit)	Normal	No errors or warnings have been detected in the system.
	Yellow (blinking)	Warning	A warning has been detected in the system.
	Red (blinking)	Error	An error has been detected in the system.


 Information

When the light icon blinks, it means that a warning or an error has been detected. Check the location of the problem from the chassis or blade panel.

If BladeViewer shows no resources with a warning or error status in either the chassis panel or blade panel, switch to the ROR console and check the event log to identify the cause of the problem.




To the right of the light icon, BladeViewer shows the number of servers with an "error", "warning", "normal", and "stop" status.

Table 3.2 Displaying the Server Icon and the Number of Units

Icon and number of units	Meaning
 N(*1)	Server and number of units

*1: N is the number of servers.


Table 3.3 Status Icons

Icon	Status	Meaning
	Normal	The resource can be used normally.
	Warning	An error occurred, however the resource can be used. Alternatively, the status of some resources cannot be obtained.
	Error	A fault or error occurred, therefore the resource cannot be used.
	Stop	The resource is stopped, therefore it cannot be used.

3.4.2 Chassis Panel

The chassis panel displays the statuses of each registered chassis.

Table 3.4 Chassis Icon

Icon	Meaning
	Chassis

See

For details on the different chassis statuses, refer to "[Table 3.3 Status Icons](#)" of "[3.4.1 Status Panel](#)".

If a chassis icon shows a warning or error status, it means that a problem occurred in a resource contained in the chassis.

For details on how to identify faulty resources, refer to "[3.4.3 Blade Panel](#)".

Information

Selecting a chassis icon from the chassis panel displays the contents of that chassis in the blade panel.

For details, refer to "[3.4.3 Blade Panel](#)".

3.4.3 Blade Panel

The blade panel displays the statuses of all the resources inserted into the selected chassis. Those resources are shown in a format representative of their physical configuration (shape and position).

To display the contents of a specific chassis in the blade panel, click on its icon in the chassis panel.

In the blade panel, the selected chassis and its LAN switches are represented by the following icons. Those icons are displayed in the upper-part of the blade panel.

Table 3.5 Chassis Icon



Icon	Meaning
	Chassis

Table 3.6 LAN Switch Icon

Icon	Meaning
	LAN switch

See

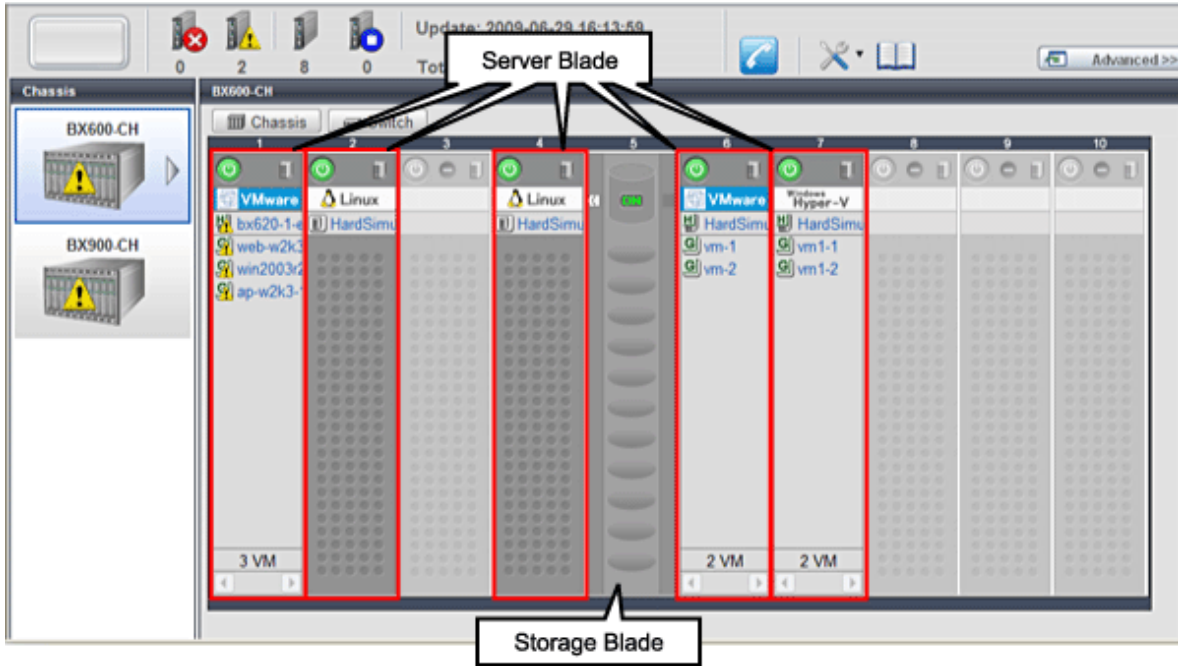
For details on the status icons that are displayed for the chassis and its LAN switches, refer to "[Table 3.3 Status Icons](#)" of "[3.4.1 Status Panel](#)".

3.4.3.1 Resource List

The blade panel graphically displays each slot within a chassis. Each server or storage blade is displayed according to their actual position (slot) within the chassis.

Note that an unregistered server is shown in light gray while an empty slot is shown in white.





Figure 3.3 Blade Panel: Resource List



Server Blade

A power button is displayed in the upper-part of each server blade. This power button is used to represent the power status of each server, as shown below.

Table 3.7 Server Blade Power Buttons





Power button	Color	Status	Meaning
	Green (lit)	Power ON	Power ON status.
	Gray (not lit)	Power OFF	Power OFF status.
	Green (blinking)	Power ON in progress	Power ON or reboot in progress.
	Orange (blinking)	Power OFF in progress	Power OFF in progress.

Information

The power status of a server blade can be easily controlled by clicking on its power button. For details, refer to "3.5.1 Server Blade".

A physical server icon is displayed on the right side of the server blade power button. The table below shows the meanings associated with each physical server icon.

Table 3.8 Physical Server Icons


Icon	Meaning
	Server
	Spare server
	Unregistered server
	Maintenance mode server

 See

For details on the different physical server statuses, refer to "Table 3.3 Status Icons" in "3.4.1 Status Panel".





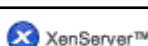
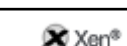

When a server blade is used as the admin server, the following admin server icon is displayed.

Table 3.9 Admin Server Icon

Icon	Status	Meaning
	Admin server	Indicates the server used as the admin server.

An OS icon is displayed below the physical server icon.
The table below shows the meaning of each OS icon.

Table 3.10 OS Icons

Icon	Meaning
	Windows OS
	Linux OS
	VMware host OS
	Hyper-V host OS
	Citrix XenServer host OS
	Linux Xen host OS
	KVM host OS

 Information

Clicking on a VM host OS icon displays a detailed list of the VM guests operating on the selected VM host.
For details, refer to "3.4.3.2 VM Guest List".

A user-defined label is displayed with a resource icon below the OS icon.




- If no label is set
The OS name is displayed.

- If the OS name cannot be acquired (because the OS has not been installed or for other reasons)

The server name (physical server name or VM guest name) is displayed.

The following table shows the resource icons used in BladeViewer and their associated meanings.

Table 3.11 Resource Icons

Icon	Meaning
	Physical OS
	VM host
	VM guest



See

For details on the resource status, refer to "Table 3.3 Status Icons" in "3.4.1 Status Panel".



Information

If a comment has been defined for a server, clicking on its label displays the [Server Properties] dialog.

The [Server Properties] dialog displays the comment and label set for the selected server, as well as its OS name, server name (for a physical OS, the physical server name, for a VM guest, the VM guest name), and IP address.



For details on defining comments, refer to "3.6.1 Listing and Editing of Labels and Comments".

Storage Blade

A power lamp is displayed in the top part of each storage blade.

The table below shows the status and meaning associated with each power lamp.

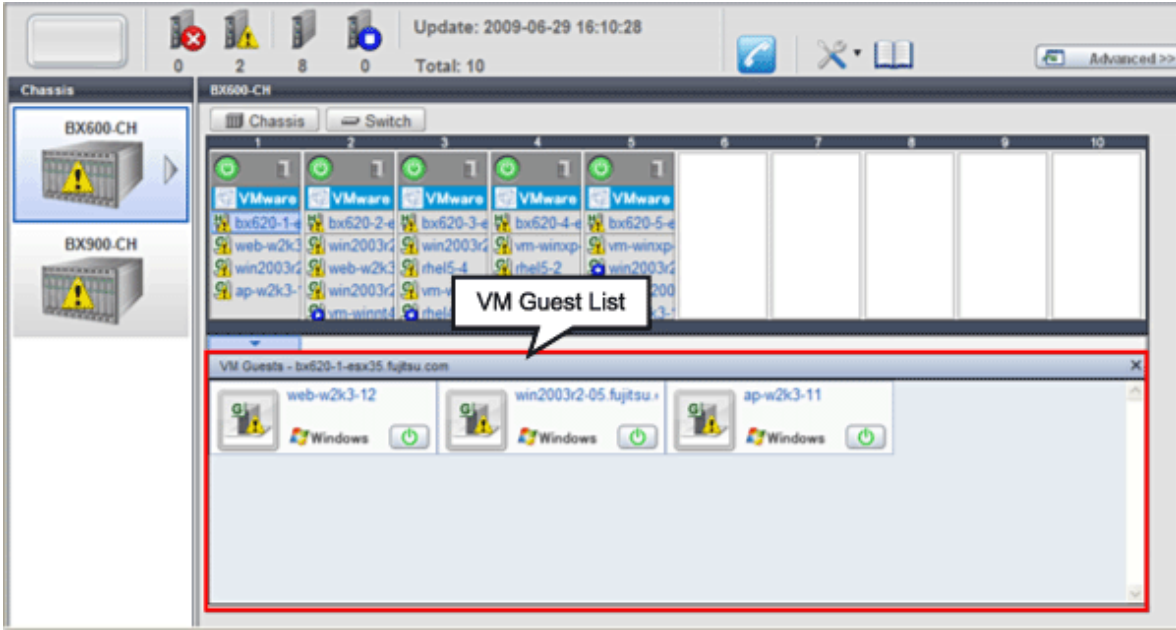
Table 3.12 Storage Blade Power Lamps

Power lamp	Color	Status	Meaning
	Green (lit)	Power ON	Power ON status.
	Gray (not lit)	Power OFF	Power OFF status.

3.4.3.2 VM Guest List


When a VM host is displayed in the blade panel, clicking the VM host OS icon displays a list of hosted VM guests with their statuses.

Figure 3.4 Blade Panel: VM Guest List



A VM guest icon is shown on the left side of each VM guest displayed in the VM guest list.

Table 3.13 VM Guest Icon

Icon	Meaning
	VM guest

 See

For details on the different VM guest statuses, refer to "Table 3.3 Status Icons" in "3.4.1 Status Panel".

A user-defined label is displayed on the upper-right side of the VM guest icon.

- If no label is set
The OS name is displayed.
- If the OS name cannot be acquired (because the OS has not been installed or for other reasons)
The VM guest name is displayed.




An OS icon is displayed below the label.


For details on the different OS icons, refer to "Table 3.10 OS Icons" in "3.4.3.1 Resource List".

A power button is displayed on the lower-right side of each VM guest.

This power button represents the power status of each VM guest, as shown below.

Table 3.14 VM Guest Power Buttons

Power button	Color	Status	Meaning
	Green (lit)	Power ON	Power ON status.
	Gray (not lit)	Power OFF	Power OFF status.
	Green (blinking)	Power ON in progress	Power ON or reboot in progress.

Power button	Color	Status	Meaning
	Orange (blinking)	Power OFF in progress	Power OFF in progress.

Information

The power status of a VM guest can be easily controlled by clicking on its power button. Refer to "[3.5.2 VM guest](#)" for details.

3.4.4 Resource Details

To view a resource's details, click on its icon (chassis, LAN switch, or physical server icon) from the blade panel.

- Chassis

Clicking a chassis icon (from the blade panel) opens up its management blade's Web interface in a new window. This Web interface provides more details on the chassis' status and contents. For details on the chassis icon, refer to "[3.4.3 Blade Panel](#)".

- LAN switch

Clicking on a LAN switch icon opens up its LAN switch details screen. This screen provides more details on the LAN switch's status and configuration. For details on the LAN switch icon, refer to "[3.4.3 Blade Panel](#)".

- Physical server

Clicking on a physical server icon opens it up in the ServerView Operation Manager's Web interface. This interface provides more details on the physical server's status and its internal components. For details on the physical server icon, refer to "[Table 3.8 Physical Server Icons](#)" in "[3.4.3.1 Resource List](#)".



3.5 Power Control

This section explains how to control the power status of server blades and VM guests from BladeViewer.

3.5.1 Server Blade

The power status of a server blade can be easily controlled by clicking its power button.

Table 3.15 Actions of Server Blade Power Buttons

Power button	Color	Status	Action
	Gray (not lit)	Power OFF	Powers on a server blade.
	Green (lit)	Power ON	Shuts down or reboots a server blade.

Power On

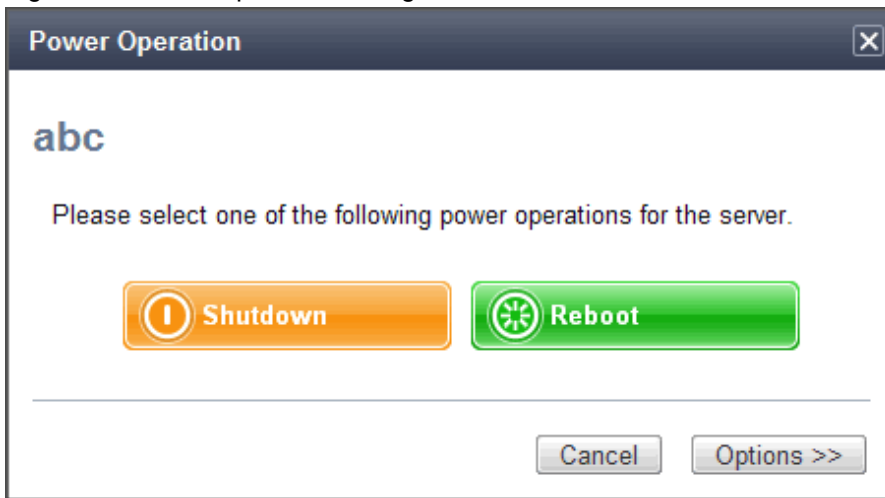
Clicking on a power button that shows "Power OFF" status will power on the target server blade. A confirmation dialog is displayed first. Clicking <OK> in the confirmation dialog powers on the server and starts its OS.

At this time, the power button changes to an intermediate "Power ON in progress" state (green - blinking). The power button finally displays a "Power ON" state after confirming that the OS has started up correctly on the target server.

Power Off and Reboot

Clicking on a power button that shows "Power ON" status will either shut down or reboot the target server blade. A [Power Operation] dialog is displayed, in which the appropriate action can be selected.

Figure 3.5 Power Operation Dialog



- "Shutdown"

Selecting "Shutdown" will shut down the target server blade. A confirmation dialog is displayed first.

Clicking <OK> in the confirmation dialog shuts down the OS and powers off the managed server.

At this time, the power button changes to an intermediate "Power OFF in progress" state (orange - blinking). The power button finally displays "Power OFF" status after confirming that the target server has been shut down correctly.

- "Reboot"

Selecting "Reboot" will reboot the target server blade. A confirmation dialog is displayed first.

Clicking <OK> in the confirmation dialog shuts down the OS and reboots the managed server.

At this time, the power button changes to an intermediate "Power ON in progress" state (green - blinking). The power button finally displays "Power ON" status after confirming that the OS has started up correctly on the target server.

Forced Power Off and Reboot

Clicking on a power button that shows "Power ON" status, and selecting <Options >>> in the displayed [Power Operation] dialog enables selection of the "Force Shutdown" and "Force Reboot" actions.

A forced shutdown (or reboot) will forcibly power off (or reboot) the managed server blade without waiting for its OS to shut down cleanly.

Figure 3.6 Power Operation Dialog (with Additional Options)



- "Force Shutdown"

Selecting "Force Shutdown" will forcibly power off the target server blade. A confirmation dialog is displayed first. Clicking <OK> in the confirmation dialog will power off the managed server without waiting for its OS to shut down cleanly. At this time, the power button changes to an intermediate "Power OFF in progress" state (orange - blinking). The power button finally displays "Power OFF" status after confirming that the target server has been shut down correctly.

- "Force Reboot"

Selecting "Force Reboot" will forcibly reboot the target server blade. A confirmation dialog is displayed first. Clicking <OK> in the confirmation dialog will power off and reboot the managed server without waiting for its OS to shut down cleanly. At this time, the power button changes to an intermediate "Power ON in progress" state (green - blinking). The power button finally displays "Power ON" status after confirming that the OS has started up correctly on the target server.

 Note

[VM Host]

Take caution regarding the following points when powering-off or rebooting a VM host.


- When using a server virtualization software's high-availability feature, confirm that the server is set to VM maintenance mode within that virtualization software. This can be confirmed from the virtualization software client.
- Perform power operations only after setting VM maintenance mode (either from the VM management software client or using the resource control command).
Refer to the server virtualization software manual, or to "3.2 rcxadm server" of the "Command Reference" for details.
Depending on the server virtualization software used, some restrictions may apply to the use of VM maintenance mode settings. For details about such restrictions, refer to "E.3 Functional Differences between Products" of the "Setup Guide VE".


3.5.2 VM guest

The power status of a VM guest can be controlled by clicking the OS icon of its VM host and then clicking its power button in the list of VM guests that is displayed.

Clicking on the power button provides power controls similar to those provided for server blades.

Table 3.16 Actions of VM Guest Power Buttons

Power button	Color	Status	Action
	Gray (not lit)	Power OFF	Powers on a VM guest.

Power button	Color	Status	Action
	Green (lit)	Power ON	Shuts down or reboots a VM guest.

Note

- VM guests need to be properly configured in order to use the shut down or reboot buttons. Attempting to shut down or reboot a VM guest that is not properly configured will result in an error. For details, refer to "E.2 Configuration Requirements" of the "Setup Guide VE".
- Depending on the server virtualization environment, a VM guest may automatically migrate to another VM host when a power control operation is performed. This may cause power control operations to fail and return an error when used on VM guests. For details, refer to "E.3 Functional Differences between Products" of the "Setup Guide VE".
- A VM guest can be configured to automatically start or stop whenever its VM host starts up or shuts down. This can be achieved by configuring the VM guest's startup and shutdown options in the server virtualization software used. For details, refer to the server virtualization software manual.

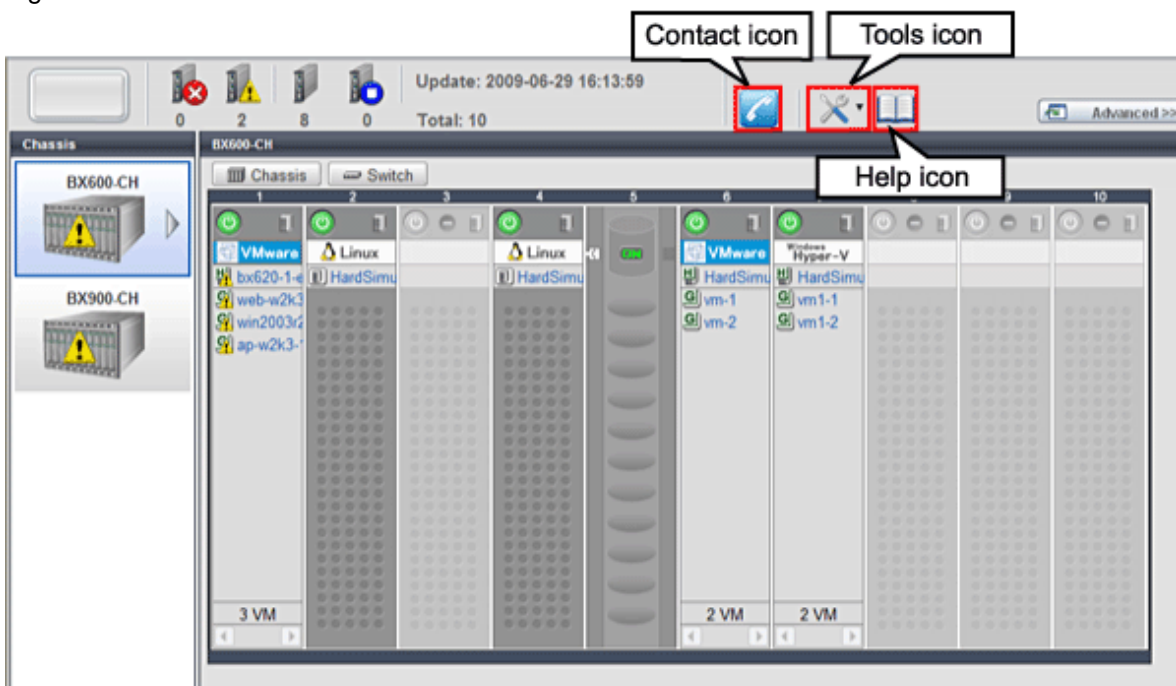
[Windows]

- Take caution regarding the following points when shutting down or rebooting a managed server running a Windows operating system.
 - If Windows is not configured to shut down when the computer's power button is pressed, the power operations in Resource Orchestrator may not function properly. To check this option, access the Control Panel, open the [Power Options], and check the settings of the [Advanced] tab in the [Power Options Properties] window.
 - If a file is being edited by a logged-in user, a dialog prompting the user to save the file is displayed, and the system may not shut down immediately. In such cases, shutdown does not take place until the user takes the appropriate action or a specified time (approximately five minutes) has elapsed.

3.6 Status Panel Operations

This section describes the operations that can be performed from the status panel.

Figure 3.7 BladeViewer: Tool Icons



Contact icon

Displays the [Contact] dialog. This dialog shows the contact information that was set for the entire system.

Tools icon

Enables selection of the following menu options:

Display Label List

Displays the [Label List] dialog.
Displays a list of labels. This list also allows modification of labels and comments.
For details on editing labels and comments, refer to "3.6.1 Listing and Editing of Labels and Comments".

Set Contact Information

Displays the [Set Contact Information] dialog.
For details on modifying contact information, refer to "3.6.2 Editing Contacts".

Change Password

Displays the [Change Password] dialog.
For details on changing passwords, refer to "3.6.3 Changing Passwords".

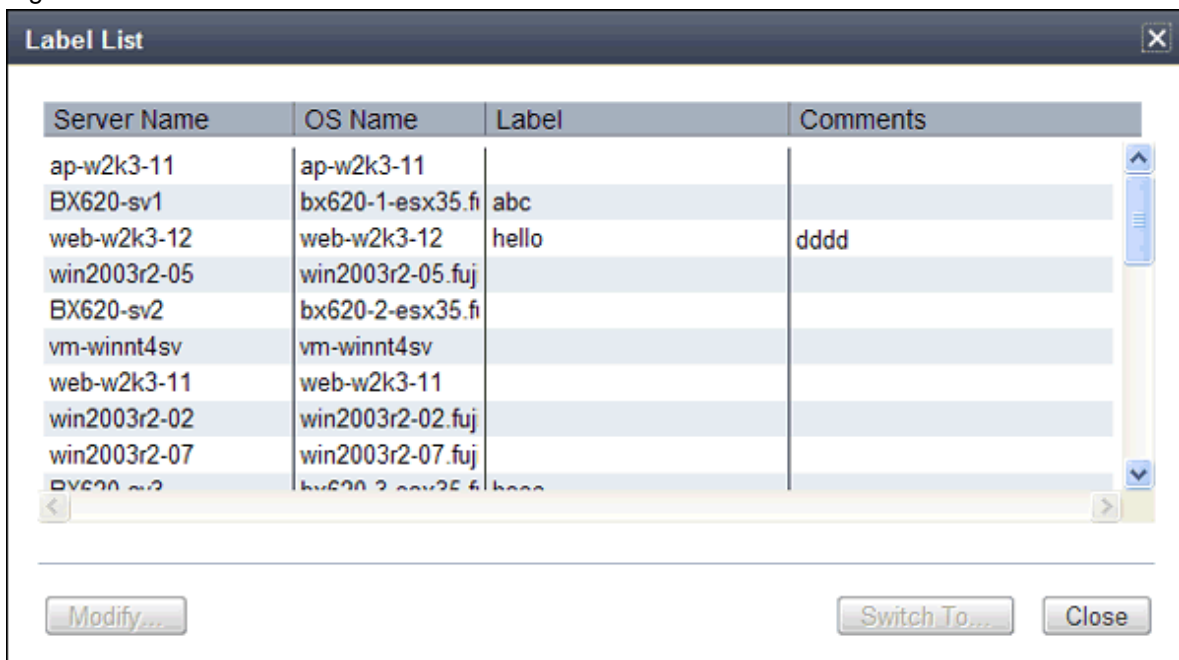
Help icon

The Help is displayed.

3.6.1 Listing and Editing of Labels and Comments

Clicking on the Tools icon and selecting "Display Label List" from the drop-down list displays the [Label List] dialog shown below. When applications are defined with labels, this list can provide a quick overview of the applications running on each server.

Figure 3.8 Label List



Contents of the label list

The [Label List] dialog displays server names, OS names, labels, and comments for each server.

Clicking <Switch To> after selecting a server from the list will switch the view to the blade panel and display the selected server within its enclosing chassis.

Editing Labels and Comments

This function is only available to privileged users.
General users are only able to consult labels and comments.

- Privileged user

In the [Label List] dialog, select a server and click <Modify>. The [Modify Server Settings] dialog is displayed.

The label and comment of the selected server can be edited directly from the [Modify Server Settings] dialog.

Enter the following items:

Label

Enter up to 32 alphanumeric characters or symbols (ASCII characters 0x20 to 0x7e).

Comments

Enter up to 256 alphanumeric characters or symbols (ASCII characters 0x20 to 0x7e).



.....
New lines are counted as two characters.
.....

Additional information such as OS name, server name (for a physical OS, the physical server name, for a VM guest, the VM guest name), and IP address are displayed to help identify the selected server.

Clicking <Save> saves the modified label and comment into the manager's database. The saved content is then updated and displayed in BladeViewer.

- General user

If logged in as a general user, <Show> is displayed in place of <Modify> in the [Label List] dialog.

Clicking <Show> displays the [Server Properties] dialog, but does not allow editing of labels or comments.

3.6.2 Editing Contacts

Clicking the Tools icon and selecting "Set Contact Information" from the drop-down list displays the [Set Contact Information] dialog. This function is only available to privileged users. If logged in as a general user, the "Set Contact Information" menu item cannot be selected.

Enter the following item.

Contact

The currently defined contact information is displayed.

Enter a maximum of 256 characters.



.....
New lines are counted as two characters.
.....

Clicking <Save> saves the modified contact information into the manager's database. The saved content will be displayed the next time the [Contact] dialog is opened.

3.6.3 Changing Passwords

Clicking the Tools icon and selecting "Change Password" from the drop-down list displays the [Change Password] dialog.

The required information varies according to the authority level of the logged in user, as described below. The password is changed after entering the required information and clicking <Change>.

- Privileged user

New password (Confirm password)

Enter a string using up to 16 alphanumeric characters or symbols.

- General user

Current password

Enter the password that is currently set.

Enter a string using up to 16 alphanumeric characters or symbols.

New password (Confirm password)

Enter a string using up to 16 alphanumeric characters or symbols.

Chapter 4 User Accounts

This chapter explains the user accounts used in Resource Orchestrator.

4.1 Overview

Managing user accounts in Resource Orchestrator prevents unsafe operations by unauthorized users, resulting in safer system administration.

User accounts are divided into the following user types.

Table 4.1 User Types

User types	Authority level	Description
Privileged user	Manage	Can perform all operations on resources.
General user	Monitor	Can only perform resource monitoring.

It is required to create at least one privileged user. The creation of general users is optional and depends on your own administration policy.

User accounts consist of the following:

- User name
- Password
- Authority level ("Manage" or "Monitor")

These Resource Orchestrator user accounts differ from the operating system user accounts on the admin server.

Refer to "1.2.1 List of Menus" of the "User's Guide VE" for information on the functions that these user accounts can execute.

4.2 Managing User Accounts

This section explains how to register, modify, and delete user accounts.

Add User Account

Only privileged users can perform this operation.

When using Single-Sign-On, register user information in ServerView Operations Manager beforehand.

1. From the ROR console menu, select [Settings]-[User Accounts].

The [User Accounts] dialog is displayed.

2. Click <Add>.

The [Add User Account] dialog is displayed.

3. Set the following:

User ID

Enter a string of up to 16 characters. The first character must be a letter and the remaining characters can include alphanumeric characters, underscores ("_"), hyphens ("-"), and periods (".").

Please note that user names are case-sensitive.

Password (Confirm password)

- When using Single-Sign-On

Enter a string using alphanumeric characters or symbols in the range of 8 to 64 characters.

- When not using Single-Sign-On

Enter a string using up to 16 alphanumeric characters or symbols.

Authority level

Select either "Manage" or "Monitor". There must be at least one privileged user.

4. Click <OK>.

The user account is created.

Change User Account Settings

Both privileged users and general users can perform this operation.

Privileged users can modify any account information. General users can only modify their own password.

1. From the ROR console menu, select [Settings]-[User Accounts].

The [User Accounts] dialog is displayed.

2. Select the user account to modify, and click <Change>.

The [Change User Account] dialog is displayed.

3. Set the following:

Password

No change/Change

Select the appropriate action.

By default, the "No change" option is selected.

Current password

Enter a string using up to 16 alphanumeric characters or symbols.

This is displayed when general users modify their own passwords.

New password (Confirm password)

Enter a string using up to 16 alphanumeric characters or symbols.

Authority Level

No change/Change

Select the appropriate action.

By default, the "No change" option is selected.

Authority level

Select either "Manage" or "Monitor".

By default, the current authority level is selected.

4. Click <OK>.

The password and authority level for the user account are changed.

Delete User Account

Only privileged users can perform this operation.

When using Single Sign-On, delete a user account on the directory service as necessary.

1. From the ROR console menu, select [Settings]-[User Accounts].

The [User Accounts] dialog is displayed.

2. Select the user account to delete, and click <Delete>.

The [Delete User Account] dialog is displayed.

3. Click <OK>.

The selected user account is deleted.

Chapter 5 Monitoring

This chapter explains how to monitor the configuration and status of managed resources.

5.1 Overview

Resource Orchestrator can centrally monitor the configuration and status of servers or other managed resources directly from the ROR console. This enables the identification of resources experiencing problems, which reduces the time spent on system maintenance. Moreover, Resource Orchestrator can easily launch external management software to precisely locate faulty parts within a managed resource.

Monitoring is based on the following three components:

- Resources

The tree displays chassis, servers, LAN switches, physical OS's, VM hosts, VM guests, and power monitoring device relationships and statuses (either PDU or UPS for management software).

When a hardware problem occurs on a server, affected guest operating systems can be easily detected.



Power monitoring devices are not subject to monitoring.

- Events

Resource Orchestrator displays events such as hardware failures, server switchovers triggered by hardware failures, and the results of every performed operation.

- Recent Operations

Resource Orchestrator displays the progress status of the various operations performed on resources.

The following table shows the level of monitoring performed for each resource monitored in Resource Orchestrator.

Table 5.1 Monitoring Level for Each Resource Type

Resource	Status monitoring	Event monitoring
Chassis	Yes	Yes
Server	Yes	Yes
Physical OS	Yes	No
VM host	Yes	No
VM guest	Yes	No
VM management software	Yes	No
LAN switch	Yes	Yes
Power monitoring device	No	No

Yes: Supported

No: Not supported

Regular update of resource data

The Resource Orchestrator manager regularly updates resource data with information gathered from the following resources.

Table 5.2 List of Regularly Updated Resources and Their Related Resources

Resources subject to regular update	Related resources	Data source
Chassis	Chassis	Server Management Unit

Resources subject to regular update	Related resources	Data source
Server	Server Physical OS VM host (*1) VM guest (*1)	ServerView Agents (*2) Server Management Unit Server Virtualization Software
LAN switch	LAN switch	LAN switch Server Management Unit (*3)
VM management software	VM management software VM host (*1) VM guest (*1)	VM management software

*1: When no VM management software is registered, the status of VM hosts and VM guests is updated during a regular update of their physical server. When VM management software is registered, their status is updated during the regular update of the VM management software.

*2: Only for PRIMERGY servers and PRIMEQUEST.

*3: Only for LAN switch blades mounted in a PRIMERGY BX chassis.

The time required to update all resources depends on the number of registered resources. For 1 chassis that contains 10 servers and 4 LAN switches, the update takes about 2 minutes. For 5 chassis that have identical configurations, the update should take about 10 minutes.

VM management software updates are independent from other resource updates, and takes approximately 3 minutes.

In the following cases, resource data is refreshed without waiting for the regular update.

- When a resource's state is changed as the result of an operation performed by Resource Orchestrator
- When a failure-triggered SNMP Trap is received from a resource

If a resource was operated externally to Resource Orchestrator, there may be a slight delay before its state is updated in the ROR console. To force an update of a resource's data, right-click the resource and select [Update] from the displayed menu. The time required to update resource data depends on the device. Generally, update should take no more than 40 seconds.

In order to restrain device and network load, resource data is not refreshed for 7 seconds following the last update time. However, when a failure-triggered SNMP Trap is received, resource data is refreshed unconditionally. When manually updating a resource from the menu right after performing an operation on that resource, if its data is not refreshed within 40 seconds, try updating it from the menu again.

5.2 Resource Status

Resources are monitored in the [Status] tab of the ROR console.

The [Status] tab shows the number of servers listed under the statuses "warning", "unknown", "error", or "fatal".

Servers whose status is "warning" or "unknown" are counted under "Warning", and servers whose status is "fatal" or "error" are counted under "Error".

Clicking on "Error" or "Warning", displays the resources under the corresponding status in the [Resource List] tab.



The status of resources can also be monitored from both the resource tree and the [Resource List] tab. When an error occurs, a status icon is added to the icon of the resource concerned.










Double-clicking on a resource icon displays the [Resource Details] tab, which provides detailed information about the corresponding resource.

Icons displayed in the ROR console

The following table shows the resource icons used in BladeViewer and their associated meanings.

Table 5.3 Resource Icons




Icon	Meaning
	Server resource
	Chassis

Icon	Meaning
	Server
	Physical OS
	VM host
	VM guest
	LAN switch
	Power monitoring device (*1)
	PDU (*1)
	UPS (*1)
	Management software

*1: Power monitoring devices (PDU or UPS) are not subject to monitoring.

The following table shows the status icons used in Resource Orchestrator and their associated meanings. It also shows which status icons require corrective actions.

Table 5.4 Status Icons

Icon	Status	Meaning	Corrective action
	normal	Normal	No action is necessary
	warning	Warning An error has occurred but the resource can still be used.(*1)	Action must be taken
	unknown	Unknown The status of the resource cannot be obtained. (*2, *3)	Action must be taken
	stop	Stop The resource has stopped and cannot be used.	No action is necessary
	error	Error An error whose cause is unknown has occurred and the resource cannot be used.	Action must be taken
	fatal	Fault A fault has occurred in the resource and the resource cannot be used.	Action must be taken

*1: When a LAN switch is in "warning" status, it may mean that the LAN switch has been replaced with another model.

To use the LAN switch as it is, first delete the registered LAN switch, and then register it again.

*2: When a VM guest is in "unknown" status, check the operation status of the VM host on which the VM guest is running.

*3: When a LAN switch is in "unknown" status, check the physical connection between the LAN switch and admin LAN as well as whether or not the LAN switch is responding to commands.

Note

- On the SPARC Enterprise T series, as statuses cannot be obtained from ILOM using SNMP, only "normal", "stop" or "unknown" statuses are shown, while "warning", "error", and "fatal" statuses cannot be detected. If an SNMP Trap indicating an error is displayed, check the status of the server on ILOM.
- For other servers, hardware statuses cannot be obtained from server management software (ServerView). Therefore, only "normal", "stop" or "unknown" statuses are shown, while "warning", "error", and "fatal" statuses cannot be detected.

- For PRIMEQUEST, all partitions within the same chassis may temporarily become "unknown" depending on the timing of change in power control status of the partition.

Table 5.5 Physical Server Icons











Icon	Meaning
	Spare server
	Maintenance mode server

Table 5.6 OS Icons

Icon	Meaning
	Windows OS
	Linux OS
	Solaris OS
	VMware host OS
	Hyper-V host OS
	Citrix XenServer host OS
	Linux Xen host OS
	KVM host OS

Information

- For server virtualization software, the following information is also displayed.
 - VM management software

VM management software statuses can be one of the following: "normal" or "unknown". If "unknown" is shown, check whether the VM management software is operating properly.
 - VM host

The status of a VM host is displayed in the same way as for a physical OS.
 - VM guest

Errors detected from server virtualization software are reflected in VM guest statuses. VM guest statuses can be one of the following: "normal", "warning", "error", "unknown", or "stop".
For details, refer to "E.3 Functional Differences between Products" of the "Setup Guide VE".
- For LAN switches, "error" and "fatal" are not displayed. Only "warning", "normal", or "unknown" are displayed.

5.3 Addressing Resource Failures

This section explains how to address problems like hardware failures that occur in a system.

Basic Procedure

The following procedure is used to confirm and resolve problems using the ROR console:

1. Confirm the existence of a problem

For the confirmation method, refer to "5.2 Resource Status" in this chapter and "1.3 Status Panel" of the "User's Guide VE".

2. Check the event log

Use the event log to check the device where the error occurred and the content of the event.

In some cases, a single problem can cause a series of events, so search back through past events to find events with dates that are close together.

3. Check the status of resources

From the resource tree, open the resource where the problem occurred and look for any affected chassis, physical servers, LAN switches, physical OS's, VM hosts, or VM guests.

If Auto-Recovery has been enabled for a physical OS or VM host, it will be automatically switched over with a spare server. If Auto-Recovery has not been enabled, server switchover can still be performed manually as long as a spare server has been designated. For more information regarding server switchover, refer to "[10.2 Switchover](#)".

4. Perform detailed investigation and recovery

From the [Resource Details] tab of the failed resource, launch the external management software to investigate the precise cause of the problem.

When no management software is available, confirm with the maintenance staff of the failed resource to investigate the problem.

Once this is done, perform the necessary maintenance work on any faulty hardware identified.

If a server hardware failure requires replacing a managed server, carry out the replacement operation as described in "[9.4 Replacing Servers](#)".

5. Perform post-recovery verification

Following recovery, confirm that there are no more icons indicating problems on the ROR console.

Chapter 6 Power Control

This chapter explains how to remotely control the power state of managed resources.

6.1 Server Power Control

This section explains how to remotely control the power states of physical servers, VM hosts, and VM guests.

Use the following procedure to perform power control operations.

1. In the ROR console server resource tree, right-click the desired server (or the physical OS or VM host running on the server) or VM guest, select [Power] from the popup menu, and select one of the following options:

ON

This option powers on a halted resource and starts its operating system.

OFF

This option powers off an active resource after shutting down its operating system.

OFF (Forced)

This option forcibly powers off an active resource without first shutting down its operating system.

Reboot

This option restarts an active resource after shutting down its operating system.

Reboot (Forced)

This option forcibly restarts an active resource without first shutting down its operating system.

The confirmation dialog is displayed.

2. Click <OK>.

The specified power control operation is executed.

3. The progress of the specified operation is displayed in the Recent Operations area. Check that the operation status is shown as "Completed", and that the resource in the server resource tree or [Resource List] tab has changed to the expected power state.



Information

A reboot or forced reboot of a physical server or VM host is done by shutting down the server once, and powering it on again (instead of a system reset).



Note

- VM guests must be properly configured in order to use the power off or reboot options. Attempting to shut down or reboot a VM guest that is not properly configured will result in an error. For details, refer to "E.2 Configuration Requirements" of the "Setup Guide VE".
- Depending on the server virtualization environment, a VM guest may automatically migrate to another VM host when a power control operation is performed. This may cause power control operations to fail and return an error when used on VM guests. For details, refer to "E.3 Functional Differences between Products" of the "Setup Guide VE".
- A VM guest can be configured to automatically start or stop whenever its VM host starts up or shuts down. This can be achieved by configuring the VM guest's startup and shutdown options in the server virtualization software used. For details, refer to the server virtualization software manual.
- Take caution regarding the following points when shutting down or rebooting a PRIMEQUEST managed server.
 - If rebooting is attempted for a server that has been placed into hardware maintenance mode, the operation fails and only powering-off is performed.

[Windows]

- Take caution regarding the following points when shutting down or rebooting a managed server running a Windows operating system.
 - If Windows is not configured to shut down when the computer's power button is pressed, the power operations in Resource Orchestrator may not function properly.
To check this option, access the Control Panel, open the [Power Options], and check the settings of the [Advanced] tab in the [Power Options Properties] window.
 - If a file is being edited by a logged-in user, a dialog prompting the user to save the file is displayed, and the system may not shut down immediately.
In such cases, shutdown does not take place until the user takes the appropriate action or a specified time (approximately five minutes) has elapsed.

[VM Host]

- Take caution regarding the following points when powering-off or rebooting a VM host.
 - When using a server virtualization software's high-availability feature, confirm that the server is set to VM maintenance mode within that virtualization software. This can be confirmed from the virtualization software client.
 - Perform power operations only after setting VM maintenance mode (either from the VM management software client or using the resource control command).
Refer to the server virtualization software manual, or to "3.2 rcxadm server" of the "Command Reference" for details.
Depending on the server virtualization software used, some restrictions may apply to the use of VM maintenance mode settings.
For details about such restrictions, refer to "E.3 Functional Differences between Products" of the "Setup Guide VE".
-

6.2 Chassis Power Control

This section explains how to remotely control the power state of a chassis.

Power operations are only possible for PRIMERGY BX server chassis.

The power state of a blade chassis can be controlled using the rcxadm chassis command.

Refer to "3.1 rcxadm chassis" of the "Command Reference" for details.

Chapter 7 Control of VM Environments

This chapter explains the Resource Orchestrator functions that are specific to VM guests and VM hosts.

Some functions may or may not be available depending on the server virtualization software used. Refer to "E.1 Common Functions of Server Virtualization Software" of the "Setup Guide VE" for details.

Other functions are similar in use to those available for regular physical OS's (without server virtualization software).

7.1 Migration of VM Guests between Servers

This section explains how to migrate a VM guest to a VM host on a different physical server.

Two methods of VM guest migration are available in Resource Orchestrator. Although such methods are named differently depending on the server virtualization software used, Resource Orchestrator makes use of the following naming convention.

For details on migration pre-requisites and terminology, refer to "E.3 Functional Differences between Products" of the "Setup Guide VE".

- Live migration

Migration of a VM guest without shutting down its VM host.

- Cold migration

Migration of a VM guest while its VM host is shut down. A VM guest after migration is set to the same power status as it was before the migration.

The availability of those methods depends on the power status of VM guests, as described below.

Table 7.1 Migration Methods Available for Each Power Status

VM Guest Power Status	Migration Method	
	Cold migration	Live migration
ON	Available	Default
OFF	Default	N/A

Default: This method is available and selected by default.

Available: This method is available.

N/A: This method is not available.

A VM guest after migration is set to the same power status as it was before the migration. For example, performing a cold migration on an operating VM guest will temporarily shut it down during migration, before starting it up again after completion of the migration process. It is therefore recommended to set the target VM guest to the desired post-migration power status before performing migration.

Use the following procedure to migrate a VM guest.

1. In the ROR console server resource tree, right-click a VM guest to migrate and select [Migrate VM Guest] popup menu.

2. The [VM Guest Migration] dialog is displayed.

Set the following items:

Destination

Select a destination VM host.

Migration Method

Select the desired migration type.

3. Click <OK>.

The selected VM guest is migrated to its new host.

VM guests can be migrated from the command-line, using the rcxadm server migrate command.

Refer to "3.2 rcxadm server" of the "Command Reference" for details.

7.2 VM Maintenance Mode of VM Hosts

This section explains how to set and release VM maintenance mode on VM hosts.

For details on VM maintenance mode, refer to "E.3 Functional Differences between Products" of the "Setup Guide VE".

VM maintenance mode can also be set or released from the command-line, using the rcxadm server set command.

Refer to "3.2 rcxadm server" of the "Command Reference" for details.

7.3 VM Home Position

This section explains VM Home Position.

By configuring the VM Home Position in advance, it is possible to restore VM guests to their original VM host using only one operation when they have been migrated to a different VM host for operation or maintenance needs.

This enables restoration of multiple VM guests to their original locations without the need to record their original locations.

7.3.1 Setting VM Home Position

When configuring a VM Home Position, the relationships of operating VM guests and registered VM hosts are retained.

Setting is only available when more than one VM guest exists.



Information

- When registering a new VM host, as the relationship between the VM host and operating VM guests is not yet retained, reconfiguration of VM Home Position is necessary.
- When a new VM guest is detected, reconfigure the VM Home Position so the relationship between that VM guest and its VM host is set.
- When configuring the home position of a system, all VM Home Positions of VM guests are set to the current configuration.
- When configuring home positions for each VM host, VM guests will be associated with the VM host on which they are operating. The relationships are retained, even when a VM guest associated with the VM host is operating on another VM host.

Configuring a System's VM Home Position

Use the following procedure to configure a VM Home Position for all VM hosts on a system:

1. Select [Operation]-[VM Home Position]-[Settings] from the ROR console menu.

The [Configure VM Home Position Settings] dialog is displayed.

2. Click <OK>.

The VM Home Position is set.

Configuring a VM Host's VM Home Position

Use the following procedure to configure the VM Home Position for a selected VM host:

1. In the ROR console server resource tree, right-click VM host and select [VM Home Position]-[Settings] from the popup menu.

The [Configure VM Home Position Setting] dialog is displayed.

2. Click <OK>.

The VM Home Position is set.

7.3.2 Migrating to VM Home Position

Migrate VM guests back to their original VM hosts using the relationship information that was registered in advance.

The method used for VM guest migration is automatically selected from cold migration and live migration after each VM guest's power status is checked.

Migrating all VM Guests to their VM Home Positions

Use the following procedure to migrate the VM guests of a system to their VM Home Position:

1. Select [Operation]-[VM Home Position]-[Back to Home] from the ROR console menu.

The [Migrate VM Guests to their VM Home Positions] dialog is displayed.

2. Click <OK>.

Migration of VM guests to their VM Home Positions will be performed.

Migrating VM Guests of a Selected VM Host to their VM Home Position

Use the following procedure to migrate VM guests associated with a selected VM host to their VM Home Position:

1. In the ROR console server resource tree, right-click a VM host and select [VM Home Position]-[Back to Home] from the popup menu.

The [Migrate VM Guests to their VM Home Position] dialog is displayed.

2. Click <OK>.

Migration of VM guests to their VM Home Position will be performed.

When migrating VM guests to their VM Home Position, use the `rcxadm server migrate` command.

For details on this command, refer to "3.2 `rcxadm server`" of the "Command Reference".

7.3.3 Clearing VM Home Position

When the VM Home Position is cleared, the relationships of VM hosts and VM guests are cleared.

Clearing a System's VM Home Position

Use the following procedure to clear the VM Home Position of all VM host's on a system:

1. Select [Operation]-[VM Home Position]-[Clear] from the ROR console menu.

The [Clear VM Home Position Settings] dialog is displayed.

2. Click <OK>.

The VM Home Position settings are cleared.

Clearing a VM Host's VM Home Position

Clear VM Home Position of selected VM hosts using the following procedure.

1. In the ROR console server resource tree, right-click a VM host, and select [VM Home Position]-[Clear] from the popup menu.

The [Clear VM Home Position Setting] dialog is displayed.

2. Click <OK>.

The VM Home Position setting is cleared.

Chapter 8 Backup and Restore

This chapter explains how to use the backup and restore functions provided in Resource Orchestrator.

8.1 Overview

The backup and restore functions allow the backup and restoration of system images from physical OS's or VM hosts.

The system images are backed up over the network and stored on a disk on the admin server.

A system image backup can be used for the following purposes.

- Software maintenance

A system image backup can be created as a precautionary measure before performing maintenance tasks such as applying patches, installing, or modifying installed software.

- Hardware maintenance

A system image backup can be used to guard against hardware problems such as disk failures.



Note

- Regardless of the boot environment (local/SAN/iSCSI) and RAID configurations, only the contents of the first disk (boot disk) recognized by the managed server's BIOS can be backed up and restored.

The contents of other disks (data disks) cannot be backed up and restored. To properly back up and restore such data disks, it is recommended to use dedicated backup software, or the copy functions available in storage devices.

When the first disk contains multiple partitions (Windows drive, Linux/VMware partition), all partitions are backed up.

Table 8.1 Examples of system image backup and restore targets

Disk	Windows Disk Name	Windows Drive Name	Target of Backup and Restore
First	Disk 0	C:	Yes
		E:	Yes
Second	Disk 1	D:	No
		F:	No

- As managed servers are restarted during backup and restore operations, their applications should be stopped beforehand.

- Restore operations can only be performed for the servers from which a backup has been collected.

- The first partition must be the boot partition.

- The operations for backup and restore of VM hosts differ depending on the server virtualization software used.

For an explanation of the behavior differences that occur when VM guests are included in the VM host's boot disk, refer to "E.3 Functional Differences between Products" of the "Setup Guide VE".

If VM guests on the boot disk are not to be backed up (and restored), VM guest files should be moved to another disk.

- To preserve the configuration of the server virtualization software used, VM guests should be backed up at the same time as VM hosts. During backup, because the target VM host will be automatically set to VM maintenance mode, the VM host should be in a state that allows VM maintenance mode to be set.

When backing up a VM host in a high-availability configuration, all VM guests stored on shared disks should be migrated to another VM host beforehand.

After backing up the VM host, migrate the VM guests back to their original VM host.

Refer to the server virtualization software manual and "E.3 Functional Differences between Products" of the "Setup Guide VE" for information on how to back up and migrate VM guests, or about the VM maintenance mode.

- To preserve the configuration of the server virtualization software used, VM guests backed up at the time of the VM host's backup should also be restored when restoring a VM host. Note that this is not required if no changes likely to alter the virtualization software configuration were made (e.g. changes such as addition or deletion of a VM guest, or changing the placeholder for VM guest definition files).

During restore, because the target VM host will be automatically set to VM maintenance mode, the VM host should be in a state that allows VM maintenance mode to be set.

If the target VM host is in a high-availability configuration, all VM guests stored on shared disks should be migrated to another VM host beforehand.

After restoring the VM host, migrate the VM guests back to their original VM host.

Refer to the server virtualization software manual and "E.3 Functional Differences between Products" of the "Setup Guide VE" for information on how to restore and migrate VM guests, or about the VM maintenance mode.

- Deleting a managed server will delete its backed up system images at the same time.
- It is not possible to backup, restore, or delete a system image from a managed server for which a system image (including different versions) is already being backed up, restored, or deleted.
- When restoring a system image on a server whose name was changed after the deployment of a cloning image, check that the "*server_name*" displayed on the server resource tree and the System Image List match the new server name before restoring the system image.
- For managed servers on which the Watchdog function is enabled, backup or restore operations on that server may be aborted by an automatic restart or shutdown. The Watchdog is a function which automatically restarts or shuts down non-responsive servers when their operating system does not respond for a given period. Therefore, it is highly recommended to disable the Watchdog function before a backup or restore operation. For details on the Watchdog function, refer to the server manual.
- If the disk size of the source (backed up) server differs from that of the destination (restored) server, restore is possible only in cases where the disk size of the destination server is larger than that of the source server. In that case, unused disk space will remain on the destination server. To use this unused disk space, a partition should first be created from it.

Restoring a system image to a server on which the disk size is smaller than that of the source (backed up) server is not possible. This also applies to server switchover and failback operations that are based on backup and restore, as well as cloning operations.

Therefore, it is also necessary to ensure that spare servers of cloning destination servers have a large enough disk.

- When backing up or restoring system images, or collecting and deploying cloning images, up to four processes can be executed simultaneously. If four processes are already being executed, any additional image operations will enter a standby state. Moreover, server switchover which is executed using the backup and restore method or any restore process performed during failback will also enter a standby state. When Auto-Recovery or manual switchover using the backup and restore method is used, please limit the number of image operations (backup or restore of system images, or collection and deployment of cloning images) performed at the same time to 3.
- When using backup and restore for PRIMEQUEST servers, check that the boot option settings and BIOS settings of the target servers match. When the settings are different, execute the function after changing the settings so they match. This boot option settings can be changed by following the instructions given in "3.2.10 Changing Boot Options" of the "User's Guide VE". Moreover, in case of PRIMEQUEST1000x2 servers, disable UEFI x2APIC mode.

8.2 Backup

This section explains how to collect a system image backup.

System images can only be backed up from managed servers that are not in "stop" status.

System images can also be backed up using commands.

Refer to "Chapter 4 Image Operations" of the "Command Reference" for details.

Preparations

Execute the following command before performing backup if a Windows manager is to be used and the managed server has the following configuration.

- In a SAN data environment using a built-in disk boot, and a physical WWN or VIOM

```
>Installation_folder\Manager\bin\rxadm server set -name physical_server -attr bootagt=dos <RETURN>
```

- When using the Red Hat Enterprise Linux 6 ext4 file system or on a server using UEFI, and one of the following conditions is met
 - In a SAN boot environment using HBA address rename
 - When using a rack mount or tower server and the server is registered with "Disable" of "Association with server management software (ServerView)" is selected

```
>Installation_folder\Manager\bin\rxadm server set -name physical_server -attr bootagt=winpe <RETURN>
```

Backing up a System Image

Use the following procedure to back up a system image from a managed server.

1. Place the target server into maintenance mode and stop all of its applications.
 - a. In the ROR console server resource tree, right-click the target server (or its physical OS or VM host) and select [Maintenance Mode]-[Set] from the popup menu.

The [Set Maintenance Mode] dialog is displayed.


As the target server is restarted during backup, all of its applications should be stopped beforehand. When backing up a VM host, all of its VM guests should also be stopped.
 - b. Click <OK>.

The target server is placed into maintenance mode.
2. Back up a system image from the target server.
 - a. In the ROR console server resource tree, right-click the target physical OS or VM host and select [Backup/Restore]-[Backup] from the popup menu.

The [Backup] dialog is displayed.
 - b. Set the following items as necessary:

Comments

Enter a comment to identify the system image.
A comment can be up to 128 characters long. Use of percent signs ("%"), backslashes ("\), double quotes ("), and linefeed characters are not allowed.

 **Note**

.....

A list of the resources that will be powered off during backup is displayed in the text area. Confirm that it is safe to shutdown those resources before continuing with the backup operation.
When backing up a VM host, all of its VM guests will also be stopped.

.....
 - c. Click <OK>.

Backup of the system image is started.

The process status can be checked in the Recent Operations area of the ROR console.

When <Cancel> is clicked in the Recent Operations area, the confirmation dialog to quit the process is displayed.

After backing up a VM host, stop and back up all of its VM guests.
For details on VM guest backup, refer to the server virtualization software manual.
3. Release the target server from maintenance mode before resuming its applications.
 - a. In the ROR console server resource tree, right-click the target server (or its physical OS or VM host) and select [Maintenance Mode]-[Release] from the popup menu.

The [Release Maintenance Mode] dialog is displayed.

- b. Click <OK>.

The target server is released from maintenance mode.

Note

- The number of system image versions that can be kept for a managed server is limited. If a new system image backup is collected when this limit has already been reached, the oldest version will be deleted. By default, the maximum number of system images is 3. This limit can be changed by following the instructions given in "3.1.3 Changing the Maximum Number of System Image Versions" of the "User's Guide VE".
- When backing up a new system image, its version number will be increased by one. The version number of the first backed up system image of a managed server will always be 1.
- When backing up a VM host in a high-availability configuration, all VM guests stored on shared disks should be migrated to another VM host beforehand. During backup, because the target VM host will be automatically set to VM maintenance mode, the VM host should be in a state that allows VM maintenance mode to be set. After backing up the VM host, migrate the VM guests back to their original VM host. Refer to the server virtualization software manual and "E.3 Functional Differences between Products" of the "Setup Guide VE" for information on how to migrate VM guests, or about the VM maintenance mode.
- When using PRIMECLUSTER GLS for admin LAN redundancy, backup of a system image may fail if the following message is displayed in the event log.

```
FJSVrcx:WARNING:41306:server.NIC takeover on Admin LAN was detected
```

If this occurs, wait for the following message to show in the event log before performing backup again.

```
FJSVrcx:INFO:23301:server.admin LAN information was successfully updated
```

8.3 Restoring System Images

This section explains how to restore a system image backup.

System images can also be restored using commands.

Refer to "Chapter 4 Image Operations" of the "Command Reference" for details.

Restoring a System Image

Use the following procedure to restore a system image to a managed server.

1. Place the target server into maintenance mode.
 - a. In the ROR console server resource tree, right-click the target server (or its physical OS or VM host) and select [Maintenance Mode]-[Set] from the popup menu.

The [Set Maintenance Mode] dialog is displayed.

As the target server is restarted during restoration, all of its applications should be stopped beforehand. When restoring a VM host, all of its VM guests should also be stopped.
 - b. Click <OK>.

The target server is placed into maintenance mode.

2. Restore a system image.

- To restore the system image from the server resource tree:

- a. In the ROR console server resource tree, right-click the target server (or its physical OS or VM host) and select [Backup/Restore]-[Restore] from the popup menu.

The [Restore] dialog is displayed.

- b. Select the system image to be restored.
- c. Click <OK>.

Restoration of the system image is started.

The process status can be checked in the Recent Operations area of the ROR console.

When <Cancel> is clicked in the Recent Operations area, the confirmation dialog to quit the process is displayed.

- To restore a system image from the [Image List] tab:

- a. In the ROR console, select the [Image List] tab.

The System Image List is displayed.

- b. Right-click the system image to be restored and select [Restore] from the popup menu.

The [Restore] dialog is displayed.

- c. Click <OK>.

Restoration of the system image is started.

The process status can be checked in the Recent Operations area of the ROR console.

When <Cancel> is clicked in the Recent Operations area, the confirmation dialog to quit the process is displayed.

When restoring a VM host, be sure to also restore the VM guest backups that correspond to the restored VM host backup version.

For details on restoring VM guests, refer to the server virtualization software manual.

3. Release the target server from maintenance mode before resuming its applications.

- a. In the ROR console server resource tree, right-click the target server (or its physical OS or VM host) and select [Maintenance Mode]-[Release] from the popup menu.

The [Release Maintenance Mode] dialog is displayed.

- b. Click <OK>.

The target server is released from maintenance mode.

Note

If the target VM host is in a high-availability configuration, all VM guests stored on shared disks should be migrated to another VM host beforehand.

During restore, because the target VM host will be automatically set to VM maintenance mode, the VM host should be in a state that allows VM maintenance mode to be set.

After restoring the VM host, migrate the VM guests back to their original VM host.

Refer to the server virtualization software manual and "E.3 Functional Differences between Products" of the "Setup Guide VE" for information on how to migrate VM guests, or about the VM maintenance mode.

Even when the restore operation is canceled, the target server cannot be returned to its previous status after the image is deployed.

When a Windows manager is to be used and the managed server has the following configuration, it may not be possible to perform backup correctly if the following command is not executed before performing backup.

- In a SAN data environment using a built-in disk boot, and a physical WWN or VIOM

```
>Installation_folder\Manager\bin\rxadm server set -name physical_server -attr bootagt=dos <RETURN>
```

- When using the Red Hat Enterprise Linux 6 ext4 file system or on a server using UEFI, and one of the following conditions is met
 - In a SAN boot environment using HBA address rename
 - When using a rack mount or tower server and the server is registered with "Disable" of "Association with server management software (ServerView)" is selected

```
>Installation_folder\Manager\bin\rxadm server set -name physical_server -attr bootagt=winpe <RETURN>
```

8.4 Viewing System Images

This section explains how to browse and view existing system image backups.

System images can also be listed using commands.

Refer to "Chapter 4 Image Operations" of the "Command Reference" for details.

In the ROR console, select the [Image List] tab.

The System Image List is displayed.

Figure 8.1 System Image List

Server Name	Version	Backup Date	Comments
HardSimulator-192-168-3-121	1	2010-05-07 11:34:00	-
HardSimulator-192-168-3-121	2	2010-05-07 20:58:00	-
HardSimulator-192-168-3-122	1	2010-05-07 11:34:00	-

Refer to "1.5.4 [Image List] Tab" of the "User's Guide VE" for details on the System Image List.

To view the most recent system image backup of a managed server, select a server OS from the server resource tree and click the [Resource Details] tab.

The latest system image backup collected from the selected server is displayed under "Latest System Image".

For details about system image information, refer to "1.5.2 [Resource Details] Tab" of the "User's Guide VE".

8.5 Deleting System Images

This section explains how to delete system image backups.

System images can also be deleted using commands.

Refer to "Chapter 4 Image Operations" of the "Command Reference" for details.

Deleting a System Image

Use the following procedure to delete a system image.

1. In the ROR console, select the [Image List] tab.
The System Image List is displayed.
2. In the System Image List, right-click the system image to delete and select [Delete] from the popup menu.
The [Delete a System Image] dialog is displayed.

3. Click <OK>.

The selected system image is deleted.

 Note

.....
A system image cannot be recovered once it has been deleted.
.....

Chapter 9 Hardware Maintenance

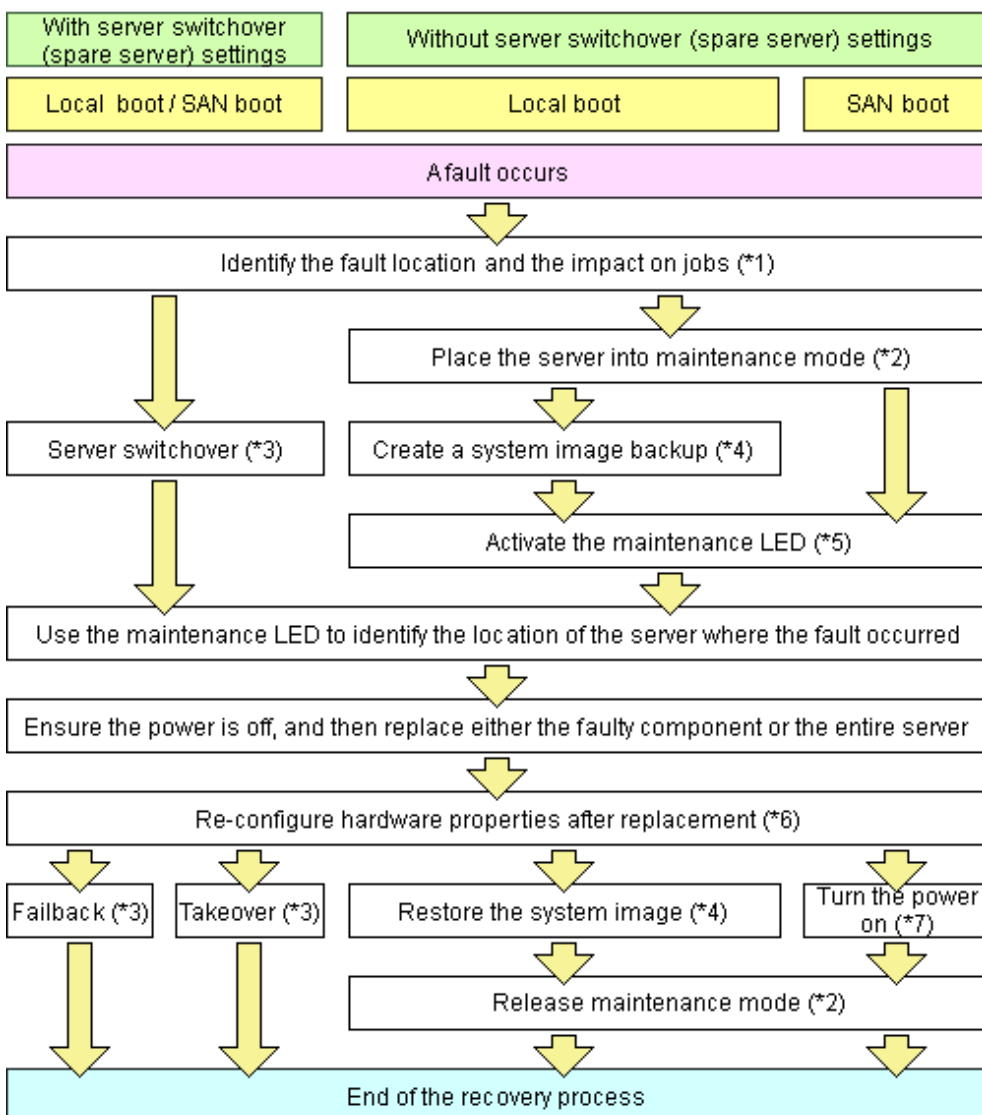
This chapter explains how to perform hardware maintenance.

9.1 Overview

This section explains how to perform maintenance on the hardware devices managed by Resource Orchestrator.

The following flowchart shows the procedure for maintaining hardware when failures occur on registered servers.

Figure 9.1 Hardware Maintenance Flow



*1: For details on how to identify failures, refer to "5.3 Addressing Resource Failures".

*2: For details on how to set and release maintenance mode settings, refer to "Appendix B Maintenance Mode" of the "User's Guide VE".

*3: For details on server switchover, failback, and takeover, refer to "Chapter 10 Server Switchover".

*4: For details on backing up and restoring system images, refer to "Chapter 8 Backup and Restore".

*5: For details on maintenance LED operations, refer to "9.2 Maintenance LEDs". Please note that maintenance LED operations are only supported for PRIMERGY BX servers.

*6: For details on re-configuring hardware properties, refer to "9.3 Re-configuring Hardware Properties".

*7: For details on power control, refer to "Chapter 6 Power Control".

The following hardware replacements can be performed:

- Replacing servers

Replace a server that has been registered in Resource Orchestrator.

For details on replacing servers, refer to ["9.4 Replacing Servers"](#).

- Replacing server components

Replace hardware components (such as a NIC, HBA, or hard disk) of a registered server.

For details on replacing or adding server components, refer to ["9.5 Replacing and Adding Server Components"](#).

- Replacing non-server hardware

Replace registered chassis, management blades, or any other hardware components external to servers.

For details on replacing non-server hardware, refer to ["9.6 Replacing Non-server Hardware"](#).

9.2 Maintenance LEDs

This section explains how to operate maintenance LEDs.

Activating a server blade's maintenance LED make it easy to identify a server from others. When replacing servers, it is recommended to use this function to identify which server blade should be replaced.

To activate the maintenance LED of a managed server running either a physical OS or a VM host, the server should be placed into maintenance mode first.

For details on the maintenance mode, refer to "Appendix B Maintenance Mode" of the "User's Guide VE".



- Maintenance LED control is only available for PRIMERGY BX servers. The actual LED used as an identification LED differs between server models.
 - For PRIMERGY BX600 servers, the power LED is used (blinks when activated).
 - For PRIMERGY BX900 servers, the ID indicator is used (lit when activated).
- If SNMP agent settings within the management blade configuration are incorrect, maintenance LED operations in Resource Orchestrator will end successfully, but the state of the identification LED will not change. SNMP agent settings should be set according to the instructions given in "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".

Activating a Maintenance LED

Use the following procedure to activate a server blade's maintenance LED.

1. In the ROR console server resource tree, right-click the target server, and select [LED]-[ON] from the popup menu.

The [Turning on Maintenance LED] dialog is displayed.

2. Click <OK>.

Selecting the "Automatically turn off" checkbox will automatically shut down the server after activating its maintenance LED.



Once the maintenance LED of a server blade is activated, new errors detected in that server cannot be checked from its LED anymore. Check the server status directly from the ROR console.

Deactivating a Maintenance LED

Use the following procedure to deactivate a server blade's maintenance LED.

1. In the ROR console server resource tree, right-click the target server, and select [LED]-[OFF] from the popup menu.

The [Turning off Maintenance LED] dialog is displayed.

2. Click <OK>.

The maintenance LED is turned off.

9.3 Re-configuring Hardware Properties

This section explains how to re-configure hardware properties for replaced hardware.

After hardware replacement, it is necessary to re-configure Resource Orchestrator with the new hardware properties.

For PRIMERGY BX servers, the hardware properties are automatically re-configured.



- Ensure this operation is performed only after the replacement of one of the following: a server itself, the NIC used for either the admin or public LAN, or the HBA.
If it is not, there is a possibility that operations on the server will not run correctly.
- When the system board or GSPB of a PRIMEQUEST server has been changed, ensure that this operation is performed.
If it is not, there is a possibility that operations on the server will not run correctly.
- After replacing the hardware, the server status becomes "unknown". The appropriate status can be restored by re-configuring the hardware properties from the server.

Prerequisites

The following prerequisites must be satisfied before this operation can be performed:

- Both the replaced server and replacement server must be the same model
A warning message is shown if the model of the replacement server differs from that of the replaced server.
- When replacing a PRIMERGY BX server, the replacement server must be inserted into the same slot as used for the replaced server
Hardware properties cannot be re-configured from a server inserted in a different slot. An error occurs if no server is inserted in the slot occupied by the previous server.
- The replaced server and replacement server must both be of the same blade type
If the blade types of the replaced and replacement servers are different, an error will occur.

To move a server to a different slot within a chassis, the server must be deleted first, and then registered again after being inserted in its new slot.

Pre-Configuration

For PRIMERGY BX servers, the hardware properties are automatically re-configured.

If automatic re-configuration is not necessary, delete the following file, and then restart the manager:

Placeholder for the Definition File

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvmr/customize_data

Name of the Definition File

auto_replace.rcxprop

Re-configuring Hardware Properties after Server Replacement

- For PRIMERGY BX servers

If the definition file has already been created, there is no need to set the hardware information again.

If the definition file has not been created, use the following procedure to re-configure properties for replaced hardware.

1. After hardware replacement, insert the server and check that the following message is displayed in the event log.

Server blade added

2. After approximately 30 seconds, right-click the target server in the ROR console server resource tree, and select [Hardware Maintenance]-[Re-configure] from the popup menu.

The [Re-configure Hardware Properties] dialog is displayed.

3. Click <OK>.

The original hardware properties of the selected managed server are updated with new hardware properties obtained from the replacement server. If the maintenance LED is on it will be turned off automatically.

- For Rack Mount and Tower Servers

Use the following procedure to re-configure properties for replaced hardware.

1. If the agent or ServerView Agents has already been registered, power on the server.

2. In the ROR console server resource tree, right-click the target server and select [Hardware Maintenance]-[Re-configure] from the popup menu.

The [Re-configure Hardware Properties] dialog is displayed.

3. Enter MAC addresses for the network interfaces used on the admin LAN.

This step can be skipped if no network interface was replaced.

- Admin LAN MAC Address (NIC1)

Required only if the agent is not registered.

- MAC address (NIC2) under SAN Boot/admin LAN redundancy

This item is only required for the following cases:

- When using the HBA address rename setup service
- When using GLS for admin LAN redundancy on the target server
- For the spare server of a managed server using admin LAN redundancy

4. Click <OK>.

The original hardware properties of the selected managed server are updated with new hardware properties obtained from the replacement server.

- For PRIMEQUEST Servers

Use the following procedure to re-configure properties for replaced hardware.

1. Replace the system board or GSPB, and insert the server.

2. After approximately 30 seconds, right-click the target server in the ROR console server resource tree, and select [Hardware Maintenance]-[Re-configure] from the popup menu.

The [Re-configure Hardware Properties] dialog is displayed.

3. Click <OK>.

The original hardware properties of the selected managed server are updated with new hardware properties obtained from the replacement server.

- For SPARC Enterprise Servers

Note that in this case there is no need to set the hardware information again.

Note

When registering an agent and performing backups of system images or cloning images, perform one of the following.

- Restart the managed server after reconfiguring the hardware properties
- Restart the related services described in "7.3 Starting and Stopping the Agent" of the "Setup Guide VE".

9.4 Replacing Servers

This section details the procedure to follow when replacing servers.

Information

- Follow the same procedure when replacing servers where VM hosts are running.
- No specific action is required in Resource Orchestrator when replacing admin servers or HBA address rename setup service servers.

For PRIMERGY BX servers

- Replacing a server assigned with spare servers

Use the following procedure to switch applications over to a spare server and replace a server with minimal interruption.

1. Perform server switchover

Switch over the server to replace with its spare server.

For details on the switchover function, refer to "[Chapter 10 Server Switchover](#)".

After the server has been switched over, its maintenance LED is automatically activated, and the server is powered down.

2. Replace the server

Replace the server whose maintenance LED is activated.

Change the BIOS settings of the replacement server to match the operating environment.

For details on BIOS settings, refer to "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".

Shut down the server after completing BIOS settings.

3. Re-configure hardware properties after replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.

For details on how to re-configure hardware properties, refer to "[9.3 Re-configuring Hardware Properties](#)".

After hardware properties have been re-configured, the maintenance LED is automatically turned off in the ROR console.

4. Perform post-server switchover operations

For details on the operations that must be performed after a server switchover, refer to "[10.3 Post-Switchover Operations](#)".

- Replacing a server with no spare server assigned

Use the following procedure to smoothly replace a server and resume its applications.

1. Place the server into maintenance mode

Place the primary server to replace into maintenance mode.

For details on the maintenance mode, refer to "Appendix B Maintenance Mode" of the "User's Guide VE".

2. Create a system image backup

For local boot servers, create a system image backup when possible.

For details and conditions of system image backups, refer to "[Chapter 8 Backup and Restore](#)".

In SAN boot environments, the boot disk can be restored without having to back up and restore a system image.

3. Activate the maintenance LED

Activate the maintenance LED on the server that is to be replaced before shutting it down.

For details on how to activate maintenance LEDs, refer to "[9.2 Maintenance LEDs](#)".

4. Replace the server

Replace the server whose maintenance LED is activated.

Change the BIOS settings of the replacement server to match the operating environment.

For details on BIOS settings, refer to "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".

Shut down the server after completing BIOS settings.

5. Re-configure hardware properties after replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.

For details on how to re-configure hardware properties, refer to "[9.3 Re-configuring Hardware Properties](#)".

After hardware properties have been re-configured, the maintenance LED is automatically turned off in the ROR console.

6. Restore the boot disk

- Local boot

There is no need to restore the boot disk if the original disk is installed on the replaced server. Simply power on the replacement server.

If the boot disk was replaced and a system image backup was collected, restore that backup.

Refer to "[8.3 Restoring System Images](#)" for details on how to restore a system image. After the system image is restored, the server will be automatically powered on.

If there is no backup of the system image, run the installation program again.

- SAN boot

As the replaced server can be easily configured to access the original boot disk using HBA address rename there is no need to restore the boot disk. Simply power on the replacement server.

7. Release maintenance mode

Release the replaced server from maintenance mode.

For details on the maintenance mode, refer to "Appendix B Maintenance Mode" of the "User's Guide VE".

- Servers with no agent registered

Use the following procedure to replace servers on which no Resource Orchestrator agent was registered.

1. Activate the maintenance LED

Activate the maintenance LED on the server that is to be replaced and shut down the server if it is still powered on.

For details on how to activate maintenance LEDs, refer to "[9.2 Maintenance LEDs](#)".

2. Replace the server

Replace the server whose maintenance LED is activated.

Change the BIOS settings of the replacement server to match the operating environment.

For details on BIOS settings, refer to "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".

Shut down the server after completing BIOS settings.

3. Re-configure hardware properties after replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.

For details on how to re-configure hardware properties, refer to "[9.3 Re-configuring Hardware Properties](#)".

After hardware properties have been re-configured, the maintenance LED is automatically turned off in the ROR console.

For Rack Mount and Tower Servers

- Replacing a server assigned with spare servers

Use the following procedure to switch applications over to a spare server and replace a server with minimal interruption.

1. Perform server switchover

Switch over the server to replace with its spare server.

For details on the switchover function, refer to "[Chapter 10 Server Switchover](#)".

The server to replace is automatically powered off after switchover.

2. Replace the server

Replace the server.

Change the BIOS settings of the replacement server to match the operating environment.

For details on BIOS settings, refer to "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".

Shut down the server after completing BIOS settings.

Configure the remote management controller of the replacement server with the same IP address, user name, password, and SNMP trap destination as those set on the original server.

3. Re-configure hardware properties after replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.

For details on how to re-configure hardware properties, refer to "[9.3 Re-configuring Hardware Properties](#)".

4. Perform post-server switchover operations

For details on the operations that must be performed after a server switchover, refer to "[10.3 Post-Switchover Operations](#)".

- Replacing a server with no spare server assigned

Use the following procedure to smoothly replace a server and resume its applications.

1. Place the server into maintenance mode

Place the primary server to replace into maintenance mode.

For details on the maintenance mode, refer to "Appendix B Maintenance Mode" of the "User's Guide VE".

2. Create a system image backup

For local boot servers, create a system image backup when possible.

For details and conditions of system image backups, refer to "[Chapter 8 Backup and Restore](#)".

In SAN boot environments, the boot disk can be restored without having to back up and restore a system image.

3. Power OFF

Shut down the server to replace if it is still powered on.

For details on shutting down servers, refer to "[Chapter 6 Power Control](#)".

4. Replace the server

Replace the server.

Change the BIOS settings of the replacement server to match the operating environment.

For details on BIOS settings, refer to "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".

Shut down the server after completing BIOS settings.

Configure the remote management controller of the replacement server with the same IP address, user name, password, and SNMP trap destination as those set on the original server.

5. Re-configure hardware properties after replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.

For details on how to re-configure hardware properties, refer to "[9.3 Re-configuring Hardware Properties](#)".

6. Restore the boot disk

- Local boot

There is no need to restore the boot disk if the original disk is installed on the replaced server. Simply power on the replacement server.

If the boot disk was replaced and a system image backup was collected, restore that backup.

Refer to ["8.3 Restoring System Images"](#) for details on how to restore a system image. After the system image is restored, the server will be automatically powered on.

If there is no backup of the system image, run the installation program again.

- SAN boot

The replaced server can be easily configured to access the original boot disk using I/O virtualization. Therefore, there is no need to restore the boot disk. Simply power on the replacement server.

7. Release maintenance mode

Release the replaced server from maintenance mode.

For details on the maintenance mode, refer to ["Appendix B Maintenance Mode"](#) of the ["User's Guide VE"](#).

- Servers with no agent registered

Use the following procedure to replace servers on which no Resource Orchestrator agent was registered.

1. Power OFF

Shut down the server to replace if it is still powered on.

For details on shutting down servers, refer to ["Chapter 6 Power Control"](#).

2. Replace the server

Replace the target server.

Change the BIOS settings of the replacement server to match the operating environment.

For details on BIOS settings, refer to ["4.1.2 Configuring the Server Environment"](#) of the ["Setup Guide VE"](#).

Shut down the server after completing BIOS settings.

Configure the remote management controller of the replacement server with the same IP address, user name, password, and SNMP trap destination as those set on the original server.

3. Re-configure hardware properties after replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.

For details on how to re-configure hardware properties, refer to ["9.3 Re-configuring Hardware Properties"](#).

For SPARC Enterprise Servers

- Replacing a server assigned with spare servers

Use the following procedure to switch applications over to a spare server and replace a server with minimal interruption.

- When replacing an HBA

1. Perform server switchover

Switch over the server to replace with its spare server.

For details on the switchover function, refer to ["Chapter 10 Server Switchover"](#).

The server to replace is automatically powered off after switchover.

2. Replace the server

Replace the HBA of the server.

Change the OBP settings of the replacement server to match the operating environment.

For details on OBP settings, refer to ["4.1.2 Configuring the Server Environment"](#) of the ["Setup Guide VE"](#).

Shut down the server after completing OBP settings.

Configure the remote management controller of the replacement server with the same IP address, user name, password, and SNMP trap destination as those set on the original server.

3. Change the WWN information settings

Change the WWN information settings for after server replacement to the WWN value of the HBA after server replacement.

Leave the value of the target CA as the one before changes were made.

4. Perform post-server switchover operations

For details on the operations that must be performed after a server switchover, refer to ["10.3 Post-Switchover Operations"](#).



Note

If takeover was performed before replacement of the HBA, release the spare server settings. Change the WWN information settings following the procedure in "Replacing a server with no spare server assigned".

- When not replacing an HBA

1. Perform server switchover

Switch over the server to replace with its spare server.

For details on the switchover function, refer to "[Chapter 10 Server Switchover](#)".

The server to replace is automatically powered off after switchover.

2. Replace the server

Replace components (other than the HBA) of the server.

Change the OBP settings of the replacement server to match the operating environment.

For details on OBP settings, refer to "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".

Shut down the server after completing OBP settings.

Configure the remote management controller of the replacement server with the same IP address, user name, password, and SNMP trap destination as those set on the original server.

3. Perform post-server switchover operations

For details on the operations that must be performed after a server switchover, refer to "[10.3 Post-Switchover Operations](#)".

- Replacing a server with no spare server assigned

When WWN information has been configured, use the following procedure to change the WWN information to that of the WWPN value of the replaced HBA.

1. Delete the target CA

When there are target CA settings in the WWN information, stop the server and then delete the target CA settings (set them as hyphens ("-")).

2. Replace the server

Replace the HBA of the server.

Change the OBP settings of the replacement server to match the operating environment.

For details on OBP settings, refer to "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".

Shut down the server after completing OBP settings.

When the target CA was deleted in step 1., configure zoning and host affinity settings in the WWPN value of the replacement HBA.

For details, refer to the ESC users guide.

3. Change the WWN information settings

Change the WWN information settings for after server replacement to the WWN value of the HBA after server replacement.

When the target CA was deleted in step 1., configure a new target CA.

After configuration, restart the server.

After starting the server, check the status of the server's HBA from ESC.

When the HBA status is "unknown", delete it.

When the HBA status is displayed as "access path inheritance is required" (yellow icon), perform access path inheritance.

For details, refer to the ESC users guide.

When the target CA was not deleted in step 1., configure the target CA as a hyphen ("-").

For PRIMEQUEST Servers

- Replacing a server assigned with spare servers

Use the following procedure to switch applications over to a spare server and replace a server with minimal interruption.

1. Perform server switchover

Switch over the server to replace with its spare server.
For details on the switchover function, refer to "[Chapter 10 Server Switchover](#)".
The server is automatically powered off after switchover.

2. Replace the server

Replace the server.
Use the Maintenance Wizard of the Management Board Web-UI to perform replacement.
For details on the Maintenance Wizard, refer to the PRIMEQUEST manual.
Also, change the BIOS settings of the replacement server to match the operating environment.
For details on BIOS settings, refer to "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".
Shut down the server after completing BIOS settings.

3. Re-configure hardware properties after replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.
For details on how to re-configure hardware properties, refer to "[9.3 Re-configuring Hardware Properties](#)".

4. Perform post-server switchover operations

For details on the operations that must be performed after a server switchover, refer to "[10.3 Post-Switchover Operations](#)".

- Replacing a server with no spare server assigned

Use the following procedure to smoothly replace a server and resume its applications.

1. Place the server into maintenance mode

Place the primary server to replace into maintenance mode.
For details on the maintenance mode, refer to "Appendix B Maintenance Mode" of the "User's Guide VE".

2. Create a system image backup

For local boot servers, create a system image backup when possible.
For details and conditions of system image backups, refer to "[Chapter 8 Backup and Restore](#)".
In SAN boot environments, the boot disk can be restored without having to back up and restore a system image.

3. Power OFF

Shut down the server to replace if it is still powered on.
For details on shutting down servers, refer to "[Chapter 6 Power Control](#)".

4. Replace the server

Replace the server.
Use the Maintenance Wizard of the Management Board Web-UI to perform replacement.
For details on the Maintenance Wizard, refer to the PRIMEQUEST manual.
Also, change the BIOS settings of the replacement server to match the operating environment.
For details on BIOS settings, refer to "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".
Shut down the server after completing BIOS settings.

5. Re-configure hardware properties after replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.
For details on how to re-configure hardware properties, refer to "[9.3 Re-configuring Hardware Properties](#)".

6. Restore the boot disk

- Local boot

There is no need to restore the boot disk if the original disk is installed on the replaced server. Simply power on the replacement server.
If the boot disk was replaced and a system image backup was collected, restore that backup.
Refer to "[8.3 Restoring System Images](#)" for details on how to restore a system image. After the system image is restored, the server will be automatically powered on.
If there is no backup of the system image, run the installation program again.

- SAN boot

As the replaced server can be easily configured to access the original boot disk using HBA address rename there is no need to restore the boot disk. Simply power on the replacement server.

7. Release maintenance mode

Release the replaced server from maintenance mode.

For details on the maintenance mode, refer to "Appendix B Maintenance Mode" of the "User's Guide VE".

- Servers with no agent registered

Use the following procedure to replace servers on which no Resource Orchestrator agent was registered.

1. Power OFF

Shut down the server to replace if it is still powered on.

For details on shutting down servers, refer to "[Chapter 6 Power Control](#)".

2. Replace the server

Replace the server.

Use the Maintenance Wizard of the Management Board Web-UI to perform replacement.

For details on the Maintenance Wizard, refer to the PRIMEQUEST manual.

Also, change the BIOS settings of the replacement server to match the operating environment.

For details on BIOS settings, refer to "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".

Shut down the server after completing BIOS settings.

3. Re-configure hardware properties after replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.

For details on how to re-configure hardware properties, refer to "[9.3 Re-configuring Hardware Properties](#)".

9.5 Replacing and Adding Server Components

This section explains how to replace and add server components.

- **Replacing and Adding Network Interfaces (Admin LAN, Public LAN)**

The procedure used to replace and add network interfaces is the same as that described in "[9.4 Replacing Servers](#)".

For details, refer to "[9.4 Replacing Servers](#)".

When adding or removing network interfaces, if the target server is running Red Hat Enterprise Linux 5 or Citrix XenServer, after completing the steps described in "[9.4 Replacing Servers](#)", log in with administrative privileges on the managed server and execute the following command.

```
# /usr/local/sbin/macbindconfig create <RETURN>
```

[Xen]

When using Citrix XenServer, reinstall XenServer referring to the Citrix XenServer manual.

When using Red Hat Enterprise Linux 5 Virtualization (Xen-Based), perform the following procedure.

1. Execute the following command to temporarily disable automatic startup of the xend daemon and then restart the managed server.

```
# chkconfig xend off <RETURN>
```

2. Once the server has restarted, execute the following commands to update MAC address bindings, re-enable automatic startup of the xend daemon, and restart the xend daemon itself.

```
# /usr/local/sbin/macbindconfig create <RETURN>
# chkconfig xend on <RETURN>
# service xend start <RETURN>
```

[Linux]

When the configuration of server components has been changed, check the configuration file of the OS, and make any necessary corrections. For details, refer to "Configuration File Check" in "2.2.1.1 Software Preparation and Checks" of the "Installation Guide VE".

[Red Hat Enterprise Linux 6]

When adding or removing network interfaces, if the target server is running Red Hat Enterprise Linux 6, after completing the steps described in "9.4 Replacing Servers", modify the configuration file.

For details, refer to "Configuration File Check" in "2.2.1.1 Software Preparation and Checks" of the "Installation Guide VE".

- Replacing a GSPB

The procedure used to replace a GSPB is the same as that described in "Replacing a network interface".

Replace NIC with GSPB in the procedure.

- Replacing an HBA

The procedure used to replace an HBA is the same as that described in "9.4 Replacing Servers".

- When using I/O virtualization, the replacement HBA will automatically inherit the WWN originally set on the replaced HBA. Therefore, there is no need to re-configure access paths on the storage side.
- When configuring WWN information, it is necessary to change WWN information settings to the replaced HBA WWN values. Refer to "3.2.11 Changing WWN Settings for ETERNUS SF Storage Cruiser Integration" of the "User's Guide VE" for details on how to change WWN information.

- Replacing a boot disk (in local boot environments)

Use the following procedure to replace a boot disk.

1. Replace the faulty boot disk with a new one.
2. If the boot disk's content was backed up, restore it.



Information

The backup and restore functions available in Resource Orchestrator can be used to restore the boot disk contents.

For details, refer to "Chapter 8 Backup and Restore".

- Replacing a system board

The procedure used to replace a system board is the same as that described in "9.4 Replacing Servers".

- Replacing an IO board

No specific action is required in Resource Orchestrator when replacing an IO board.

- Replacing other server components

No specific action is required in Resource Orchestrator when replacing onboard server components like memory modules or other parts.

9.6 Replacing Non-server Hardware

This section explains how to replace hardware external to servers.

- Replacing chassis

No specific action is required in Resource Orchestrator.

- Replacing management blades

No specific action is required in Resource Orchestrator.

- Replacing management boards

No specific action is required in Resource Orchestrator.

- Replacing LAN switch blades

No specific action is required for PRIMERGY BX900/BX400 LAN switch blades in IBP mode.

For other LAN switch blades of PRIMERGY BX models, after replacing a switch blade, update the new LAN switch blade with the VLAN settings that were previously configured in Resource Orchestrator.

Use the following procedure to replace a LAN switch blade.

1. Replace the faulty LAN switch blade.
2. Restore the LAN switch blade configuration backup (which includes all of the LAN switch blade settings) to the new LAN switch blade.

If the LAN switch blade configuration was not been backed up in advance, it has to be restored by configuring each setting (except VLAN settings) to the same values set during the initial installation.

Refer to the manual of the LAN switch blade used for details on how to back up and restore LAN switch blade configurations.

3. Update the new LAN switch blade with the latest VLAN settings configured in Resource Orchestrator.
 - a. In the ROR console server resource tree, right-click the target LAN switch, and select [Restore] from the popup menu.
The [Restore LAN Switch] dialog is displayed.
 - b. Click <OK>.
VLAN settings are applied to the specified LAN switch blade.

Note

To replace LAN switch blades with different models, first delete the registered LAN switch blade, and then register the replacement LAN switch blade.

After the LAN switch blade is registered, the VLAN settings must be configured for the internal and external ports.

For details on the VLAN settings, refer to "2.3.4 Configuring VLANs on LAN Switch Blades" of the "User's Guide VE".

When changing from IBP to another mode, or vice versa, when using a PRIMERGY BX900/BX400 series LAN switch blade, delete the registered LAN switch blade and register it again.

- Replacing Fibre Channel switch blades

No specific action is required in Resource Orchestrator.

- Replacing power monitoring devices (PDU or UPS)

After replacing a power monitoring device, re-configure the power monitoring device's (PDU or UPS) hardware properties.

Use the following procedure to replace a power monitoring device.

1. Replace the faulty power monitoring device.
2. Set the admin LAN IP address and SNMP community on the replacement device to the same values as those that were set on the faulty device.
3. Re-configure the power monitoring device's hardware properties.

- a. In the ROR console server resource tree, right-click the target power monitoring device (PDU or UPS), and from the popup menu, select [Hardware Maintenance]-[Re-configure].

The [Re-configure Hardware Properties] dialog is displayed.

- b. Click <OK>.

The target power monitoring device's hardware properties are re-configured.

- Replacing storage blades

No specific action is required in Resource Orchestrator when replacing a storage blade that does not contain the boot disk of a server blade.

Use the following procedure to replace a storage blade that contains the boot disk of a server blade.

1. Replace the storage blade.

2. Insert the server blade's boot disk in the new storage blade.
3. If the boot disk's content was backed up, restore it.



Information

The backup and restore functions available in Resource Orchestrator can be used to restore the boot disk contents. For details, refer to "[Chapter 8 Backup and Restore](#)".

- **Replacing LAN switches**

No specific action is required in Resource Orchestrator when replacing a LAN switch.

Chapter 10 Server Switchover

This chapter explains how to use the server switchover function.

10.1 Overview

Server switchover is a function that enables applications to be switched over to and restarted on a pre-assigned spare server when a primary server fails or needs to be shut down for maintenance.

Server switchover is the basis for the Auto-Recovery function, which is able to automatically switch over applications to a spare server upon failure.

Server switchover settings must be configured before using the server switchover function.

For details on server switchover settings and an overview of the server switchover function, refer to "Chapter 8 Server Switchover Settings" of the "User's Guide VE".



Note

- When the switchover method is backup and restore

When backing up or restoring system images, or collecting and deploying cloning images, up to four processes can be executed simultaneously. If four processes are already being executed, any system image restore triggered by a switchover or failback operation will enter a standby state.

Any process put under standby state will be resumed after one of the already running processes completes.

- When the MAK method is used for license authentication

The license authentication may be requested again after server switchover or failback operations. In such cases, authenticate again as quickly as possible.

10.2 Switchover

A server switchover can be triggered either manually from the user, or automatically with the Auto-Recovery function.

Regardless of what triggered a switchover, the user must decide whether to switch back applications to their original server (failback), or let the spare server indefinitely take over those applications (takeover). Choosing takeover will result in the spare server becoming the new active server.

For details, refer to "10.3 Post-Switchover Operations".

Different switchover methods are available according to each managed server's hardware configuration.

For details, refer to the "Note" in "1.5 Hardware Environment" of the "Setup Guide VE".



Note

- In configurations where a server OS is operating on a spare server, if the boot methods of primary servers and spare servers are different, server switchover may fail and damage the primary server OS. Ensure that the boot methods are the same.

- During switchover, server restarts and configuration changes may trigger SNMP Traps (which are shown in the Event Log). For details, refer to "Chapter 1 Resource Orchestrator Messages" of the "Messages VE".

- When using the backup and restore switchover method, do not start up the original primary server during or after the switchover operation.

The primary server and spare server both run the same system image. Having the two servers running together will cause conflicts of IP addresses and other information. This can adversely affect the applications recovered on the spare server.

If it becomes necessary to start the primary server, for maintenance or other tasks, ensure that it does not start up from the same system image as that of the spare server. This can be done by turning off the spare server first, or by stopping the primary server at its BIOS screen (before startup of the OS).

- When using PRIMERGY BX servers, the maintenance LED of a switched over server is automatically activated.
- If switchover takes place when a spare server is operating, the spare server is turned off.

- When switching over to the spare server of a VM host, the VM host of the spare server will be placed into VM maintenance mode.
- After shutting down a spare server, if the power is not turned off within 15 minutes, the spare server will be forcibly powered off.

Auto-Recovery

- For PRIMERGY BX servers and PRIMEQUEST

By enabling Auto-Recovery in the spare server settings of a server, it will be automatically switched over to a spare server when its status changes to either "error" or "fatal", and no response is obtained from its OS.

- For rack mount, tower servers, and SPARC Enterprise

By enabling Auto-Recovery in the spare server settings of a server, it will be automatically switched over to a spare server when it receives an "Error" level SNMP trap, and no response is obtained from its OS.

For the decision criteria for whether an OS has stopped, refer to "8.4 Conditions Required for Auto-Recovery" of the "User's Guide VE".

Manual Switchover

Use the following procedure to manually switch over applications from a primary server to a spare server.

Manual switchover can be either performed at will when necessary, or to verify that the switchover process operates properly.

For details on the conditions for a server switchover, refer to "Conditions for Server Switchover" in "8.3 Server Switchover Conditions" of the "User's Guide VE".

1. In the ROR console server resource tree, right-click the physical OS or VM host to be switched, and select [Spare Server]-[Switchover] from the popup menu.

The [Execute Switchover Operation] dialog is displayed.

2. Select the switchover destination server.

If "Automatic allocation" is selected, the switchover destination server is automatically selected.

3. Click <OK>.

The configuration for server switchover is started. The process status can be checked in the Recent Operations area of the ROR console. The primary server stops, and the physical OS or VM host starts on the spare server. For the backup and restore method, clicking <Cancel> in the Recent Operations area displays the confirmation dialog.



Note

If the server switchover/failback operation is canceled, the original server will be powered off. To continue server operations, power on the server. If the server switchover/failback operation is canceled, OS images that have the same information (such as IP addresses) as that of the original server may remain on the internal disk of the destination server.



Information

- Manual switchover can be performed regardless of the status of the primary server.
- If "Automatic allocation" is selected for Auto-Recovery or manual switchover, the spare server to be allocated will be selected based on the following order of priority:
 1. Physical servers with no settings configured
 2. Physical servers for which HBA address rename information or a VIOM server profile is configured
 3. Physical servers with no agents registered

Spare servers are selected based on the names of their physical servers, in the following order of priority.

1. "-"

2. Numbers
 3. Uppercase letters
 4. Lowercase letters
-

10.3 Post-Switchover Operations

After a switchover was performed (either manually or automatically), perform either one of the following post-switchover recovery procedures.

For details on how to replace hardware, refer to "[Chapter 9 Hardware Maintenance](#)".

When using the storage affinity switchover method, confirm the HBA status of servers on ESC, before recovering them using Resource Orchestrator.

- When the HBA status before switchover is "unknown"

Delete the HBA.

- When the HBA status is displayed as "access path inheritance is required" (yellow icon) after switchover

Perform access path inheritance.

For details, refer to the ESC users guide.

- When performing "[Failback](#)"

Perform the following operations.

1. Replace failed server hardware to recover.
2. Perform "[Failback](#)" to keep the configuration created before server switchover.

When using the storage affinity switchover method, after performing failback operations, confirm the HBA status of servers on ESC and perform the same corrective actions as performed after switchover. After performing corrective action, for a spare server that had an agent registered, restore the zoning of spare servers and host affinity configurations for storage units following the procedures described in "Information".

- When performing "[Takeover](#)"

Perform the following operations.

1. Replace failed server hardware to recover.
2. Perform "[Takeover](#)" to keep the configuration created by a server switchover.

When using storage affinity switchover methods and a spare server that had an agent registered, restore the zoning of spare servers and host affinity configurations for storage units following the reference procedures in "Information" below.

Information

For a server takeover procedure, server hardware can be replaced either before or after the "[Takeover](#)" operation.

Use the following procedures to restore the zoning of spare servers and host affinity configurations for storage units in the storage affinity switchover methods.

1. Check the zoning and host affinity configurations for spare servers using the zoning and host affinity information displayed in "WWN Settings" of the [Resource Details] tab.
2. Use the `storageadm zone info` command to confirm the zoning and host affinity configurations.
3. Use the `storageadm zone add/delete` command to confirm the zoning of spare servers and host affinity configurations.

For details on how to use the `storageadm zone` command, refer to the "ETERNUS SF Storage Cruiser User's Guide".

Note

When the failed server is a VM host, that VM host will be placed into VM maintenance mode. After restoring the failed server and executing "Failback" or "Takeover", in order to use the failed server, release the VM maintenance mode if necessary.

Failback

Use the following procedure to return to a pre-switchover configuration.

For details on the conditions for server failback, refer to "Conditions for Server Failback" in "8.3 Server Switchover Conditions" of the "User's Guide VE".

1. In the ROR console server resource tree, right-click the physical OS or VM host that was switched over to the spare server, and select [Spare Server]-[Failback] from the popup menu.

The [Failback] dialog is displayed.

2. Click <OK>.

The configuration for server switchover is started. The process status can be checked in the Recent Operations area of the ROR console. The spare server is stopped and the server OS is switched back to the primary server. For the backup and restore method, clicking <Cancel> in the Recent Operations area displays the confirmation dialog.

Note

- If the server switchover/failback operation is canceled, the original server will be powered off. To continue server operations, power on the server. OS images that have the same information (such as IP addresses) as that of the original server may remain on the internal disk of the destination server.
- When using the backup and restore switchover method, do not start up the original spare server during or after the failback operation. As the primary server and spare server both run the same system image, having the two servers running together will cause conflicts of IP addresses and other information. This can adversely affect the applications switched back to the spare server. If it becomes necessary to start the primary server, for maintenance or other tasks, ensure that it does not start up from the same system image as that of the spare server. This can be done by turning off the primary server first, or by stopping the spare server at its BIOS screen (before startup of the OS).
- When using the backup and restore switchover method, and it is necessary to transfer newly generated data from the spare server to the primary server, back up the spare server before performing the failback. Refer to "Backing up a System Image" in "8.2 Backup", and replace the "managed server" with "spare server". Unless there is a need to keep the data that was generated on the spare server while active, backup of the spare server can be skipped. In that case, a system image backed up prior to failure will be restored to the primary server.
- When using PRIMERGY BX servers, the maintenance LED of a primary server is automatically deactivated after a server failback.
- When the spare server is using I/O virtualization, the spare server will be powered on after failback.

Takeover

Use the following procedure to keep the configuration created by a server switchover:

1. In the ROR console server resource tree, right-click the physical OS or VM host that was switched over to the spare server, and select [Spare Server]-[Takeover] from the popup menu.

The [Takeover] dialog is displayed.

2. Click <OK>.

The spare server continues operating as the primary server and the server that functioned as the primary server before switchover becomes a spare server.

If the spare server was originally shared by multiple primary servers, all those servers will now use the original primary server as their spare server.



Example

1. Status before switchover

Application 1: Server A (active) - Server B (spare)

Application 2: Server C (active) - Server B (spare)

2. Status after a fault in Server A triggered a switchover of Application 1

Application 1: Server A (fault) - Server B (active)

Application 2: Server C (active) - Server B (*1)

3. Status after replacing Server A and letting Server B take over Application 1

Application 1: Server B (active) - Server A (spare)

Application 2: Server C (active) - Server A (spare)

*1: At this point, manual switchover or Auto-Recovery from Server C to Server B becomes impossible.



Note

Once server switchover has taken place, Auto-Recovery and manual server switchover cannot be performed until either failback or takeover has been executed.

Perform either failback or takeover to enable switchover to be performed again.

When the managed server is PRIMEQUEST, set the PSA-MMB IP address after deployment. For details, refer to the PRIMERGY Partition Model manual.

Chapter 11 Maintaining Software with Cloning [Windows/Linux]

This chapter explains how to perform software maintenance using server cloning.

11.1 Overview

Cloning servers allows users to apply patches and install or modify installed software on a managed server before propagating those changes to other servers.

After performing necessary maintenance tasks on one managed server, a cloning image can be collected from that server and deployed to other managed servers. This minimizes the time required for the software maintenance of multiple managed servers while reducing the risk of mistakes during operation.

Using the network parameter auto-configuration function also enables automatic configuration of public LAN settings for each cloned server. This is done by re-configuring the network interfaces used for the public LAN following deployment of a cloning image.

For details on the cloning function, refer to "Chapter 7 Cloning [Windows/Linux]" of the "User's Guide VE".



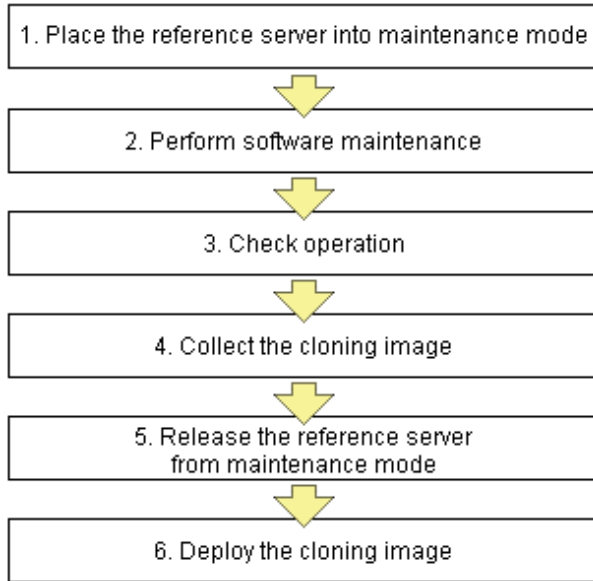
- Software maintenance tasks performed using the cloning function only apply to servers that share the same hardware and software configuration.
 - Deployment of a cloning image will reset the VLAN settings used for the public LAN of each target server. Those settings need to be restored either manually or automatically using the network parameter auto-configuration function.
 - The following data will also be reset on the servers to which a cloning image is deployed. If necessary, this data should be manually backed up (copied) before deployment, and restored once complete.
 - OS system log
 - Application settings and logs
-

11.2 Software Maintenance Procedure

This section explains how to perform maintenance operations on managed servers.

Maintenance operations should be performed first on one reference server before propagating changes to the remaining target servers.

Figure 11.1 Software Maintenance Procedure Using Cloning



Each of these steps is explained below.

1. Place the reference server into maintenance mode

- a. Stop all applications on the target server.
- b. In the ROR console server resource tree, right-click the target server (or its physical OS or VM host) and select [Maintenance Mode]-[Set] from the popup menu.
For details on the maintenance mode, refer to "Appendix B Maintenance Mode" of the "User's Guide VE".

2. Perform software maintenance

Perform the necessary software maintenance tasks (such as patch application, or software addition or modification) on the reference server.

3. Check operation

After completion of maintenance tasks, confirm that the OS and applications still operate properly to validate the changes made during maintenance.

4. Collect the cloning image

Once all changes have been validated, collect a cloning image from the reference server.
For details on collecting cloning images, refer to "7.2 Collecting a Cloning Image" of the "User's Guide VE".

5. Release the reference server from maintenance mode

Release the managed server from maintenance mode.
In the ROR console server resource tree, right-click the server (or physical OS or VM host on the server) to be released from maintenance mode, and select [Maintenance Mode]-[Release] from the popup menu.
For details on the maintenance mode, refer to "Appendix B Maintenance Mode" of the "User's Guide VE".

6. Deploy the cloning image

Propagate the changes made during maintenance by deploying the cloning image collected in step 4. to the remaining target servers.
For details on how to deploy cloning images, refer to "7.3 Deploying a Cloning Image" of the "User's Guide VE".

Chapter 12 Network Map

This chapter provides an overview of the Network Map and describes its features.

12.1 Overview

The Network Map displays the following information for resources managed in Resource Orchestrator.

- Network configuration of physical and virtual servers (including virtual switches and VM guests)
- Statuses of network links between all resources
- VLAN configuration affecting each physical and virtual server

Two different maps (listed below) are available within the Network Map. Switch between the maps as necessary.

- Overall map

Displays chassis, servers, and their connections (network links) with adjacent LAN switches.

- Local map

Shows a more detailed map focused on the selected resource (chassis or server). This map displays resources contained in the selected resource (e.g. server blades, LAN switch blades, VM hosts, VM guests, virtual switches), and their connections (links) with adjacent LAN switches or chassis. Up to two chassis can be displayed at a time.

In the Network Map, resource icons are used to represent the status of each resource. Moreover, different colors are used to represent different link statuses.

The network map creates physical/logical links by searching the related resources.

When there are more resources (chassis, physical/virtual servers, NICs, physical/virtual switches and ports), the number of network links increases, and it takes more time for drawing. (*1)

These drawing operations are performed when displaying overall maps and local maps, and when updating networks automatically (at one-minute intervals).

When updating the network map automatically, drawing operations cannot be accepted.

When stopping the automatic update after once displaying the network map, network link operations are possible without being affected by drawing operations.

The automatic update configurations are recorded in the browser, and taken over when login is performed again.

*1: As a guide, it takes about 1 to 10 minutes for drawing in environments with 100 to 1,500 physical/virtual servers. This changes depending on the workload of the admin server or admin client.



See

- For details on resource icons, refer to "[12.4 Resource Icons](#)".
- For details on link statuses, refer to "[12.5 Network Links](#)".
- Operations of the ROR console may not be able to be executed when updating the network map automatically.

Stop automatic update by clearing the "Automatic Updates" checkbox, and then operations of the ROR console will be able to be executed during updating of the network map.

In order to update the network map to show the latest status, click the update button.



Note

As Windows bridge connections are not supported, network links will not be displayed.

The following actions are available in the Network Map.

- Switching between map types

- Screen scrolling
 - Scroll button
 - Map drag and drop
 - Navigation map drag and drop
- Maximizing and minimizing of the display area
- Configuring automatic update to show the latest status
- Updating to show the latest status
- Hiding of the navigation map
- Hiding of display filter options
- Showing or hiding of the following information
 - Resource descriptions
 - Network links
 - VLANs
- Resetting to initial display
- Highlighting of a selected resource
- Showing or hiding of details for the following resources
 - Servers (including VM hosts)
 - LAN switches
 - VM guests
 - Virtual switches

12.2 Preparations

The following preparations are required to add display content to the Network Map.

1. Register LAN switches (LAN switch blades included in a chassis or external switches)

For details on the registration method, refer to "2.4.2 Registering LAN Switches" of the "User's Guide VE".
The following LAN switches are supported by the Network Map.

- BX600 GbE Switch Blade 30/12
 - PY CB Eth Switch/IBP 1Gb 36/12
 - PY CB Eth Switch/IBP 1Gb 36/8+2
 - PY CB Eth Switch/IBP 1Gb 18/6
 - PY CB Eth Switch/IBP 10Gb 18/8
 - Cisco Catalyst 2950 series
 - Cisco Catalyst 2960 series
 - Cisco Catalyst 3560 series
 - Cisco Catalyst 3750 series
2. Detect physical network links
 - a. From the ROR console menu, select [Tools]-[Topology]-[Detect physical links].
The [Detect Physical Links] dialog is displayed.
 - b. Click <OK>.

Note

- If no LAN switch blades have been registered, only network links between external LAN switches will be displayed. If only one external switch is registered, no network links will be displayed at all.
- If a non-supported LAN switch is registered, network links may not be properly displayed for that switch.
- The Network Map cannot display network links between BX600 GbE Switch Blade 30/12 and the following LAN switch blades:
 - PY CB Eth Switch/IBP 1Gb 36/12
 - PY CB Eth Switch/IBP 1Gb 36/8+2
 - PY CB Eth Switch/IBP 1Gb 18/6
- Links between two supported LAN switches may not be displayed properly if an un-registered or un-supported LAN switch is placed between them.

Example

In such a case, the following inconsistencies may be displayed. A LAN switch port maybe seen as being connected to multiple switches (multiple links are shown attached to that switch port).

12.3 Screen Layout

This section describes the Network Map's layout.

The main part of the Network Map is the network view.

12.3.1 Network Map Layout

This section describes the Network Map's layout.

Network view

Shows the statuses of registered resources and the network links between them.

Map selection area

Provides buttons to select which map to display (overall map or local map).

Scroll button

Scrolls the network view into the selected direction (up, down, left, or right).

Reset button

Resets the network view to its initial display.

Magnification slider

Maximizes or minimizes the network view.

"Automatic Updates" checkbox

To configure automatic updating of the network map, check the checkbox.

Clearing the checkbox stops automatic updating of the network map.

Update button

Update the network map to show the latest status.

Display filter area

Provides checkboxes to select which information to display in the network view.

Map navigation area

Shows a zoomed-out version of the selected map (including items which are too far away to be displayed in the network view).

VLAN display area

Displays the selected VLAN ID in the VLAN tree.

12.3.2 Map Types

This section explains the different types of map available.

Overall map

The overall map displays links between chassis, servers, and adjacent LAN switches for all the resources managed in Resource Orchestrator.

Local map button

Selecting a resource icon in the network view will show a button on the upper-right side of this icon. Clicking this button shows the local map.



.....

The local map and overall map buttons in the map selection area are initially disabled. Selecting a chassis in the network view enables them.

.....

Local map

The local map displays all resources contained in the selected resource, as well as their connections (network links) with other resources.



-
- Up to two chassis can be expanded in the local map.
 - When two chassis are already expanded, expanding a new one will close the chassis that was expanded first.
-

- When selecting a chassis

The following items are displayed:

- Server blades
- VM hosts
- VM guests
- Virtual switches
- LAN switch blades
- LAN switches connected to LAN switch blades
- Chassis connected to LAN switches
- Network links

- When selecting a server

The following items are displayed:

- NICs

In addition, the following items will be displayed when the selected server is a VM host:

- VM guests
 - Virtual switches
 - Ports
 - Network links
- When selecting a LAN switch blade

The following items are displayed:

- Ports

Selecting a LAN switch blade will show all its ports. For PRIMERGY BX900/BX400 LAN switch blades operating in IBP mode, a list of port groups is displayed. Selecting a port group from the list will highlight (in blue) the ports belonging to the selected port group.

Moreover, selecting a port from a switch in IBP mode will show a list of port groups to which the selected port belongs. If the selected port belongs to more than one port group, all port groups are shown in the displayed list.

Expand button

Selecting an item listed below will show this button on the upper-right side of this icon. Clicking this button expands the resource contents.

- Server blade
- LAN switch blade
- VM server
- VM guest
- Virtual switch
- LAN switch

Close button

Clicking this button closes expanded chassis contents, replacing them with a chassis icon.



Clicking the close button will close the detailed content (server blades, LAN switch blades) that was shown for the selected chassis.


12.4 Resource Icons

This section describes the icons used to represent resource statuses on BladeViewer.

12.4.1 Resource Statuses

The following table details the resource statuses associated with each icon.

Table 12.1 Chassis Icons

Icon	Status	Meaning
	normal	No new errors or warnings were detected from the chassis.




Icon	Status	Meaning
	warning	A warning was detected from the chassis.
	unknown	The status of the chassis could not be obtained.
	error	An error was detected from the chassis.
	fatal	A fatal error was detected from the chassis, which is now unusable.
	stop	The chassis was detected to have been powered off.

Table 12.2 Server Icons













Icon	Status	Meaning
	normal	No new errors or warnings were detected from the server.
	warning	A warning was detected from the server.
	unknown	The status of the server could not be obtained.
	error	An error was detected from the server.
	fatal	A fatal error was detected from the server, which is now unusable.
	stop	The server was detected to have been powered off.

Table 12.3 LAN Switch Blade Icons

Icon		Status	Meaning
	 (*1)	normal	No new errors or warnings were detected from the LAN switch blade.

Icon		Status	Meaning
	 (*1)	warning	A warning was detected from the LAN switch blade.
		unknown	The status of the LAN switch blade could not be obtained.
	 (*1)	error	An error was detected from the LAN switch blade.
		fatal	A fatal error was detected from the LAN switch blade, which is now unusable.
	 (*1)	stop	The LAN switch blade was detected to have been powered off.

*1: When operating in IBP mode

Table 12.4 VM Host Icons






Icon	Status	Meaning
	normal	No new errors or warnings were detected from the VM host.
	warning	A warning was detected from the VM host.
	unknown	The status of the VM host could not be obtained.
	error	An error was detected from the VM host.
	fatal	A fatal error was detected from the VM host, which is now unusable.
	stop	The VM host was detected to have been powered off.

Table 12.5 VM Guest Icons

Icon	Status	Meaning
	normal	No new errors or warnings were detected from the VM guest.




Icon	Status	Meaning
	warning	A warning was detected from the VM guest.
	unknown	The status of the VM guest could not be obtained.
	error	An error was detected from the VM guest.
	fatal	A fatal error was detected from the VM guest, which is now unusable.
	stop	The VM guest was detected to have been powered off.

Table 12.6 Virtual Switch Icons






Icon	Status	Meaning
	normal	No new errors or warnings were detected from the virtual switch.
	warning	A warning was detected from the virtual switch.
	unknown	The status of the virtual switch could not be obtained.
	error	An error was detected from the virtual switch.
	fatal	A fatal error was detected from the virtual switch, which is now unusable.
	stop	The virtual switch was detected to have been powered off.

Table 12.7 LAN Switch Icons

Icon	Status	Meaning
	normal	No new errors or warnings were detected from the LAN switch.










Icon	Status	Meaning
	warning	A warning was detected from the LAN switch.
	unknown	The status of the LAN switch could not be obtained.
	error	An error was detected from the LAN switch.
	fatal	A fatal error was detected from the LAN switch, which is now unusable.
	stop	The LAN switch was detected to have been powered off.

Table 12.8 Port Icons

Icon	Status	Meaning
 	normal	No errors were detected from the port.
 	error	An error was detected from the port (e.g. its opposite port or NIC was disabled, or the cable between this link and its opposite port or NIC was disconnected).
 	disabled	The port was detected to have been disabled (offline).



*1: This icon is displayed for the following ports.








- The currently selected port.
- The port opposite to the selected port.
- In IBP mode, all ports that belong to the selected port group.
- In IBP mode, all ports that belong to the same port group as the selected port.

12.4.2 VLAN Display

The following resource icons are used when displaying VLANs in the Network Map.

Table 12.9 Resource Icons for VLAN Display

Icon	Meaning
	Chassis
	Server

Icon		Meaning
	 (*1)	LAN switch blade
		VM host
		VM guest
		Virtual switch
		LAN switch
		Port

*1: When operating in IBP mode

Information

If a problem occurs on a resource, a status icon indicating the problem is shown on top of the resource's own icon.

For details on status icons, refer to "[12.4.1 Resource Statuses](#)".

12.4.3 Other Icons

The following tables detail the icons displayed in the Network Map.

Table 12.10 Admin Server Icon








Icon	Status	Meaning
	Admin server	Indicates the server used as the admin server.

Table 12.11 Map Navigation Icons

Icon	Meaning
	Chassis

Icon	Meaning
	Server
	VM host
	VM guest
	Switch
	VM switch





12.5 Network Links

This section details the network links displayed in the Network Map.

12.5.1 Link Display

The following table details the physical and virtual links displayed between resources.

Table 12.12 Links



Link	Meaning
	Represents a physical or virtual link.
	Represents a VLAN link.
	Represents a VLAN link related to the selected resource.
	Represents a disabled port.

12.5.2 Link Statuses

Link statuses are shown by adding colored outlines to displayed links (as described in "[12.5.1 Link Display](#)").

The following table shows display examples of abnormal link statuses.

Table 12.13 Statuses of Physical or Virtual Links

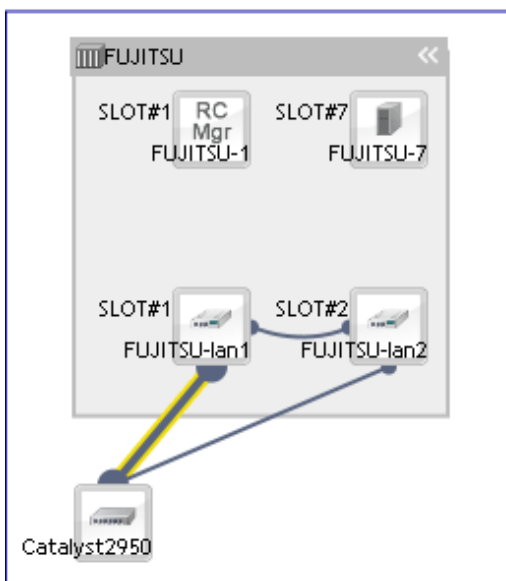
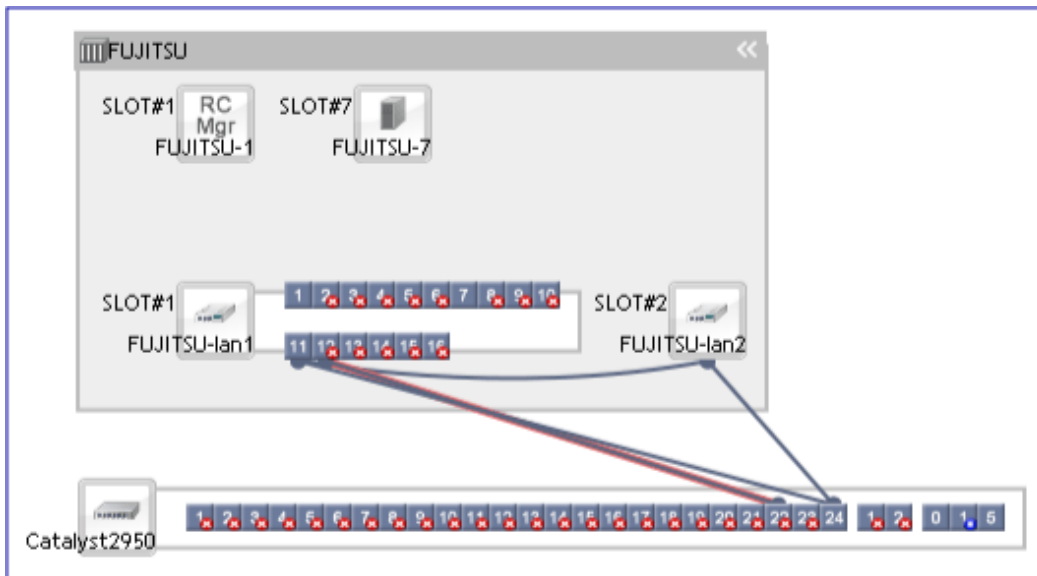
Link	Meaning
	Represents a link with an error status (e.g. its opposite port or NIC is disabled, or the cable between this link and its opposite port or NIC is disconnected).
	Represents a link with a warning status. For example, an aggregated link (as described in " 12.5.3 Aggregate Display of Network Links ") will show a warning status if only a subset of its links have an error status.

12.5.3 Aggregate Display of Network Links

When two resources are linked by two or more links, those links are represented as one aggregated link (please note that this appellation is not related with the Link Aggregation Protocol, but only refers to the display representation of multiple links as one entity).

Aggregated links are shown as thick lines in the Network Map. The following diagram shows an example of aggregate display.

Example



Note

Selecting a displayed resource will focus display on that resource. In such a focus mode, all links that are not directly related to the selected resource will be shown in lighter colors.

12.6 Display Filters

This section explains how to use display filters.

Resource descriptions

The display filter area includes the following filters (checkboxes). Selecting or clearing a filter's checkbox will either show or hide the content associated with that filter.

Physical links

The display filter area includes the following filters (checkboxes). Disabling this filter will hide all physical links between resources on the network map.

VLANs

Only displayed when the VLAN tree is displayed. The display filter area includes the following filters (checkboxes). Disabling this filter will hide the VLAN selected in the VLAN tree on the network map.

Chapter 13 Collecting Power Consumption Data and Displaying Graphs

This chapter explains how to export the power consumption data collected from registered power monitoring targets and how to display it as graphs, and also describes the exported data's format.

13.1 Overview

This section details the power consumption data that is collected from registered power monitoring targets.

Resource Orchestrator calculates the power (in Watts) and energy (Watt-hours) consumed by a power monitoring target by multiplying its collected electrical current (Amperes) by its registered voltage value (Volts).

This data can then be exported to a file in CSV format or as a graph.

The data can then be summarized or visualized as a graph, using an external tool such as Excel, to obtain a graphical representation of the power consumed by each power monitoring target.

Information

In Resource Orchestrator, power consumption is calculated as the product of electrical current (A) multiplied by voltage (V). Normally, power consumption is the product of an electrical current multiplied by a voltage and an additional phase factor (if the phase difference between the current and voltage is defined as " θ ", this factor is expressed as " $\cos \theta$ ").

Note

This data should only be used as a reference to evaluate the power consumption status. It should not be used as an exact power consumption measurement for billing purposes.

13.2 Exporting Power Consumption Data

This section explains how to export power consumption data.

The power consumption data for each power monitoring target that is registered in the power monitoring environment can be exported in CSV format.

The exported data can be selected by specifying the desired data types (power and energy), time spans, and sampling rate.

Use the following procedure to export power consumption data.

1. In the ROR console server resource tree, right-click a power monitoring target, and select [Export]-[Environmental Data] from the popup menu.

The [Export Environmental Data (*power_monitoring_target*)] dialog is displayed.

2. Set the following items:

Figure 13.1 [Export Environmental Data (power_monitoring_target)] Dialog

Choose the type and period of environmental data that will be exported.

Target Resources

Select	Device Name	Comments
<input checked="" type="checkbox"/>	ups	

Data Type

Select	Data Type	Unit	Description
<input checked="" type="checkbox"/>	Power	W	Instantaneous power consumption
<input type="checkbox"/>	Average power	W	Average power consumption during the selected time span
<input type="checkbox"/>	Energy	Wh	Total energy consumption during the selected time span

Output time span: Last hour

Rate: Finest sampling

Format: CSV

OK Cancel Help

Target Resources

Specify the power monitoring target to export the power consumption data of.
Select the checkboxes of each desired target. More than one target can be selected.

Data Type

Specify the type of data to export.
Check the checkbox of each desired data type. More than one data type can be selected.

Output time span

Select the time span for which to export data from the drop-down menu.
Select one of the following options:

- Last hour
- Last day
- Last week
- Last month
- Last year
- Custom

When "Custom" is selected, the following fields must all be specified:

- Start day
- Start time
- End day
- End time

Rate

Select the data sampling rate to export from the drop-down menu.

Select one of the following options:

- Finest sampling
- Hourly
- Daily
- Monthly
- Annual

3. Click <OK>.

In the download dialog that is displayed, specify the name of the export file. The data will be exported to the specified file.



Exporting large amounts of data will take time.

The operation will fail when it takes over five minutes.

If the operation fails, as processing on the server may not have finished, wait for a while before performing the operation again. In that case, change the settings of "Target Resources" and "Output time span" to reduce the amount of data output.

The recommended export settings for environmental data are as listed below.

Table 13.1 Recommended export settings

Rate	Output time span	Output device count
Finest sampling	Last day	12
Hourly	Last month	30
Daily	Last year	30
Monthly	Select "Custom" and specify 5 years	60
Annual	Select "Custom" and specify 5 years	60

13.3 Power Consumption Data File (CSV Format)

This section explains the power consumption data file format (CSV format).

Each defined item of the exported power consumption data is separated by a comma (",").

Each line is exported in the following format.

- Data format

Data is exported using the following format:

```
Time,power_monitoring_target_name(data_type)[,power_monitoring_target_name(data_type)]...  
time1,data1[,data1]...  
time2,data2[,data2]...
```


- Header line

The header line contains column titles identifying the data (from line 2 and later) that is displayed under each column. Each column title is set according to the data types that have been selected in the [Export Environmental Data (*power_monitoring_target_type*)] dialog.

- Time

This column displays the date and time at which each data sample was collected.

Within data lines, the entry corresponding to this column is displayed in the following format: "YYYY-MM-DD hh:mm:ss" ("YYYY": Year, "MM": Month, "DD": Date, "hh:mm:ss": Hours:Minutes:Seconds). The time is displayed according to the time zone set in the admin server operating system.

- *power_monitoring_target_name*(*data_type*)

The *power_monitoring_target_name* part displays the name of the selected target.

The *data_type* part displays the following data types:

- Power (W) is shown as "power"
 - Average Power (W) as "power-average"
 - Energy (Wh) as "energy"

- Data lines

Each data line contains data values corresponding to each of the column titles shown in the header line.

A hyphen ("-") is displayed for any data that could not be collected.



Note

- Regardless of the specified power monitoring target, the data held within Resource Orchestrator that fits the conditions given for the selected time span and rate will be exported.
- Depending on the statuses of specified power monitoring targets, the data corresponding to the specified time span and rate may not have been collected.
In this case, a hyphen ("-") will be displayed for any data that could not be collected.
Hyphens can be displayed when data was collected from another power monitoring target (including a deleted one) at the same collection time, and data was not collected from the specified power monitoring target.
No data is collected from servers on which ServerView Agents is not running. In this case, missing data is shown using hyphens ("-").
- When power consumption data is exported, if the latest data is being collected at that point, some data may be shown using hyphens ("-").
- If the "Finest sampling" "rate" is selected in the [Export Environmental Data (*power_monitoring_target*)] dialog, the power and average power values will be equal for each data sample.
- If a "rate" other than "Finest sampling" has been selected in the [Export Environmental Data (*power_monitoring_target*)] dialog, values for each sample are displayed as follows. If data was collected at the displayed sample time, that value is displayed. If no data was collected at the displayed sample time, the last data collected in the time interval between that sample and the previous sample will be displayed.
- The energy (Wh) value of a finest sample is calculated under the assumption that the power value (W) collected for the sample stayed at the same value until the next sampling (in other words it is assumed that power values (W) do not vary during the duration of the polling interval).
- Only daily average data can be collected from blade chassis.
- Data collected from servers does not include power consumed by storage blades.
- For rates other than "Finest sampling", the energy value is calculated as the sum of energy samples. In such cases, the energy value of samples for which no data could be collected will be deemed to be 0.
- The average power (W) of each sample is calculated from the energy value (Wh) of that sample and its corresponding time interval.

13.4 Displaying Power Consumption Data Graphs

This section explains how to display power consumption data as graphs.

The power consumption data for each power monitoring target that is registered in the power monitoring environment can be displayed as graphs.

The collected power consumption data and average values of the specified time span and rate can be displayed in line graphs.

Use the following procedure to display power consumption data as graphs.

1. Select [Tools]-[Environmental Data Graph] from the ROR console menu.

The [Environmental Data Graph] dialog is displayed.




2. Set the following items:

Figure 13.2 [Environmental Data Graph] dialog

Environmental Data Graph

Choose the desired resources and output time.
Up to 18 resources can be selected.

Target Resources

 Chassis
  Server
  Power Monitoring Device

Select	Resource Name	Resource Type
<input type="checkbox"/>	bx900	Chassis
<input type="checkbox"/>	bx900-2	Server
<input type="checkbox"/>	bx900-3	Server
<input type="checkbox"/>	bx900-4	Server
<input type="checkbox"/>	bx900-6	Server
<input type="checkbox"/>	bx900-7	Server
<input type="checkbox"/>	bx900-8	Server
<input type="checkbox"/>	bx900-9	Server
<input type="checkbox"/>	bx900-10	Server

Graph Settings

Data Type: Power (Instantaneous power consumption)
 Average power (Average power consumption during the selected time span)

Output Time Span: Last hour ▼

Rate: Finest sampling ▼

Target Resources

Specify the power monitoring target name to display the power consumption data graph of.

Select the checkboxes of each desired target.

Up to 18 targets can be selected.

Graph Settings

Data Type

Specify the type of data to display the graph.

Specify either one of the following for the data type:

- Power (Instantaneous power consumption)
- Average power (Average power consumption during the selected time span)

Output Time Span

Select the time span for the data from the drop-down menu.

Select one of the following options:

- Last hour
- Last day
- Last week
- Last month
- Last year
- Custom

When "Custom" is selected, the following fields must all be specified:

- Start day
- Start time
- End day
- End time

Rate

Select the graph output interval to export from the drop-down menu.

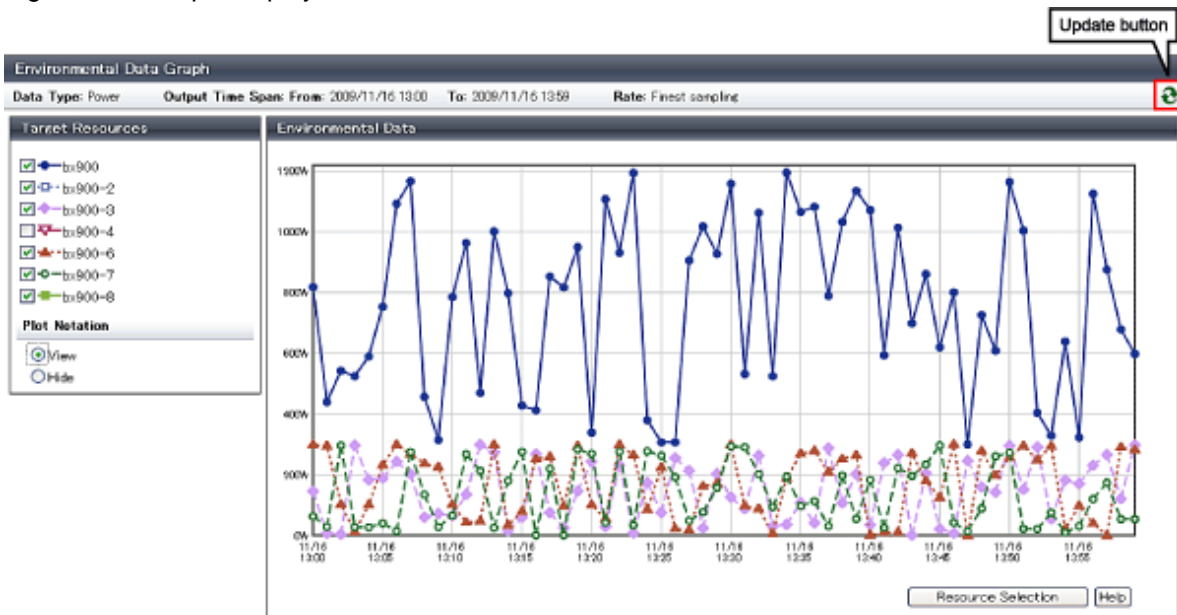
Select one of the following options:

- Finest sampling
- Hourly
- Daily
- Monthly
- Annual

3. Click <Graph Output>.

After switching to the graph display window, the selected power consumption data can be displayed in line graphs.

Figure 13.3 Graph Display Window



The following operations can be performed from the graph display window.

- Switching resource display

By selecting and clearing the checkbox of the "Target Resources", it is possible to display or hide the corresponding graph.

- Switching plot symbol display

Selecting the "View" or "Hide" radio button of "Plot Notation" switches between displaying and hiding plot symbols in line graphs.

- Data update

Clicking the update button on the upper right of the screen updates the displayed graph.

- Return to resource selection window.

Clicking <Resource Selection> displays the [Environmental Data Graph] dialog.

Note

If you change the size of the web browser when displaying graphs, click the update button after doing so.

Chapter 14 Customizing the ROR Console

This chapter explains how to customize the ROR console.

14.1 Dialogs

This section explains how to enable or disable display of some of the confirmation (or warning) dialogs used by the ROR console.

Use the following procedure to change dialog display settings:

1. Select [Tools]-[Options] from the ROR console menu.

The [Options] dialog is displayed.

2. Click the "Dialog" category title, and change the following settings in the displayed area.

Dialog display options (checkboxes)

To disable further display of a confirmation or warning dialog, select its corresponding checkbox.

To restore display of a disabled dialog, deselect its corresponding checkbox.

<Select All> button

Selects all dialog checkboxes.

<Deselect All> button

Deselects all dialog checkboxes.

3. Click <Apply>.

The new settings are applied.

14.2 External Software

This section explains how to configure the settings required by Resource Orchestrator to interact with third party software.

VM management console

To launch an external VM management console (provided by the virtualization software used) from the ROR console, users must be granted the permission to launch this management console in the Java Plug-in policy settings. For details on the VM management consoles that can be started from the ROR console, refer to "E.2 Configuration Requirements" of the "Setup Guide VE".

Use the following procedure to enable launch of the VM management console.

1. In the ROR console server resource tree, right-click the target VM host or VM guest, and select [VM Management Console] from the menu that is displayed.

The [Launch VM Management Console] dialog is displayed.

2. Click <OK>.

If launch of the VM management console from the ROR console has not been enabled yet, a [Download] dialog for the Java policy setup script is displayed.

3. Click <OK>.

This will download the Java policy setup script. Save the script to an arbitrary location.

4. Execute the saved Java policy setup script. This will configure Java policy settings and allow launch of the VM management console.

5. Close all Web browsers.

After closing all open Web browsers, start a new Web browser and re-log into the ROR console. The VM management console can now be launched from the ROR console.



Information

Depending on script-related settings, the command prompt opened by the Java policy setup script may close right after finishing its execution, making it impossible to confirm whether the script ended successfully.

In this case, select [start]-[Run] from the Windows start menu, and execute the following command.

```
wscript "Full_path_name_of_the_Java_policy_setup_script"
```

Chapter 15 Troubleshooting

This chapter explains how to address problems that occur, and how to collect data in order to request investigation of problems.

15.1 Types of Troubleshooting Data

If a problem occurs on a system using Resource Orchestrator, use the following procedures to collect troubleshooting data so that Fujitsu technical staff can investigate the problem.

Two kinds of troubleshooting data can be collected. Collect the data which is relevant to one of the situations described below:

1. Collect initial troubleshooting data

To identify the cause of a problem, collect the data required to perform an initial diagnostic of the problem and contact Fujitsu technical staff.

The amount of data collected is small enough to be sent by e-mail.

Refer to "[15.1.1 Collecting Initial Troubleshooting Data](#)" for more information.

2. Collect exhaustive troubleshooting data

In some cases, the cause of a problem can be identified from the initial troubleshooting data alone, but in other cases, additional information is required.

In such cases, a large volume of data is required to perform a more exhaustive investigation and identify the cause of a problem.

As a result, exhaustive troubleshooting data is significantly larger than initial troubleshooting data.

Collect and send exhaustive troubleshooting data if requested to do so by Fujitsu technical staff.

Refer to "[15.1.2 Collecting Exhaustive Troubleshooting Data](#)" for more information.



Note

Once a problem occurs, troubleshooting data should be collected promptly. Otherwise, data necessary for a problem investigation may be overwritten.

15.1.1 Collecting Initial Troubleshooting Data

This section explains how to collect the data required to diagnose the causes of problems.

About Collection Methods

The initial troubleshooting data can be collected using the following methods.

Based on each collection method's characteristics, choose the appropriate one according to the environment and system state in which the problem occurred.

- **Collecting data from the admin server**

This method involves executing a troubleshooting data collection command (`rcxadm mgrctl snap -all`) on the admin server.

This method allows collection of data from all managed servers at once via the network. This is easier than executing a command individually on each managed server.

For how to collect the data, refer to "[Collecting Data from the Admin Server \(rcxadm mgrctl snap -all\)](#)".

Executing the `rcxadm mgrctl snap -all` command requires approximately the free space determined by the following formula:
Number_of_registered_servers * 30 MB + 65 MB

- **Collecting data separately from each server**

This method involves executing a data collection command (`rcxadm mgrctl snap` or `rcxadm agtctl snap`) on each server.

For how to collect the data, refer to "[Collecting Data Separately from each Server \(rcxadm mgrctl snap, rcxadm agtctl snap\)](#)".

Around 65 MB of free space is required to execute the `rcxadm mgrctl snap` command, and around 30 MB of free space is required to execute the `rcxadm agtctl snap` command.

- Collecting HBA address rename Setup Service Environment Data

This method involves collecting data that is required for identifying the cause of a problem that occurs on the HBA address rename setup service.

For how to collect the data, refer to "[Collecting HBA address rename Setup Service Environment Data](#)".

About 8 MB of free space is required to collect troubleshooting data for the HBA address rename server.



Note

[VMware]

- For VMware ESX4, please also collect and send the following data to Fujitsu technical staff.
 - Use the copy command to collect and send the following files.
 - /var/log/vmware/hostd.log
 - /var/log/vmware/hostd-*.log
 - /var/log/vmware/hostd-*.log.gz
 - Collect and send the result (output) of the following command.
 - /usr/sbin/esxcfg-firewall -q
- For VMware ESXi, perform the following procedures on the server from which data is to be collected:
 - When VMware ESXi is not registered with VM management software
 1. Connect with VMware ESXi on the target VMware client.
 2. Select [Export]-[Export System Logs] from the [File] menu.
The [Export System Logs] dialog is displayed.
 3. Specify the system log download destination.
 4. Click <OK>.
 - When VMware ESXi is registered with VM management software
 1. Connect with VM management software on the VMware client.
 2. Select [Export]-[Export System Logs] from the [File] menu.
The [Export System Logs] dialog is displayed.
 3. Select the target VMware ESXi.
 4. Specify the system log download destination.
 5. Click <OK>.

Send the data output to the download destination to Fujitsu technical staff.

Collecting Data from the Admin Server (rcxadm mgrctl snap -all)

Troubleshooting data from every managed server can be collected all at once by executing the command for collecting troubleshooting data, rcxadm mgrctl snap -all, on an admin server.

The following method is used to collect data with the data collection command, rcxadm mgrctl snap -all.

Collection Method

Perform the following procedure on the admin server to collect investigation data:

1. Log on to the admin server with OS administrative privileges.
 - OS administrative privileges are required to collect troubleshooting data.

2. Execute the `rcxadm mgrctl snap -all` command.

[Windows]

```
>"Installation_folder\Manager\bin\rcxadm" mgrctl snap [-dir directory] -all <RETURN>
```

[Linux]

```
# /opt/FJSVrcvnr/bin/rcxadm mgrctl snap [-dir directory] -all <RETURN>
```

3. Send the collected troubleshooting data to Fujitsu technical staff.

Note

- The manager must be running on the admin server in order to collect data from the admin server. If the manager cannot be run, collect data from each server.
- When collecting data via the admin server, data cannot be collected from a managed server in the following cases.
 - Communication cannot be established with the server
 - The managed server is stopped

In either case, however, data will continue to be collected from other managed servers.

Use the command execution logs to check the execution results.

Refer to "5.7 rcxadm mgrctl" of the "Command Reference" for details.

For managed servers where data collection has failed, collect data by either executing the `rcxadm mgrctl snap -all` command on the admin server again, or by executing the `rcxadm agtctl snap` command on the managed server where data collection failed.

[VMware]

- When a managed server is VMware ESXi, data cannot be collected from that managed server.
Use the procedure described in "[About Collection Methods](#)" for collecting data.

Collecting Data Separately from each Server (`rcxadm mgrctl snap`, `rcxadm agtctl snap`)

In addition to the `rcxadm mgrctl snap -all` command, which can collect troubleshooting data from all the managed servers at once, the commands `rcxadm mgrctl snap` and `rcxadm agtctl snap` are also provided. These collect data from only the server on which they are executed.

Use the following procedure to collect data with the `rcxadm mgrctl snap` command or the `rcxadm agtctl snap` command.

Collection Method

Perform the following procedure on the server from which data is to be collected:

1. Log on to the server with OS administrator privileges.
OS administrative privileges are required to collect troubleshooting data.
2. Execute the `rcxadm mgrctl snap` command or the `rcxadm agtctl snap` command.

Note that the command differs depending on the server from which data is collected.

- Admin servers

[Windows]

```
>"Installation_folder\Manager\bin\rcxadm" mgrctl snap [-dir directory] <RETURN>
```

[Linux]

```
# /opt/FJSVrcvnr/bin/rcxadm mgrctl snap [-dir directory] <RETURN>
```

- Managed servers

[Windows]

```
>"Installation_folder\Agent\bin\rcxadm" agtctl snap [-dir directory] <RETURN>
```

[Linux/VMware]

```
# /opt/FJSVrcxat/bin/rcxadm agtctl snap [-dir directory] <RETURN>
```

[Solaris]

```
# /opt/FJSVrcvat/bin/rcxadm agtctl snap [-dir directory] <RETURN>
```

3. Send the collected troubleshooting data to Fujitsu technical staff.

For details, refer to "5.1 rcxadm agtctl" or "5.7 rcxadm mgrctl" of the "Command Reference".



Note

[VMware]

When the managed server is VMware ESXi, collect data using the procedure described in "[About Collection Methods](#)".

Collecting HBA address rename Setup Service Environment Data

The following method is used to collect the troubleshooting data necessary to investigate problems that occur on an HBA address rename setup service.

Collection Method

Perform the following procedure on the HBA address rename server to collect troubleshooting data.

1. Collect files from the HBA address rename server.

[Windows]

From the HBA address rename server, collect the log file *installation_folder\WWN Recovery\rcxinstaller.log*, and all files and folders under the following folder: *installation_folder\WWN Recovery\var*.

[Linux]

Collect the log file */var/tmp/rcxhbainstaller.log*, and all files and folders under the following folder: */var/opt/FJSVrcvnb*.

2. Obtain OS system logs.

[Windows]

Collect event logs (application and system logs).

[Linux]

Collect all */var/log/messages* and */var/log/messages.X* files. (The *messages.X* part represents the file name such as *messages.1* or *messages.2*)

3. Take a screenshot of the window displayed when the problem occurred.

Perform the following operation on the server for HBA address rename setup service from which the data is to be collected in order to take a screenshot of the window:

Press the Print Screen key to copy image data onto the Clipboard, and then paste the image data into an image editing tool and save it as a bitmap file.

4. Obtain system version information.

[Windows]

From Windows explorer, right-click the "My Computer" icon, and select [Properties] from the popup menu.

In the [System Properties] dialog click the [General] tab and use the procedure explained in step 3 to obtain information such as the OS type, version and level, and service pack number.

[Linux]

Execute and collect the results of the following commands.

cat /etc/redhat-release <RETURN>
cat /proc/version <RETURN>
cat /proc/meminfo <RETURN>
cat /proc/cpuinfo <RETURN>
rpm -qa <RETURN>

5. Send the collected troubleshooting data to Fujitsu technical staff.

15.1.2 Collecting Exhaustive Troubleshooting Data

This section explains how to collect exhaustive troubleshooting data.

When the cause of a problem cannot be determined from the initial troubleshooting data, exhaustive troubleshooting data becomes necessary.

About Collection Methods

The troubleshooting data used to identify the causes of problems is collected by executing troubleshooting data collection commands (rcxadm mgrctl snap -full or rcxadm agtctl snap -full) on each server.

About 80 MB of free space is required to use this function.

Collection Method

Perform the following procedures on the server from which data is to be collected:

1. Log on to the server with OS administrator privileges.
OS administrative privileges are required for collecting investigation data.
2. Execute the rcxadm mgrctl snap -full command or the rcxadm agtctl snap -full command.

Note that the command differs depending on the server from which data is collected.

- Admin servers

[Windows]

```
>"Installation_folder\Manager\bin\rcxadm" mgrctl snap -full [-dir directory] <RETURN>
```

[Linux]

```
# /opt/FJSVrcvnr/bin/rcxadm mgrctl snap -full [-dir directory] <RETURN>
```

- Managed servers

[Windows]

```
>"Installation_folder\Agent\bin\rcxadm" agtctl snap -full [-dir directory] <RETURN>
```

[Linux/VMware]

```
# /opt/FJSVrcxat/bin/rcxadm agtctl snap -full [-dir directory] <RETURN>
```

[Solaris]

```
# /opt/FJSVrcvat/bin/rcxadm agtctl snap -full [-dir directory] <RETURN>
```

3. Send the collected troubleshooting data to Fujitsu technical staff.

For details, refer to "5.1 rcxadm agtctl" or "5.7 rcxadm mgrctl" of the "Command Reference".



[Hyper-V]

The following files should also be collected manually.

Collect them using Explorer and then send them to Fujitsu technical staff.

OS system log

All files under the following folder: `windows_folder\system32\wbem\logs`

[VMware]

For VMware ESX 4 or VMware ESXi, collect data referring to "About Collection Methods" in "15.1.1 Collecting Initial Troubleshooting Data".

15.2 OS Startup Issues (with I/O Virtualization)

This section explains how to troubleshoot startup issues on managed servers.

- When using HBA address rename

When using HBA address rename, the WWN that was set for the server's HBA is set from the manager when the power to the server is turned on again.

When errors occur within the admin server, the HBA address rename setup service sets the WWN for the server's HBA.

Use the following procedure to confirm and correct the problem.

1. If the server was replaced immediately beforehand, confirm that hardware information was successfully re-configured following server replacement.
For details, refer to "9.3 Re-configuring Hardware Properties".
2. Check the storage environment.
Check that the WWN set for the server's HBA have access to the appropriate storage device and logical volume. Set a proper access path if none was configured yet.
For details, refer to "4.3.2 Configuring the Storage Environment" of the "Setup Guide VE".
3. Check the manager's startup status.
For details on how to check the startup status of the manager, refer to "7.2 Starting and Stopping the Manager" of the "Setup Guide VE".
4. Perform either one of the following based on the manager's startup status.
 - If the manager is not running
Start the manager.
If the manager cannot start because of a server fault, for example, recover the server after completing step 5.
 - If the manager is already running
Occasionally the timing of the manager startup can prevent it from controlling a managed server. If this is the case, restart the managed server.
Even if the manager is running, if communication problems happen on the admin LAN (due to issues with network interfaces, cabling, or LAN switches), the managed server will not start. After performing step 5, the LAN configuration must be repaired.

5. Check the running state of the HBA address rename setup service.

Check the running state of this service in the server for HBA address rename setup service.

Start the server where this service has been set up if it is not running yet, then start the managed server.

The WWN for the managed server's HBA will then be set using the most recent state synchronized with the admin server.

6. Check the managed server console.

Check the managed server console to confirm that it has successfully started up.

If an error message is output, take action according to the corresponding message ID in the "Messages VE".

7. For managed servers other than PRIMERGY BX servers, check that the MAC address entered at registration is correct. If it is incorrect, re-configure the server's hardware properties.

The registered MAC address can be confirmed in the [Resource Details] tab for the corresponding physical server.

Refer to "1.5.2 [Resource Details] Tab" of the "User's Guide VE" for details.

8. Check the following network environment.

- Whether communication between the admin server and the managed server is possible
- Whether there are any DHCP or PXE servers running on the subnet used by managed servers
- When the admin server and the managed server belong to different subnets, whether the DHCP relay agent of the router is correctly configured

- When using VIOM

1. Check settings for the WWN of server HBA, the MAC addresses of NIC, booting, and networking which are managed by VIOM.

Check if the admin LAN server profile is correct or not by opening the VIOM client.

2. Check the storage environment.

Check if the settings for WWN of the server's HBA, the MAC addresses of NIC, and booting can access correct storage units and volume. If the setting was not completed, set the proper access path.

For details, refer to "4.3.2 Configuring the Storage Environment" of the "Setup Guide VE".

15.3 "unknown" Server Status

This section explains how to troubleshoot a registered managed server whose status is "unknown" even though the managed server is still running.

When errors or warning messages are displayed in the event log, take the appropriate action referring to the "Messages VE". Check the following points and resolve the cause of any problems:

- Communication between the admin server and the server management unit is not possible

Check if it is possible to connect to either the Web or telnet interface of the server management unit (management blade or remote management controller).

- Communication between the admin server and the managed server is not possible

Check that the admin LAN IP address is correctly set on the managed server.

Check LAN switch blade configurations to confirm that the same VLAN ID or the same port group (for switch blades operating in IBP mode) is set for the ports used by the managed server and the admin server on the admin LAN.

When using PRIMERGY BX600 servers and changing the VLAN ID used for the admin LAN, proceed as follows to preserve communication from the admin server to the LAN switch blade. First, change the VLAN ID set for the admin LAN port (on the LAN switch blade) connected to the admin server, as well as the VLAN ID set for the switch blade's own network interface. Then, change the VLAN ID for the admin LAN port connected to the managed server.

For the overview and the setup of the VLAN for the managed server, refer to "4.2.1 Network Configuration" of the "Setup Guide VE" and "3.2.8 Changing the VLAN Settings of LAN Switch Blades" of the "User's Guide VE".

- Communication is not allowed for the ports used by Resource Orchestrator

Allow communication for the ports described in "Appendix A Port List" of the "Setup Guide VE".

- The Resource Orchestrator agent is not running

Make sure that the agent is running on the managed server.

- ServerView Agents is not running

For PRIMERGY servers, check whether ServerView Agents is running properly on the managed server.

[Windows/Hyper-V]

From the Windows Control Panel, open "Administrative Tools" and then open the [Services] window. Check that the status of the Server Control Service and SNMP Service is shown as "Started".

[Linux/VMware/Xen/KVM]

Execute the following commands to check if the ServerView Agents service is running.

```
# /etc/init.d/srvmagt status <RETURN>
# /etc/init.d/eecd status <RETURN>
# /etc/init.d/snmpd status <RETURN>
```

The above commands are not available if ServerView Agents is not installed. If they are not available, install ServerView Agent on the managed server.

If ServerView Agents is not running, refer to the ServerView Agent manual for how to start the ServerView Agents.

- SNMP community settings are incorrect

Make sure that the SNMP community settings on the management blade, management board, and managed server match those set in Resource Orchestrator during chassis and server registration.

- Hardware properties were not re-configured after replacing the server

Identify the MAC address of the replacement server, and check if it is the same address as that set for the admin LAN (MAC address) in the [Resource Details] tab of the ROR console.

If the MAC address is different, re-configure the hardware properties from the ROR console.

- No information could be obtained from the server virtualization software running on the managed server

In environments where no VM management software was registered, or for VM hosts that are not managed by VM management software, the status of a VM guest is displayed as "unknown" if its information could not be obtained from the server virtualization software used to run that VM guest. Check whether the server virtualization software is operating correctly.

If it is operating correctly, its account information (user account name and password) may have changed. As a result, the settings no longer correspond to those registered in Resource Orchestrator. In that case, change the virtualization software's account settings registered in Resource Orchestrator.

Refer to "3.2.7 Changing VM Host Login Account Information" of the "User's Guide VE" for details.

- No information could be obtained from VM management software

In environments where VM management software was registered, the status of a VM guest (on a VM host managed by this VM management software) is displayed as "unknown" if its information could not be obtained from the VM management software. Check whether the VM management software is operating correctly.

If it is operating correctly, its account information (user account name and password) may have changed. As a result, the settings no longer correspond to those registered in Resource Orchestrator. In that case, change the VM management software's account settings registered in Resource Orchestrator.

For details, refer to "3.6 Changing VM Management Software Settings" of the "User's Guide VE".

- The remote management controller's IP address, user name, or password was changed after server registration

Change the IP address, user name and password settings registered for this remote management controller in Resource Orchestrator. Refer to "3.2.5 Changing Server Management Unit Configuration Settings" of the "User's Guide VE" for details.

- The remote server management IP address, user name, or password was changed after server registration

Change the IP address for remote server management, user name, and password settings registered in Resource Orchestrator. Refer to "3.2 Changing Chassis and Managed Servers Settings" of the "User's Guide VE" for details.

- High load on the admin server, server management unit, or managed server

Resource statuses may be temporarily shown as "unknown".

- Power control of partitions has been performed on PRIMEQUEST
Resource statuses may be temporarily shown as "unknown".
- The chassis has been powered off on PRIMEQUEST
The statuses of the target chassis and servers are all shown as "unknown".
- The routing settings of the router are not correctly configured
When using an admin server to manage managed servers belonging to other subnets, configure the router settings.
For details, refer to "4.2.6 Configuring the Network Environment" of the "Setup Guide VE".

15.4 Image Operation Issues [Windows/Linux] [Hyper-V]

If the admin server IP address that was set up in the [Admin Server Registration] window described in "2.2.2 Installation [Windows/Hyper-V]", or "2.2.3 Installation [Linux/VMware/Xen/KVM/Oracle VM]" of the "Installation Guide VE" is incorrect, the following message is displayed when collecting or deploying cloning images, or when backing up or restoring system images.

FJSVrcx:ERROR:68295:deployment engine error:
no response from the managed server node. invalid BIOS setting found *detail*

detail

The information describing error details is displayed.

Use the following procedure to confirm and correct the problem.

[Windows/Hyper-V]

1. On the managed server, select [start]-[Run], and then execute the following command.

Installation_folder\Agent\scw\config.bat

The IP address of the admin server that has been set up and the port settings are displayed.



Note

Note that the "Deployment Server" referred to in this section actually refers to the admin server.

2. In the Deployment Server field, check that either the admin server IP address or the server name is correctly set up.

If the settings are incorrect, change the value displayed and click <OK>.



Note

When entering the server name, check that the IP address on the managed server side of the admin server can be resolved from the server name.

In the confirmation dialog asking to restart the client agent, click the <Yes> button.

3. Click <Yes>.

[Linux]

1. Open the /etc/scwagent.conf file on the managed server.

Confirm the admin server IP address and the settings of the port currently being used.

2. In the server_ip field, check that either the admin server IP address or the server name is correctly set up.

If the settings are incorrect, edit scwagent.conf directly, and then restart the managed server.

After resolving the cause of the error, execute the operation again as described in step 4. of "Message number 68295" of the "Messages VE".

If the settings are found to be satisfactory, take the corrective action described in "Message number 68295" of the "Messages VE".

15.5 Public LAN Communication Issues

This section explains how to troubleshoot communication issues for managed servers on the public LAN.

Use the following procedure to confirm and resolve any problems.

- The VLAN is not correctly set up
LAN switch blade internal ports must be set to the same VLAN ID(s) as external public LAN ports.
- Port groups are not correctly set up
For LAN switch blades operating in IBP mode, internal ports and external ports should belong to the same port group.
- The public LAN IP address is not correctly set up
Check that the public LAN IP address is correctly set on the managed server.
 - The subnet mask must be correct
 - There should be no IP address conflicts
- Routing information is not correctly set up
Verify that the routing settings for the server allow for communication to an address on a different subnet.

15.6 Multipath Configuration Issues

This section explains how to troubleshoot startup issues on managed servers set with a multi-path configuration.

When using HBA address rename, the managed server will start in a single path configuration if the selected number of HBA ports was set to "1" in the "HBA Address Rename Settings" dialog. For a multi-path configuration, the number of HBA ports for HBA address rename should be set correctly.

For details on how to re-configure this setting, refer to "8.2 HBA address rename Settings" of the "Setup Guide VE".

15.7 Cloning Issues Following Manager Re-installation

This section explains how to troubleshoot cloning issues that occur after re-installing the manager.

When performing a cloning image operation (collection or deployment) on a managed server that was already registered on the manager before re-installation, the following problem may occur. The manager and agent certificates may not match, resulting in the admin server being unable to communicate with its managed server. In such a case, trying to deploy or collect an image to or from the managed server will fail. This problem occurs when the following conditions are met.

- The manager was re-installed, but its certificate store was not properly backed up, as described in "3.1.2 Uninstallation [Windows]" or "3.1.3 Uninstallation [Linux]" of the "Installation Guide VE"
- Both the manager and agent were re-installed (and their certificates renewed), but a cloning image that was collected before the re-installation has been deployed, thus restoring an outdated agent certificate on the managed server

Use the following procedure to correct the problem.

To avoid the same certificate problem, recollect the cloning images which include the cause of the problem after the problem has been corrected.

Checking the Certificates

How to check certificates

1. Stop the manager and then display SSL certificate data by executing the following commands on the admin server.
[Windows]


```
>"Installation_folder\Manager\bin\rxadm" mgretl stop <RETURN>
>"Installation_folder\Manager\bin\rxadm" certctl list <RETURN>
```

[Linux]

```
# /opt/FJSVrcvmr/bin/rxadm mgretl stop <RETURN>
# /opt/FJSVrcvmr/bin/rxadm certctl list <RETURN>
```

For information on these commands, refer to "5.2 rxadm certctl" and "5.7 rxadm mgretl" of the "Command Reference".

Example Results

```
Truststore:
-----

Keystore type: jks
Keystore provider: SUN

The key store includes four entries.

client2,May,10,2007, trustedCertEntry,
Certificate fingerprint (MD5): 0F:4E:1C:DB:19:AE:3B:82:9D:74:93:6C:46:D8:7C:D2
client1,May,10,2007, trustedCertEntry,
Certificate fingerprint (MD5): 9D:99:ED:88:C0:8F:32:26:60:FA:4C:96:A2:34:5A:45
server4,May,11,2007, trustedCertEntry,
Certificate fingerprint (MD5): DC:E3:19:59:08:6D:C4:AD:B4:C7:F6:5C:E1:52:0A:1A (*1)
server3,May,11,2007, trustedCertEntry,
Certificate fingerprint (MD5): 9B:EB:94:58:90:E8:09:BE:BD:FA:14:83:9D:87:3A:E4
...

Keystore:
-----

Keystore type: jks
Keystore provider: SUN

2 entries are included in the keystore.

client, 2007/05/11, keyEntry,
Certificate fingerprint (MD5):
AA:55:85:54:6B:57:80:4F:8C:6E:2E:AA:7C:77:DB:F6 (*2)
server, 2007/05/11, keyEntry,
Certificate fingerprint (MD5):
14:48:31:68:C9:CA:66:E1:E0:34:8A:FC:1C:17:19:EF
```

2. Stop the agent and display SSL certificate data by executing the following commands on the managed server where the error occurred.

[Windows]

```
>"Installation_folder\Agent\bin\rxadm" agtctl stop <RETURN>
>"Installation_folder\Agent\bin\rxadm" certctl list <RETURN>
```

[Linux]

```
# /opt/FJSVrcxat/bin/rxadm agtctl stop <RETURN>
# /opt/FJSVrcxat/bin/rxadm certctl list <RETURN>
```

[Solaris]

```
# /opt/FJSVrcvat/bin/rxadm agtctl stop <RETURN>
# /opt/FJSVrcvat/bin/rxadm certctl list <RETURN>
```

For information on these commands, refer to "5.1 rxadm agtctl" and "5.2 rxadm certctl" of the "Command Reference".

Example Results

```
Truststore:
-----

Keystore type: jks
Keystore provider: SUN

The key store includes one entry.

client1, 2007/05/11, trustedCertEntry,
Certificate fingerprint (MD5):
AA:55:85:54:6B:57:80:4F:8C:6E:2E:AA:7C:77:DB:F6 (*2)
...

Keystore:
-----

Keystore type: jks
Keystore provider: SUN

The key store includes one entry.

server, 2007/05/11, keyEntry,
Certificate fingerprint (MD5): DC:E3:19:59:08:6D:C4:AD:B4:C7:F6:5C:E1:52:0A:1A (*1)
```

3. Check the fingerprint that is contained in the agent Keystore.

As shown in the example in (*1), check that the fingerprint that is contained in the agent Keystore is also contained in the manager Truststore that is shown in "Example Results" of step 1.

If it is not, refer to "Corrective Action" to take proper corrective action.

4. Check the fingerprint that is contained in the agent Truststore.

As shown in the example in (*2), check that the fingerprint that is contained in the agent Truststore is also contained in the manager Keystore that is shown in "Example Results" of step 1.

If it is not, refer to "Corrective Action" to take proper corrective action.

Corrective Action

1. Execute the following commands on the server for which the problem occurred to re-initialize its SSL certificate, and restart its agent.

[Windows]

```
>"Installation_folder\Agent\bin\rxadm" certctl init <RETURN>
>"Installation_folder\Agent\bin\rxadm" agtctl start <RETURN>
```

[Linux]

```
# /opt/FJSVrcxat/bin/rxadm certctl init <RETURN>
# /opt/FJSVrcxat/bin/rxadm agtctl start <RETURN>
```

[Solaris]

```
# /opt/FJSVrcvat/bin/rcxadm certctl init <RETURN>
# /opt/FJSVrcvat/bin/rcxadm agtctl start <RETURN>
```

2. Execute the following command on the admin server to start the manager.

[Windows]

```
>"Installation_folder\Manager\bin\rcxadm" mgrctl start <RETURN>
```

[Linux]

```
# /opt/FJSVrcvnr/bin/rcxadm mgrctl start <RETURN>
```

15.8 Server Switchover and Failback Issues

This section explains the troubleshooting steps to be performed when the server switchover or server failback process fails.

If server switchover or server failback is performed without all the conditions specified in "8.3 Server Switchover Conditions" of the "User's Guide VE" being satisfied, one of the following error messages may be output:

Switchover:

```
FJSVrcx:ERROR:61143:switchover:failed
FJSVrcx:ERROR:69122:timeout occurred while executing power control modules
```

Failback:

```
FJSVrcx:ERROR:61143:failback:failed
FJSVrcx:ERROR:69122:timeout occurred while executing power control modules
```

Use the following procedure to confirm and correct the problem.

1. Recheck the spare server conditions with reference to "8.3 Server Switchover Conditions" of the "User's Guide VE".
If any conditions are not satisfied, change the configuration to ensure that all conditions are met.
2. If HBA address rename is being used and the following error message is output to the managed server console, the WWN may have failed to be set for the server HBA.
Take the action specified for "Message number 61308" of the "Messages VE". Note that in this case there is no need to set the WWN again.

```
FJSVrcx:ERROR:61308:WWN setting failed. code=%1,%2
```

An internal error code is displayed in %1.

Either one of the following message is displayed in %2.

- a. HBA adapter not found
 - b. command error
 - c. TFTP error
3. Perform the switchover or failback operation again.

15.9 HBA Address Rename is Set by Mistake

This section explains the troubleshooting steps to perform when HBA address rename is mistakenly set for a managed server that does not need it (such as when the managed server only uses internal disks).

If HBA address rename is set for a server that does not have an HBA, the following message will be output to the managed server console when the managed server is restarted:

```
FJSVrcx:ERROR:61308:WWN setting failed. code=%1,%2
```

An internal error code is displayed in %1.
Either one of the following message is displayed in %2.

- a. HBA adapter not found
- b. command error
- c. TFTP error

To prevent HBA address rename from being used, delete and then re-register the managed server.

15.10 Boot Issues (Boot Order Related)

This section explains the action to take when a managed server cannot be booted from the CD-ROM, or the system disk (local disk or SAN storage) cannot be recognized even though the managed server can be booted from the CD-ROM.

If this trouble occurs, it may mean that the priority boot order of the system BIOS is incorrect.

Refer to "BIOS Settings for Managed Servers" in "4.1.2 Configuring the Server Environment" of the "Setup Guide VE", and check that the boot order of the system BIOS is correct.

15.11 Boot Issues (Endless Reboot Cycle)

This section explains how to troubleshoot a managed server stuck in an endless reboot cycle, when that managed server is using HBA address rename.

Confirm the following points to identify and resolve the cause of this issue.

- Make sure that BIOS settings were properly configured. For instructions on BIOS settings, refer to "BIOS Settings for Managed Servers" in "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".
- Make sure that the network environment was properly configured. For instructions on the network configuration, refer to "Required Network Configuration when Using HBA address rename" in "4.2.1 Network Configuration" of the "Setup Guide VE".
- Make sure that all manager services are started. For details on manager services, refer to "7.2 Starting and Stopping the Manager" of the "Setup Guide VE".
- Make sure that HBA firmware/BIOS version installed on a managed server are supported.

15.12 When the Display of Resource Information in the [Resource] Tab of the ROR Console Collapses

[Description]

While updating the window of the [Resource] tab of the ROR console, if resource information is hidden or another tab switched to, update will continue to be performed for the hidden area.

At that time, because the web browser cannot handle modification of the size of the window being updated or the coordinate information, after a certain length of time (after regular update of resources), the display of resource information that was updated may collapse.

[Corrective Action]

Perform the following corrective actions:

- When there is update information for resources
Update will be performed automatically during the regular update.
- When there is no update information for resources
Click the page switch button for the resource information.
- When there is no update information for resources, and no page switch button for the resource information
Select a different resource from the tree.

Appendix A Notes on Operating ServerView Resource Orchestrator

This appendix provides important reminders for the operation of Resource Orchestrator.

Server Switchover

- In configurations where a server OS is operating on a spare server, if the boot methods of primary servers and spare servers are different, server switchover may fail and damage the primary server OS. Ensure that the boot methods are the same.
It is recommended that system images of primary servers are regularly backed up in order to prepare for unexpected situations.
- Servers can be set as spare servers even if it may not be possible to switch over with them.
Ensure that server switchover is possible after setting up spare servers.
For details on server switchover conditions, refer to "8.3 Server Switchover Conditions" of the "User's Guide VE".
- Auto-Recovery cannot be performed if maintenance mode has not been released.
Ensure maintenance mode is released once maintenance operations are complete.
- Note the following points regarding the occurrence of a fault in the switchover destination spare server during server switchover.
 - The server switchover state returns to pre-switchover state. Additionally, maintenance mode is set for the switchover source server, and server switchover processing ends. If the switchover source server has been stopped, the switchover source server does not start.
 - Even when more than one spare server is set for the primary server, there is no automatic switch to another spare server. Specify another spare server, then perform server switchover manually.
 - To perform operations on the switchover source server, start the server and then release maintenance mode. However, when Auto-Recovery is enabled and the switchover source server is faulty, Auto-Recovery occurs when maintenance mode is released. Restore the switchover source server to its pre-fault status and then release maintenance mode.

Redundancy Configurations for the Admin LAN

If communication issues occur on the admin LAN, or one of the network interfaces used by a managed server on the admin LAN fails, the following operations may result in errors. In such cases, restore the admin LAN network as quickly as possible.

- Backup and restore operations
- Collection and deployment of cloning images
- Server switchover and failback

HBA Address Rename

- With Resource Orchestrator, the factory-set WWN of a managed server's HBA is overridden when the HBA address rename function is used. The WWN is reset to its factory-set value when the server is deleted from Resource Orchestrator.
Before using HBAs in an environment that is not managed by Resource Orchestrator, first delete the server in which it is mounted using the ROR console.
For information on deleting servers, refer to "5.2 Deleting Managed Servers" of the "User's Guide VE".
- The WWN of a managed server is set during startup, using a network boot session to connect to the admin server. Once set up with a proper WWN, the managed server reboots into its own Operating System.
Therefore, a managed server may reboot during its startup.
- Do not move HBAs whose HBA address rename settings have been set up to different managed servers. If operating HBAs without resetting their WWNs, when the same WWN is configured on multiple servers data may be damaged by same volume access.

ETERNUS SF Storage Cruiser Coordination

- When using ETERNUS SF Storage Cruiser integration for Resource Orchestrator, zoning of Fibre Channel switches connecting to the HBAs of managed servers, and host affinity configurations for storage units will be changed by the WWN information settings. When deleting a server, the relevant zoning and host affinity settings are also deleted. For information on deleting servers, refer to "5.2 Deleting Managed Servers" of the "User's Guide VE".
- When configuring WWN information during OS operation, do not delete existing configurations. If a server is deleted accidentally, users may be unable to access the disk, the OS may hang, or the contained data may be damaged.

Changing the Manager's System Time

- When the admin server's system time is reset to a time in the past, the resource monitoring by the manager stops for this period. To reset the system time to more than just a few minutes in the past, return the time and then restart the manager. To restart the manager, refer to "7.2 Starting and Stopping the Manager" of the "Setup Guide VE".

Restarting Managers

By default, the manager services restart at 3:45 am everyday for stable system operation.

The settings for restarting can be changed depending on the authority level. To change the configuration, perform the following:

- Configuration File

[Windows]

Installation_folder\Manager\rails\config\rcx\rcx_manager_params.rb

[Linux]

/opt/FJSVrcvnr/rails/config/rcx/rcx_manager_params.rb

- Configuration Parameters

Table A.1 Configuration Parameters

Parameter	Meaning	Default Value
RESTART_ENABLE	Select the restart operation status. Specify one of the following: <ul style="list-style-type: none">- When restarting the manager services Specify "true".- When not restarting the manager services Specify "false".	true
RESTART_HOUR	Specify the restart time (hour) from 0 to 23.	3
RESTART_MIN	Specify the restart time (minutes) from 0 to 59.	45
RESTART_CYCLE	Specify the restart interval (days) from 1 to 5.	1

- Parameter change procedure

1. Stop the manager.
2. Use an editor and change the parameters of the rcx_manager_params.rb file.
3. Restart the manager.

For details on how to start and stop the manager, refer to "7.2 Starting and Stopping the Manager" of the "Setup Guide VE".



The conditions for restarting are, that more than `RESTART_CYCLE * 24` hours have passed since manager was started and it is the time specified for `RESTART_HOUR` and `RESTART_MIN`.

Modifying Multiplicity of the Manager Processes

For the manager, the number of processes executed at the same time is limited to optimize the memory usage.

Depending on the environment for use, the upper limit can be modified. To modify the configuration, edit the following definition file.

If there is no definition file, create one.

Placeholder for the Definition File

[Linux]

`/etc/opt/FJSVrcvmt/customize_data`

[Windows]

`Installation_folder\Manager\etc\customize_data`

Name of the Definition File

`rcx_base.rcxprop`

Format of the Definition File

For the definition file, write each line in the following format:

`Key = Value`

Items in the Definition File

Specify the following items.

Table A.2 Items in the Definition File

Item	Key	Value	Remarks
Multiplicity	<code>TASK_WORKER_COUNT</code>	Specify the multiplicity from 5 - 30.	The initial value is "5". If there is no definition file, the default value is used.

Example of the Definition File

The following is an example of the definition file. In this example, the multiplicity is set to "10".

`TASK_WORKER_COUNT=10`

Modification Procedure for the Definition File

- When the manager is operating in a normal environment
 1. Stop the manager.
 2. Use an editor and change the value of `TASK_WORKER_COUNT` in the `rcx_base.rcxprop` file.
If there is no `rcx_base.rcxprop` file, create one.
 3. Restart the manager.
- When the manager is operating in a cluster environment

[Windows]

1. Stop the manager.
2. Place the shared disk of the manager online. Place other cluster resources offline.

- Use an editor and change the value of "TASK_WORKER_COUNT" in the rcx_base.rcxprop file on the shared disk. If there is no rcx_base.rcxprop file, create one.

Placeholder for the Definition File

Drive_name\Fujitsu\ROR\SVROR\customize_data\rcx_base.rcxprop

- Restart the manager.

[Linux]

- Stop the manager.
- Mount the shared disk for the admin server on the primary or secondary node.
- Use an editor and change the value of TASK_WORKER_COUNT in the rcx_base.rcxprop file on the shared disk. If there is no rcx_base.rcxprop file, create one.

Placeholder for the Definition File

Mount_destination_of_shared_disk\Fujitsu\ROR\SVROR/etc/opt/FJSSVrcvmr/customize_data\rcx_base.rcxprop

- Unmount the shared disk for the admin server from the node mounted in step 2.
- Restart the manager.

For details on how to start and stop the manager, refer to "7.2 Starting and Stopping the Manager" of the "Setup Guide VE".



Note

Memory usage will increase according to the multiplicity.

For details on the memory usage to increase, refer to "[Table A.3 Increased Memory Use with Multiple Operations](#)".

Calculate the memory used from a value in the table and the memory size required for the manager operations described in "1.4.2.6 Memory Size" of the "Setup Guide VE", and then add memory if necessary.

Table A.3 Increased Memory Use with Multiple Operations

Multiplicity	Increase in Memory Use (Unit: MB)
5	-
6 - 14	$1080 + (Multiplicity * 40)$
15 - 30	$2104 + (Multiplicity * 40)$

Appendix B Admin Server Backup and Restore

This section explains how to back up and restore the admin server.

B.1 Overview

By backing up the resources of Resource Orchestrator listed below, it is possible to restore the admin server even if files needed to boot the OS are deleted, or files of the manager are deleted from the installation folder making it impossible to boot this software, or other mistakes made by system administrators result in damage to the system.

It is recommended that you create a backup once a system has been set up under Resource Orchestrator, and after the registration, modification, or deletion of resources. By backing up those resources periodically, the environment can be restored to its previous state (when the backup was created).

B.1.1 Managed Resources and Update Timing

The resource files managed by Resource Orchestrator are as shown below:

- Configuration definition information of Resource Orchestrator (the database of the Resource Orchestrator manager)
- System images and cloning images (files in the image file storage folder)

Table B.1 Backup Targets and Update Timing

Target Resources	Relevant Backup Command	Resources to Back Up when Configuring a System	When Backup is Necessary	Necessity of Stopping Managers	Remarks
Certificates	rcxkeydefbackup	Yes	None	Not Required	-
Session encryption keys	rcxkeydefbackup	Yes	After password saving (after execution of the rcxlogin -save command)	Not Required	-
System images and cloning images	scwbackup	Yes	After addition, deletion, and modification of physical server images	Not Required	-
Configuration definition information	rcxbackup	Yes	After creation, registration, modification, unregistration, and deletion of resources	Not Required	-
Information related to image files	scwbackup	Yes	After the registration and unregistration of VM hosts	Not Required	-
Definition files	rcxkeydefbackup	Yes	Modification of definition files	Not Required	-
Image management information	rcxkeydefbackup	Yes	After rcxadm imagemgr command operations	Not Required	-

Backup operations are necessary at the timing listed in "Table B.1 Backup Targets and Update Timing", and after the following maintenance operations.

After backup, only when the following hardware configuration and configuration changes have not been performed, it is possible to perform restoration.

When performing hardware configuration or configuration changes, perform backup again.

- Replacement of a chassis, LAN switch, managed server, power monitoring device hardware

- Replacement of a managed server NIC
- LAN connection between managed servers and LAN switches
- Server switchover or takeover (*1)

*1: If failback has been performed after server switchover, restore can be performed.

Note

The configuration definition information managed by Resource Orchestrator is the target of backup and restore.

VM management software, VM hosts, VM guest boot images, and VM guest virtual disks are not the target of backup and restore. Perform backup and restore another way.

B.1.2 Backup

This section explains backup of the admin server.

The following two types of backup operations can be performed.

Backup after Environment Creation

After environment creation, back up all of the management information (Resource Orchestrator resources on the admin server) using the following procedure.

For details, refer to "[B.2.1 Backing Up All Management Information](#)".

1. Back up certificates, session encryption keys, definition files, and image management information (rcxkeydefbackup)
2. Back up information related to image files, system images, and cloning images (scwbackup)
3. Back up configuration definition information (rcxbackup)

Periodical Backup and the Backup of Configuration Definition Information

There are backup methods such as periodical backup operations in short intervals (such as backup performed once every hour) and backup performed repeatedly whenever the configuration definition information is updated.

For details, refer to "[B.2.2 Backing up Configuration Definition Information](#)".

B.1.3 Restoring the Admin Server

Restore backed up resources to the admin server using the following procedure.

For details, refer to "[B.3 Restore](#)".

1. Reinstall the manager and restore the certificates, session encryption keys, definition files, and image management information (rcxkeydefrestore)
2. Restore information related to image files, system images, and cloning images (scwrestore)
3. Restore configuration definition information (rcxrestore)

When collecting backups periodically or after registering, modifying, or deleting resources, it is not necessary to collect all resources. It is usual to back up configuration definition information. When resources other than configuration definition information are updated, collect all resources of Resource Orchestrator on the admin server.

Information

Recovery can be performed by first backing up the entire admin server disk, and then restoring it.

In a clustered manager configuration, the disk shared between cluster nodes should also be backed up and restored.

When backing up Resource Orchestrator resources after backing up the entire disk of the admin server, restore the entire disk of the admin server and then perform steps 2. - 6. in "[B.3 Restore](#)", and restore system images, cloning images, and configuration definition information.

B.1.4 Backup and Restore Commands

Use the backup and restore commands to perform backup and restoration of configuration definition information (the database of Resource Orchestrator manager).

The Backup and Restore commands support online backup, which is the backup of managers without stopping them.

After restoration, the status is the same as that immediately after the backup operation.

For details on the command, refer to "Chapter 6 Backup and Restore the Configuration of Resource Orchestrator" in the "Command Reference".



Execution Timing for the Backup and Restore Command

When executing the backup and restoration commands, take care regarding the following points:

- While the following operations are being performed, do not execute backup or restore of the admin server:
 - Server switchover and failback
 - Backup and restoration of system images
 - Collection and deployment of cloning images

When a periodical backup operation is performed without stopping the manager, if a conflict between the backup operation and the operations mentioned above occurs, the backup operation will be postponed until the operation is completed.

B.2 Backup

This section explains how to back up the admin server.

For the admin server, the following two types of backup operations can be performed.

- Backup after Environment Creation

For details, refer to "[B.2.1 Backing Up All Management Information](#)".

- Periodical Backup and the Backup of Configuration Definition Information

There are backup methods such as periodical backup operations in short intervals (such as backup performed once every hour) and backup performed repeatedly whenever the configuration definition information is updated.

For details, refer to "[B.2.2 Backing up Configuration Definition Information](#)".

Before starting periodical backup, it is necessary to decide the following items:

Backup Setting Items and What to Decide

- Frequency of Backing Up All Management Information

Decide how often you want to back up all of the management information.



After setting up a system

03:00 A.M. on the 1st day of every month

- Frequency of Periodical Backup

Specify how often you want to back up the configuration definition file.

Example

Once every hour

- Backup Destination

Decide the disk on which the backup data will be stored.

It is recommended to specify a different disk from the one that Resource Orchestrator is installed on.

For details on the free disk space necessary for backups, refer to the notes in "[B.2.1 Backing Up All Management Information](#)".

Backup Destination

The backup destination for configuration definition information can be defined beforehand. Define the following:

Storage location for the tuning parameter file

[Windows]

Installation_folder\Manager\etc\customize_data

[Linux]

/etc/opt/FJSVrcvmr/customize_data

Name for the tuning parameter file

manager_backup.rcxprop

Format of the tuning parameter file

Set the following parameter in the tuning parameter file:

```
backup_dir=Backup_destination_folder
```

If this tuning parameter file is omitted, the backup data will be saved in the following folder:

[Windows]

Installation_folder\Manager\var\backup

[Linux]

/var/opt/FJSVrcvmr/backup

For details, refer to "[B.2.2 Backing up Configuration Definition Information](#)".

Note

- Backup files of the admin server should be stored on external storage media to prevent the backup data from being corrupted due to server failure.
- From the second and successive backups, there are no problems even if backed up folders and configuration definition information from the last time are deleted. Delete earlier backups when disk space constraints make it advisable to do so.
- While the following operations are being performed, do not execute backup:
 - Creation, modification, and deletion of resources
 - Server switchover and failback
 - Backup and restoration of system images
 - Collection and deployment of cloning images

When a periodical backup operation is performed without stopping the manager, if a conflict between the backup operation and the operations mentioned above occurs, the backup operation will be postponed until the operation is completed.

- In a clustered manager configuration, because files are stored on the shared disk, the files and folders to be copied in this procedure are those stored on the shared disk.
For details on the folder names used on the shared disk, refer to "Appendix B Manager Cluster Operation Settings and Deletion" in the "Installation Guide VE".

B.2.1 Backing Up All Management Information

This section explains the backup operation after configuring a system using Resource Orchestrator.

1. Back up certificates, session encryption keys, definition files, and image management information

Execute the `rcxkeydefbackup` command to back up certificates, session keys, definition files, and image management information. For details on the `rcxkeydefbackup` command, refer to "6.5 `rcxkeydefbackup`" in the "Command Reference".

[Windows]

`Installation_folder\Manager\bin\rcxkeydefbackup`

[Linux]

`/opt/FJSVrcvmr/bin/rcxkeydefbackup`

```
rcxkeydefbackup [-dir directory] [[-immediate]][-timeout value] <RETURN>
```

Backup files are created in the specified folder, using the following format:

Format

[Windows]

`Host_name_keydef_YYYYMMDD_HHMM.jar`

[Linux]

`Host_name_keydef_YYYYMMDD_HHMM.tar.bz2`

Date/Time format

`YYYYMMDD` is the date when certificates, session keys, definition files and image management information were backed up.

Item	Value
YYYY	Year
MMDD	Month and date
HHMM	Time

Note

- When this command is executed while Resource Orchestrator is being operated, command execution will be postponed until the operation is complete.
- The file size of backup files varies depending on the number of definition files. The backup file for a configuration storing 100 definition files of 10KB requires less than 1MB. Use this size as a guide when you prepare the backup area.

As saved passwords are stored in the home directory of the OS user account for which the password was saved using the `rcxlogin` command, it is also recommended to back up of the contents of the home directory.

2. Back up information related to image files, system images, and cloning images

Execute the `scwbackup` command to back up information related to image files, system images, and cloning images. For details on the `scwbackup` command, refer to "6.3 `scwbackup`" in the "Command Reference".

[Windows]

`Installation_folder\Manager\bin\scwbackup`

[Linux]

`/opt/FJSVrcvmr/bin/scwbackup`

```
>scwbackup [-dir directory] [[-immediate]][-timeout value] <RETURN>
```

Information related to image files, system images, and cloning images are stored in the folders with the following formats created in the specified folder.

Format

Host_name_scw_YYYYMMDD_HHMM

Date/Time format

YYYYMMDD indicates when the system information was backed up.

Item	Value
YYYY	Year
MMDD	Month and date
HHMM	Time

Note

- When this command is executed while Resource Orchestrator is being operated, command execution will be postponed until the operation is complete.
- The file size of backup files and directories varies depending on the number of resources in image files information. Prepare the area for backup information referring to "Image File Storage Area" in "1.4.2.5 Dynamic Disk Space" in the "Setup Guide VE".

3. Back up virtual machines of VM management software

For details on how to perform backup, refer to the manual of the VM management software.

4. Back up configuration definition information

Execute the following commands to write configuration definition information. Specify a directory or folder to write the configuration definition information and the version XML to.

Specify the directory or folder using `-dir`. If the specified directory or folder does not exist, an error occurs.

For details on the `rcxbackup` command, refer to "6.1 `rcxbackup`" in the "Command Reference".

[Windows]

```
Installation_folder\Manager\bin\rcxbackup
```

[Linux]

```
/opt/FJSVrcvnr/bin/rcxbackup
```

```
>rcxbackup [-dir directory] [[-immediate]][-timeout value] <RETURN>
```

Backup files are created in the specified folder, using the following format:

Format

[Windows]

Host_name_YYYYMMDD_HHMM.jar

[Linux]

Host_name_YYYYMMDD_HHMM.tar.bz2

Date/Time format

YYYYMMDD indicates when the configuration definition information was backed up.

Item	Value
YYYY	Year
MMDD	Month and date
HHMM	Time

Note

- When this command is executed while Resource Orchestrator is being operated, command execution will be postponed until the operation is complete.
- The file size of backup files varies depending on the number of resources defined in the configuration definition information. The backup file for a configuration managing 1,000 VM guests requires less than 2MB. Use this size as a guide when you prepare the backup area. Although this file is created as a compressed file, a decompressed file is temporarily created during the backup process. Therefore, sufficient free space for the decompressed file (e.g. approximately 150 MB for 1,000 VM guests) is necessary.

5. Back up the directory service

When using a directory service for user management, back up the directory service.

For details on how to perform backup, refer to the manual of the directory service.

B.2.2 Backing up Configuration Definition Information

This section explains backup methods such as periodical backup operations in short intervals (Example: Backup performed every hour) and backup performed repeatedly whenever the configuration definition information is updated.

Execute the following commands to write configuration definition information. Configuration definition information and the version XML are written to that directory or folder in compressed format. Specify the destination folder.

Specify the folder using `-dir`. If the specified folder does not exist, an error occurs.

For details on the `rcxbackup` command, refer to "6.1 `rcxbackup`" in the "Command Reference".

[Windows]

```
Installation_folder\Manager\bin\rcxbackup
```

[Linux]

```
/opt/FJSVrcvnr/bin/rcxbackup
```

```
>rcxbackup [-dir directory] [[-immediate]][-timeout value] <RETURN>
```

Note

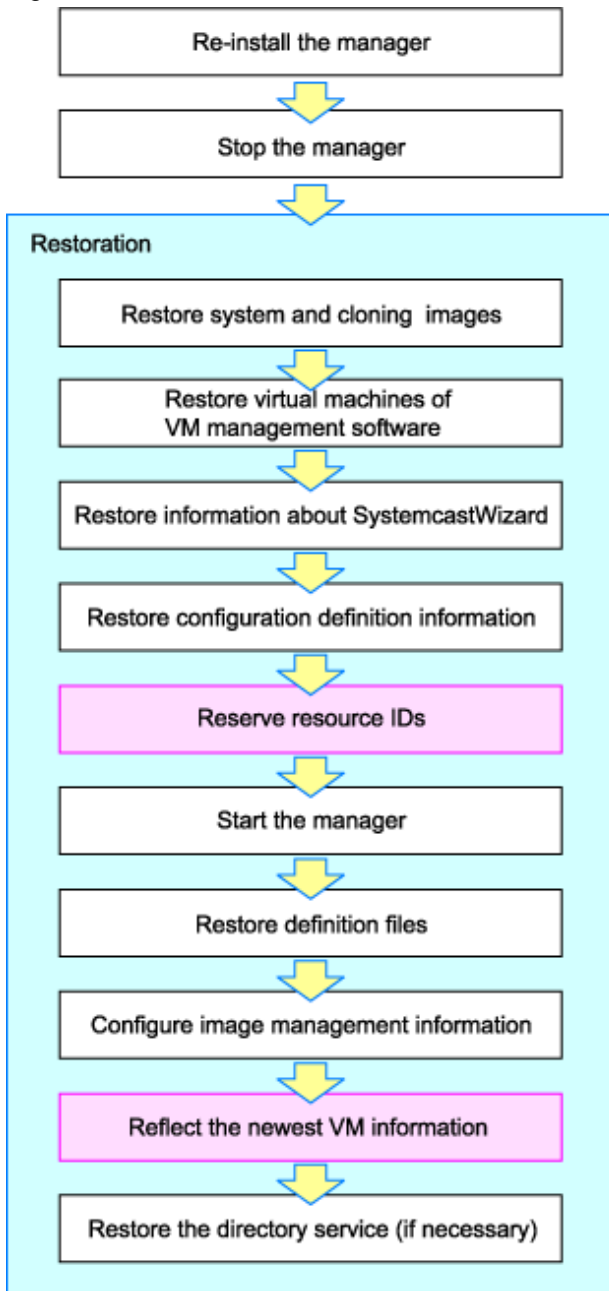
When this command is executed while Resource Orchestrator is being operated, command execution will be postponed until the operation is complete.

B.3 Restore

This section explains how to restore the admin server.

Restore the admin server using the following procedure:

Figure B.1 Flow of Admin Server Restoration



 : Activities performed when restoring the operations from after a backup

Note

In a clustered manager configuration, restore backed up contents to the cluster-shared disk.

For details on the folder names used on the shared disk, refer to "Appendix B Manager Cluster Operation Settings and Deletion" in the "Installation Guide VE".

Restore the admin server using the following procedure:

1. Reinstall the manager, stop it, restore the certificates, session encryption keys, definition files, and image management information
 - a. When the manager does not operate correctly due to damaged files, uninstall the manager and then reinstall it.

Note

When using HBA address rename, the procedure for uninstallation during restoration is different.

Do not perform the operation described in "1. Delete servers" in "Pre-uninstallation Advisory Notes" of "3.1.1 Preparations" in the "Installation Guide VE".

Stop the manager after re-installation.

For details on how to stop the manager, refer to "7.2 Starting and Stopping the Manager" of the "Setup Guide VE".

- b. Execute the `rcxkeydefrestore` command to restore certificates, session encryption keys, definition files, and image management information.

For details on the `rcxkeydefrestore` command, refer to "6.6 `rcxkeydefrestore`" in the "Command Reference".

[Windows]

```
Installation_folder\Manager\bin\rcxkeydefrestore
```

[Linux]

```
/opt/FJSVrcvmr/bin/rcxkeydefrestore
```

```
>rcxkeydefrestore -file filename <RETURN>
```

Because saved passwords are stored in the home directory of the OS user account for which the password was saved, authentication may fail if the home directory contents were damaged. In that case, either restore the contents of the home directory or save the password again using the `rcxlogin` command.

2. Restore information related to image files, system images and cloning images

Execute the `scwrestore` command to restore information related to image files, system images, and cloning images.

For details on the `scwrestore` command, refer to "6.4 `scwrestore`" in the "Command Reference".

[Windows]

```
Installation_folder\Manager\bin\scwrestore
```

[Linux]

```
/opt/FJSVrcvmr/bin/scwrestore
```

```
>scwrestore -dir directory <RETURN>
```

3. Restore virtual machines of VM management software

For details on restoration, refer to the manual of the VM management software.

4. Restore configuration definition information

Restore the configuration definition information exported by following the instructions given in "[B.2.2 Backing up Configuration Definition Information](#)".

Execute the following command.

For details on the `rcxrestore` command, refer to "6.2 `rcxrestore`" in the "Command Reference".

[Windows]

```
Installation_folder\Manager\bin\rcxrestore
```

[Linux]

```
/opt/FJSVrcvmr/bin/rcxrestore
```

```
>rcxrestore -file filename <RETURN>
```

Note

Specify the command using an absolute path.

5. Start the manager

For details on how to start the manager, refer to "7.2 Starting and Stopping the Manager" in the "Setup Guide VE".

6. Reflect the newest information of VM on Resource Orchestrator using VM management software.

For details on the rcxadm vmmgr refresh command, refer to "1.7.3 rcxadm vmmgr" in the "Reference Guide (Resource Management) CE".

```
>rcxadm vmmgr refresh <RETURN>
```

Wait for at least 60 seconds.

```
>rcxadm vmmgr refresh <RETURN>
```

 Note

Be sure to wait for 60 seconds or more before executing the rcxadm vmmgr refresh command for the second time. Otherwise, the newest information of VM may not be reflected correctly.

7. Restore a directory service

When using a directory service for user management, restore the directory service.

For details on how to perform restoration, refer to the manual of the directory service.

 Note

- In a clustered manager configuration, restore backed up contents to the cluster-shared disk.
For details on the folder names used on the shared disk, refer to "Appendix B Manager Cluster Operation Settings and Deletion" in the "Installation Guide VE".
- If you are setting a VM host as a spare server, leave "operation" as a hyphen ("-") in the "SpareServer" section of the corresponding physical server. After completing restoration, configure the spare server for the target physical server from the ROR console.
- While the following operations are being performed, do not execute restore:
 - Creation, modification, and deletion of resources
 - Server switchover and failback
 - Backup and restoration of system images
 - During collection and deployment of cloning images
- When performing restoration of certificates, configuration definition information, and system images and cloning images, restore backups taken at the same point in time.
- When the following changes are made to the following hardware settings or configuration definition information after backup, restoration is not possible. Ensure backup is performed again.
 - When backing up of all management information is necessary
 - Replacement of a chassis, LAN switch blade, managed server, or power monitoring device hardware
 - Replacement of a managed server NIC
 - LAN connections between managed servers and LAN switch blades
 - Collection of snapshots
 - Server switchover or takeover (*1)
 - When backing up of configuration definition information again is necessary

*1: If failback has been performed after server switchover, restore can be performed. During restoration of an admin server, do not perform the following operations:

- Migration of VM guests between VM hosts
 - Registration or release of VM guests on VM management software
 - Managed servers using HBA address rename must be restarted after being restored.
 - Maintenance mode settings cannot be recovered after restore. Set the maintenance mode in accordance with the information recorded at the time of backup.
 - When an agent is registered on a managed server and when backup of system images and collection of cloning images is being used, perform either of the following after restoring the admin server.
 - Restart the managed server
 - Restart the services described in "7.3 Starting and Stopping the Agent" in the "Setup Guide VE"
 - LAN switches and physical link data (used by the Network Map) cannot be backed up. Register LAN switches and network links following the instructions, refer to "12.2 Preparations" in the "Operation Guide VE".
 - VIOM coordination user names and passwords cannot be backed up. Register VIOM coordination before performing restoration. For details on operation methods, refer to "2.1 Registering VIOM Coordination" in the "User's Guide VE".
-

Appendix C Event Handling

This appendix explains the event handling function.

This function allows execution of a pre-defined file whenever the admin server receives SNMP Traps (events) from a registered device. This function works with the following devices.

- Chassis (Management blade, management board)
- Managed servers (ServerView)
- Remote Management Controller
- LAN switch

The following file is executed each time an event occurs.

[Windows]

Installation_folder\Manager\etc\trapop.bat Argument 1 Argument 2 Argument 3 Argument 4 Argument 5 Argument 6

[Linux]

/etc/opt/FJSVrcvmr/trapop.sh Argument 1 Argument 2 Argument 3 Argument 4 Argument 5 Argument 6

The default-installed file will log each event, but will not trigger any action based on those events.

However, it is possible to trigger operations such as email notifications or calls to external management software (command calls or event notifications) by providing a custom-script to use in place of the default script.

- The following information is passed as arguments:
 - Argument 1
Message describing the event
 - Argument 2
IP address of the device in which the event occurred
 - Argument 3
Host name (FQDN) inferred from the IP address received in Argument 2 (when the name cannot be inferred, this is set to the device's IP address)
 - Argument 4
Number of milliseconds counted from 01/01/1970 00:00:00 GMT until the current time
 - Argument 5
Event level ("INFO", "WARNING", or "ERROR")
 - Argument 6
Name of the device in which the event occurred

For the following events, however, only the event log is displayed. The file is not executed.

- Events logged during ROR console operations, command execution, or automatic server switchovers due to Auto-Recovery
 - Start of processing, in-progress status, end of processing
 - Changes in resource status during a running process
 - Errors that occur within Resource Orchestrator
- Errors detected from regular monitoring (when no SNMP Trap is sent, or when SNMP traps do not reach the manager because of communication errors or an abnormally high load on the system)



Note

In a clustered manager configuration, it is necessary to store the same file on both the primary and secondary nodes for this function to work properly.

E-Mail Notification Sample

Below is a sample program that will send e-mail notifications for each event received.

To customize e-mail contents and adapt the program to your practical configuration, it is recommended to create your own version using this sample as a reference.

[Windows]

Set the following addresses (in the "E-Mail Notification Sample") to match actual environment values.

- Mail server address
- Sender address
- Destination address

E-Mail Notification Sample (*Installation_folder\Manager\etc\trapop.bat*)

```
@echo off

rem set MAIL_SERVER_ADDRESS=server.address          <- mail server address
rem set MAIL_FROM=from_your@e-mail.address         <- sender address
rem set MAIL_TO=to_your@e-mail.address             <- destination address

rem set MAIL_SUBJECT="Resource Coordinator VE (%COMPUTERNAME%) event mail"

rem set SENDMAIL_VBS=sendmail.vbs

rem set MAILCMD=cscript "%~dp0%SENDMAIL_VBS%" %MAIL_FROM% %MAIL_TO% %MAIL_SUBJECT%
%MAIL_SERVER_ADDRESS% %1 %2 %3 %4 %5 %6 //nologo
rem %MAILCMD%
```

When actually using this script, remove all comments and enter appropriate addresses.

```
@echo off

set MAIL_SERVER_ADDRESS=server.address          <- mail server address
set MAIL_FROM=from_your@e-mail.address         <- sender address
set MAIL_TO=to_your@e-mail.address             <- destination address

set MAIL_SUBJECT="Resource Coordinator VE (%COMPUTERNAME%) event mail"

set SENDMAIL_VBS=sendmail.vbs

set MAILCMD=cscript "%~dp0%SENDMAIL_VBS%" %MAIL_FROM% %MAIL_TO% %MAIL_SUBJECT% %MAIL_SERVER_ADDRESS%
%1 %2 %3 %4 %5 %6 //nologo
%MAILCMD%
```

Information

The sample `sendmail.vbs` file (stored in the same folder as `trapopt.bat`) makes use of Windows CDO (Microsoft Collaboration Data Objects) to connect to an external SMTP server and send e-mail notifications.

For details on VBScript and CDO, refer to the technical reference provided by Microsoft.

[Linux]

Set the following addresses (in the "E-Mail Notification Sample") to match actual environment values.

- Sender address
- Destination address

E-Mail Notification Sample (`/etc/opt/FJSVrcvmr/trapop.sh`)

```
#!/bin/sh

# MAIL_FROM=from_your@e-mail.address  <- sender address
# MAIL_TO=to_your@e-mail.address      <- destination address

# HOSTNAME=`/bin/uname -n`
# MAILCMD="/usr/sbin/sendmail -t"

# $MAILCMD <<ENDMAIL
# From: $MAIL_FROM
# To: $MAIL_TO
# Subject: Resource Coordinator VE($HOSTNAME) event mail

# -----
# Resource Coordinator VE: event mail
# -----
# $1

# ENDMAIL
```

When actually using this script, remove all comments and enter appropriate addresses.

```
#!/bin/sh

MAIL_FROM=from_your@e-mail.address  <- sender address
MAIL_TO=to_your@e-mail.address      <- destination address

HOSTNAME=`/bin/uname -n`
MAILCMD="/usr/sbin/sendmail -t"

$MAILCMD <<ENDMAIL
From: $MAIL_FROM
To: $MAIL_TO
Subject: Resource Coordinator VE($HOSTNAME) event mail

-----
Resource Coordinator VE: event mail
```

```
-----  
$1
```

```
ENDMAIL
```



Information

.....
The above sample assumes that the sendmail command is available on the admin server. Adapt the path to the sendmail command to your own environment. The outgoing SMTP server can be defined by changing the sendmail command's configuration files.
.....

Appendix D Backing Up and Restoring Image Files

This appendix explains how to back up system images and cloning images stored on the admin server to external media and other disks, and how to restore image files backed up on external media or other disks to the admin server.

D.1 Configuration of Folders and Files

This section explains the configuration of image file folders on admin servers.

The descriptions in this section are based on Windows.

For Linux, change "Folder" to "Directory", and "\" to "/".

1. Folders

Image files are stored in the following folders (hereinafter image file storage folder).

- Default Destination

[Windows]

```
"Installation_folder"\SVROR\ScwPro\depot\Cloneimg
```

[Linux]

```
/var/opt/FJSVscw-deploysv/depot/CLONEIMG
```

- When the image files storage destination is changed after installation, using the rcxadm imagemgr command

[Windows]

```
"Specified_folder"\Cloneimg
```

[Linux]

```
"Specified_folder"/CLONEIMG
```

System images and cloning images are stored in different image file storage folders (hereinafter resource folder).

- System image resource folder

```
"Image_file_storage_folder"\Managed_server_name@0@0@Management_information@Management_information@ Version
```

Managed_server_name is the "physical_server_name" registered on the manager.

Management_information is the fixed information.

Version is the version number of the system image of the managed server.

- Cloning image resource folder

```
"Image_file_storage_folder"\Cloning_image_name@ Version
```

Cloning_image_name is the name specified when collecting cloning images.

Version is the version number of cloning images.

2. Files

The following two files are stored in each resource folder for system images and cloning images.

- diskimg.fc2
- diskimg.ini

D.2 Backing Up Image Files

This section explains how to back up image files stored on the admin server.

1. Preparations

a. Confirm the following information regarding backup image files in the [Image List] tab on the ROR console.

- For system images
Server name and version
- For cloning images
Cloning image name and version

b. Logout from all ROR consoles.

c. For Resource Orchestrator, confirm that no operations are being performed.

2. Stop the manager

For details on how to stop the manager, refer to "7.2 Starting and Stopping the Manager" of the "Setup Guide VE".



Confirm whether both the "Manager services" and "Related services" have been stopped.

3. Backing up image files

Copy the resource folders corresponding to the items confirmed in step 1.

The back up operation can be performed to arbitrary folders or external recordable media other than the image file storage folder, using Explorer (for Windows) or the copy command.



The back up operation of image files should be performed for each resource folder.

Start the manager

To start the manager, refer to "7.2 Starting and Stopping the Manager" of the "Setup Guide VE".



Confirm whether both the "Manager services" and "Related services" have been started.

4. Post operation confirmation

a. In the ROR console, select the [Image List] tab.

b. Confirm whether the restored system images and cloning images displayed are the same as the ones displayed during preparation.

D.3 Restoring Image Files

This section explains the procedure to restore the image files backed up on external media.



- System images of managed servers which have not been registered with the manager should not be restored.

- Do not restore image files of managed servers which do not meet the following hardware conditions:
 - The model, motherboard, and CPU of the managed server are identical.
 - The hardware configuration of each server must be identical, including optional cards, expansion boards, and the slots they are mounted in.
 - Make sure that BIOS settings are properly configured. For details of BIOS settings, refer to "BIOS Settings for Managed Servers" in "4.1.2 Configuring the Server Environment" of the "Setup Guide VE".
 - All servers must use the same redundancy configuration (if any) and the same number of redundant paths for LAN and SAN connections. All servers must also be able to access the same network and storage devices.
- The maximum number of versions of image files managed by the manager is three. Do not restore image files of managed servers which exceed the maximum number of versions.

1. Preparations

Confirm the system images and cloning images in the [Image List] tab on the ROR console.

2. Delete image files

Delete system images and cloning images as necessary.

Delete any unnecessary system images and cloning images from the ROR console in advance, to avoid exceeding the maximum number of versions that can be retained for each managed server.

3. Stop the manager

For details on how to stop the manager, refer to "7.2 Starting and Stopping the Manager" of the "Setup Guide VE".



Note

Confirm whether both the "Manager services" and "Related services" have been stopped.

4. Restoring image files

Copy each backed up resource folder to the image file storage folder.



Note

Copy the image files in the image file storage folders using the names of the resource folders when they were backed up.

However, if a resource folder of the same version exists, change the version part of the resource folder to an integer in the range of "1 to the maximum version number plus 1", which does not overlap.

5. Start the manager

To start the manager, refer to "7.2 Starting and Stopping the Manager" of the "Setup Guide VE".



Note

Confirm whether both the "Manager services" and "Related services" have been started.

6. Post operation confirmation

- a. In the ROR console, select the [Image List] tab.
- b. Confirm whether the restored system images and cloning images are displayed.

Glossary

access path

A logical path configured to enable access to storage volumes from servers.

active mode

The state where a managed server is performing operations.

Managed servers must be in active mode in order to use Auto-Recovery.

Move managed servers to maintenance mode in order to perform backup or restoration of system images, or collection or deployment of cloning images.

active server

A physical server that is currently operating.

admin client

A terminal (PC) connected to an admin server, which is used to operate the GUI.

admin LAN

A LAN used to manage resources from admin servers.

It connects managed servers, storage, and network devices.

admin server

A server used to operate the manager software of Resource Orchestrator.

affinity group

A grouping of the storage volumes allocated to servers. A function of ETERNUS.

Equivalent to the LUN mapping of EMC.

agent

The section (program) of Resource Orchestrator that operates on managed servers.

Auto-Recovery

A function which continues operations by automatically switching over the system image of a failed server to a spare server and restarting it in the event of server failure.

This function can be used when managed servers are in a local boot configuration, SAN boot configuration, or a configuration such as iSCSI boot where booting is performed from a disk on a network.

- When using a local boot configuration

The system is recovered by restoring a backup of the system image of the failed server onto a spare server.

- When booting from a SAN or a disk on a LAN

The system is restored by having the spare server inherit the system image on the storage.

Also, when a VLAN is set for the public LAN of a managed server, the VLAN settings of adjacent LAN switches are automatically switched to those of the spare server.

BACS (Broadcom Advanced Control Suite)

An integrated GUI application (comprised from applications such as BASP) that creates teams from multiple NICs, and provides functions such as load balancing.

BASP (Broadcom Advanced Server Program)

LAN redundancy software that creates teams of multiple NICs, and provides functions such as load balancing and failover.

blade server

A compact server device with a thin chassis that can contain multiple server blades, and has low power consumption. As well as server blades, LAN switch blades, management blades, and other components used by multiple server blades can be mounted inside the chassis.

blade type

A server blade type.
Used to distinguish the number of server slots used and servers located in different positions.

BladeViewer

A GUI that displays the status of blade servers in a style similar to a physical view and enables intuitive operation. BladeViewer can also be used for state monitoring and operation of resources.

BMC (Baseboard Management Controller)

A Remote Management Controller used for remote operation of servers.

boot agent

An OS for disk access that is distributed from the manager to managed servers in order to boot them when the network is started during image operations.

CA (Channel Adapter)

An adapter card that is used as the interface for server HBAs and fibre channel switches, and is mounted on storage devices.

chassis

A chassis used to house server blades and partitions.
Sometimes referred to as an enclosure.

cloning

Creation of a copy of a system disk.

cloning image

A backup of a system disk, which does not contain server-specific information (system node name, IP address, etc.), made during cloning.
When deploying a cloning image to the system disk of another server, Resource Orchestrator automatically changes server-specific information to that of the target server.

Cloud Edition

The edition which can be used to provide private cloud environments.

Domain

A system that is divided into individual systems using partitioning. Also used to indicate a partition.

DR Option

The option that provides the function for remote switchover of servers or storage in order to perform disaster recovery.

end host mode

This is a mode where the uplink port that can communicate with a downlink port is fixed at one, and communication between uplink ports is blocked.

environmental data

Measured data regarding the external environments of servers managed using Resource Orchestrator.
Measured data includes power data collected from power monitoring targets.

ESC (ETERNUS SF Storage Cruiser)

Software that supports stable operation of multi-vendor storage system environments involving SAN, DAS, or NAS. Provides configuration management, relation management, trouble management, and performance management functions to integrate storage related resources such as ETERNUS.

Express

The edition which provides server registration, monitoring, and visualization.

FC switch (Fibre Channel Switch)

A switch that connects Fibre Channel interfaces and storage devices.

fibre channel switch blade

A fibre channel switch mounted in the chassis of a blade server.

GLS (Global Link Services)

Fujitsu network control software that enables high availability networks through the redundancy of network transmission channels.

GSPB (Giga-LAN SAS and PCI_Box Interface Board)

A board which mounts onboard I/O for two partitions and a PCIe (PCI Express) interface for a PCI box.

GUI (Graphical User Interface)

A user interface that displays pictures and icons (pictographic characters), enabling intuitive and easily understandable operation.

HA (High Availability)

The concept of using redundant resources to prevent suspension of system operations due to single problems.

hardware initiator

A controller which issues SCSI commands to request processes.
In iSCSI configurations, NICs fit into this category.

hardware maintenance mode

In the maintenance mode of PRIMEQUEST servers, a state other than Hot System Maintenance.

HBA (Host Bus Adapter)

An adapter for connecting servers and peripheral devices.
Mainly used to refer to the FC HBAs used for connecting storage devices using Fibre Channel technology.

HBA address rename setup service

The service that starts managed servers that use HBA address rename in the event of failure of the admin server.

HBAAR (HBA address rename)

I/O virtualization technology that enables changing of the actual WWN possessed by an HBA.

host affinity

A definition of the server HBA that is set for the CA port of the storage device and the accessible area of storage.
It is a function for association of the Logical Volume inside the storage which is shown to the host (HBA) that also functions as security internal to the storage device.

Hyper-V

Virtualization software from Microsoft Corporation.

Provides a virtualized infrastructure on PC servers, enabling flexible management of operations.

I/O virtualization option

An optional product that is necessary to provide I/O virtualization.

The WWNN address and MAC address provided is guaranteed by Fujitsu Limited to be unique.

Necessary when using HBA address rename.

IBP (Intelligent Blade Panel)

One of operation modes used for PRIMERGY switch blades.

This operation mode can be used for coordination with ServerView Virtual I/O Manager (VIOM), and relations between server blades and switch blades can be easily and safely configured.

ILOM (Integrated Lights Out Manager)

The name of the Remote Management Controller for SPARC Enterprise T series servers.

image file

A system image or a cloning image. Also a collective term for them both.

IPMI (Intelligent Platform Management Interface)

IPMI is a set of common interfaces for the hardware that is used to monitor the physical conditions of servers, such as temperature, power voltage, cooling fans, power supply, and chassis.

These functions provide information that enables system management, recovery, and asset management, which in turn leads to reduction of overall TCO.

IQN (iSCSI Qualified Name)

Unique names used for identifying iSCSI initiators and iSCSI targets.

iRMC (integrated Remote Management Controller)

The name of the Remote Management Controller for Fujitsu's PRIMERGY servers.

iSCSI

A standard for using the SCSI protocol over TCP/IP networks.

LAN switch blades

A LAN switch that is mounted in the chassis of a blade server.

license

The rights to use specific functions.

Users can use specific functions by purchasing a license for the function and registering it on the manager.

link aggregation

Function used to multiplex multiple ports and use them as a single virtual port.

With this function, if one of the multiplexed ports fails its load can be divided among the other ports, and the overall redundancy of ports improved.

logical volume

A logical disk that has been divided into multiple partitions.

LSB (Logical System Board)

A system board that is allocated a logical number (LSB number) so that it can be recognized from the domain, during domain configuration.

maintenance mode

The state where operations on managed servers are stopped in order to perform maintenance work.

In this state, the backup and restoration of system images and the collection and deployment of cloning images can be performed.

However, when using Auto-Recovery it is necessary to change from this mode to active mode. When in maintenance mode it is not possible to switch over to a spare server if a server fails.

managed server

A collective term referring to a server that is managed as a component of a system.

management blade

A server management unit that has a dedicated CPU and LAN interface, and manages blade servers.

Used for gathering server blade data, failure notification, power control, etc.

Management Board

The PRIMEQUEST system management unit.

Used for gathering information such as failure notification, power control, etc. from chassis.

manager

The section (program) of Resource Orchestrator that operates on admin servers.

It manages and controls resources registered with Resource Orchestrator.

master slot

A slot that is recognized as a server when a server that occupies multiple slots is mounted.

multi-slot server

A server that occupies multiple slots.

NAS (Network Attached Storage)

A collective term for storage that is directly connected to a LAN.

network device

The unit used for registration of network devices.

L2 switches and firewalls fit into this category.

network map

A GUI function for graphically displaying the connection relationships of the servers and LAN switches that compose a network.

network view

A window that displays the connection relationships and status of the wiring of a network map.

NFS (Network File System)

A system that enables the sharing of files over a network in Linux environments.

NIC (Network Interface Card)

An interface used to connect a server to a network.

OS

The OS used by an operating server (a physical OS or VM guest).

PDU (Power Distribution Unit)

A device for distributing power (such as a power strip).

Resource Orchestrator uses PDUs with current value display functions as Power monitoring devices.

physical LAN segment

A physical LAN that servers are connected to.

Servers are connected to multiple physical LAN segments that are divided based on their purpose (public LANs, backup LANs, etc.).

Physical LAN segments can be divided into multiple network segments using VLAN technology.

physical OS

An OS that operates directly on a physical server without the use of server virtualization software.

physical server

The same as a "server". Used when it is necessary to distinguish actual servers from virtual servers.

pin-group

This is a group, set with the end host mode, that has at least one uplink port and at least one downlink port.

Pool Master

On Citrix XenServer, it indicates one VM host belonging to a Resource Pool.

It handles setting changes and information collection for the Resource Pool, and also performs operation of the Resource Pool.

For details, refer to the Citrix XenServer manual.

port backup

A function for LAN switches which is also referred to as backup port.

port VLAN

A VLAN in which the ports of a LAN switch are grouped, and each LAN group is treated as a separate LAN.

port zoning

The division of ports of fibre channel switches into zones, and setting of access restrictions between different zones.

power monitoring devices

Devices used by Resource Orchestrator to monitor the amount of power consumed.

PDUs and UPSs with current value display functions fit into this category.

power monitoring targets

Devices from which Resource Orchestrator can collect power consumption data.

pre-configuration

Performing environment configuration for Resource Orchestrator on another separate system.

primary server

The physical server that is switched from when performing server switchover.

public LAN

A LAN used for operations by managed servers.

Public LANs are established separately from admin LANs.

rack

A case designed to accommodate equipment such as servers.

rack mount server

A server designed to be mounted in a rack.

RAID (Redundant Arrays of Inexpensive Disks)

Technology that realizes high-speed and highly-reliable storage systems using multiple hard disks.

RAID management tool

Software that monitors disk arrays mounted on PRIMERGY servers.

The RAID management tool differs depending on the model or the OS of PRIMERGY servers.

Remote Management Controller

A unit used for managing servers.

Used for gathering server data, failure notification, power control, etc.

- For Fujitsu PRIMERGY servers

iRMC2

- For SPARC Enterprise

ILOM (T series servers)

XSCF (M series servers)

- For HP servers

iLO2 (integrated Lights-Out)

- For Dell/IBM servers

BMC (Baseboard Management Controller)

Remote Server Management

A PRIMEQUEST feature for managing partitions.

Reserved SB

Indicates the new system board that will be embedded to replace a failed system board if the hardware of a system board embedded in a partition fails and it is necessary to disconnect the failed system board.

resource

Collective term or concept that refers to the physical resources (hardware) and logical resources (software) from which a system is composed.

resource pool

On Citrix XenServer, it indicates a group of VM hosts.

For details, refer to the Citrix XenServer manual.

resource tree

A tree that displays the relationships between the hardware of a server and the OS operating on it using hierarchies.

ROR console

The GUI that enables operation of all functions of Resource Orchestrator.

SAN (Storage Area Network)

A specialized network for connecting servers and storage.

server

A computer (operated with one operating system).

server blade

A server blade has the functions of a server integrated into one board.
They are mounted in blade servers.

server management unit

A unit used for managing servers.
A management blade is used for blade servers, and a Remote Management Controller is used for other servers.

server name

The name allocated to a server.

server virtualization software

Basic software which is operated on a server to enable use of virtual machines. Used to indicate the basic software that operates on a PC server.

ServerView Deployment Manager

Software used to collect and deploy server resources over a network.

ServerView Operations Manager

Software that monitors a server's (PRIMERGY) hardware state, and notifies of errors by way of the network.
ServerView Operations Manager was previously known as ServerView Console.

ServerView RAID

One of the RAID management tools for PRIMERGY.

ServerView Update Manager

This is software that performs jobs such as remote updates of BIOS, firmware, drivers, and hardware monitoring software on servers being managed by ServerView Operations Manager.

ServerView Update Manager Express

Insert the ServerView Suite DVD1 or ServerView Suite Update DVD into the server requiring updating and start it.

This is software that performs batch updates of BIOS, firmware, drivers, and hardware monitoring software.

Single Sign-On

A system among external software which can be used without login operations, after authentication is executed once.

slave slot

A slot that is not recognized as a server when a server that occupies multiple slots is mounted.

SMB (Server Message Block)

A protocol that enables the sharing of files and printers over a network.

SNMP (Simple Network Management Protocol)

A communications protocol to manage (monitor and control) the equipment that is attached to a network.

software initiator

An initiator processed by software using OS functions.

Solaris Container

Solaris server virtualization software.

On Solaris servers, it is possible to configure multiple virtual Solaris servers that are referred to as a Solaris zone.

Solaris zone

A software partition that virtually divides a Solaris OS space.

SPARC Enterprise Partition Model

A SPARC Enterprise model which has a partitioning function to enable multiple system configurations, separating a server into multiple areas with operating OS's and applications in each area.

spare server

A server which is used to replace a failed server when server switchover is performed.

storage blade

A blade-style storage device that can be mounted in the chassis of a blade server.

storage unit

Used to indicate the entire secondary storage as one product.

switchover state

The state in which switchover has been performed on a managed server, but neither failback nor continuation have been performed.

System Board

A board which can mount up to 2 Xeon CPUs and 32 DIMMs.

system disk

The disk on which the programs (such as the OS) and files necessary for the basic functions of servers (including booting) are installed.

system image

A copy of the contents of a system disk made as a backup.

Different from a cloning image as changes are not made to the server-specific information contained on system disks.

tower server

A standalone server with a vertical chassis.

UNC (Universal Naming Convention)

Notational system for Windows networks (Microsoft networks) that enables specification of shared resources (folders, files, shared printers, shared directories, etc.).



Example

.....
\\hostname\dir_name
.....

UPS (Uninterruptible Power Supply)

A device containing rechargeable batteries that temporarily provides power to computers and peripheral devices in the event of power failures.

Resource Orchestrator uses UPSs with current value display functions as power monitoring devices.

URL (Uniform Resource Locator)

The notational method used for indicating the location of information on the Internet.

VIOM (ServerView Virtual-IO Manager)

The name of both the I/O virtualization technology used to change the MAC addresses of NICs and the software that performs the virtualization.

Changes to values of WWNs and MAC addresses can be performed by creating a logical definition of a server, called a server profile, and assigning it to a server.

Virtual Edition

The edition that can use the server switchover function.

Virtual I/O

Technology that virtualizes the relationship of servers and I/O devices (mainly storage and network) thereby simplifying the allocation of and modifications to I/O resources to servers, and server maintenance.

For Resource Orchestrator it is used to indicate HBA address rename and ServerView Virtual-IO Manager (VIOM).

virtual server

A virtual server that is operated on a VM host using a virtual machine.

virtual switch

A function provided by server virtualization software to manage networks of VM guests as virtual LAN switches.

The relationships between the virtual NICs of VM guests and the NICs of the physical servers used to operate VM hosts can be managed using operations similar to those of the wiring of normal LAN switches.

VLAN (Virtual LAN)

A splitting function, which enables the creation of virtual LANs (seen as differing logically by software) by grouping ports on a LAN switch.

Using a Virtual LAN, network configuration can be performed freely without the need for modification of the physical network configuration.

VLAN ID

A number (between 1 and 4,095) used to identify VLANs.

Null values are reserved for priority tagged frames, and 4,096 (FFF in hexadecimal) is reserved for mounting.

VM (Virtual Machine)

A virtual computer that operates on a VM host.

VM guest

A virtual server that operates on a VM host, or an OS that is operated on a virtual machine.

VM Home Position

The VM host that is home to VM guests.

VM host

A server on which server virtualization software is operated, or the server virtualization software itself.

VM maintenance mode

One of the settings of server virtualization software, that enables maintenance of VM hosts.

For example, when using high availability functions (such as VMware HA) of server virtualization software, by setting VM maintenance mode it is possible to prevent the moving of VM guests on VM hosts undergoing maintenance.

For details, refer to the manuals of the server virtualization software being used.

VM management software

Software for managing multiple VM hosts and the VM guests that operate on them.

Provides value adding functions such as movement between the servers of VM guests (migration).

VMware

Virtualization software from VMware Inc.

Provides a virtualized infrastructure on PC servers, enabling flexible management of operations.

Web browser

A software application that is used to view Web pages.

WWN (World Wide Name)

A 64-bit address allocated to an HBA.

Refers to a WWNN or a WWPN.

WWNN (World Wide Node Name)

The WWN set for a node.

The Resource Orchestrator HBA address rename sets the same WWNN for the fibre channel port of the HBA.

WWPN (World Wide Port Name)

The WWN set for a port.

The Resource Orchestrator HBA address rename sets a WWPN for each fibre channel port of the HBA.

WWPN zoning

The division of ports into zones based on their WWPN, and setting of access restrictions between different zones.

Xen

A type of server virtualization software.

XSB (eXtended System Board)

Unit for domain creation and display, composed of physical components.

XSCF (eXtended System Control Facility)

The name of the Remote Management Controller for SPARC Enterprise M series servers.

zoning

A function that provides security for Fibre Channels by grouping the Fibre Channel ports of a Fibre Channel switch into zones, and only allowing access to ports inside the same zone.