

# **FUJITSU Software**

## **ServerView Resource Orchestrator**

### **Virtual Edition V3.4.0**

A decorative horizontal band with a red-to-dark-red gradient, featuring abstract, glowing white and red lines that swirl and intersect, creating a sense of motion and technology.

# Operation Guide

Windows/Linux

J2X1-7605-09ENZ0(03)  
October 2020

# Preface

---

## Purpose of This Document

This manual explains how to operate FUJITSU Software ServerView Resource Orchestrator Virtual Edition (hereinafter Resource Orchestrator).

## Intended 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 2 Overview" of the "Design 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 3 Resource Management Overview" in the "User's Guide VE".

## Structure of This Document

This manual is composed as follows:

### Part 1 Overview

#### [Chapter 1 Overview of Operations, Maintenance, and Monitoring](#)

Provides an overview of the operation, maintenance, and monitoring of Resource Orchestrator.

### Part 2 Operation

#### [Chapter 2 Starting and Stopping Managers and Agents](#)

Explains the methods for deliberately starting and stopping managers and agents.

#### [Chapter 3 Managing User Accounts](#)

Explains the management of user accounts.

#### [Chapter 4 Server Switchover](#)

Explains how to use the server switchover function.

#### [Chapter 5 Event Handling](#)

Explains the event handling function.

### Part 3 Maintenance

#### [Chapter 6 Hardware Maintenance](#)

Explains the maintenance of hardware.

#### [Chapter 7 Maintaining Software with Cloning \[Physical Servers\]](#)

Explains how to perform software maintenance using the cloning function.

#### [Chapter 8 Backup and Restoration of Managed Servers](#)

Explains how to back up and restore managed servers.

#### [Chapter 9 Backup and Restoration of Admin Servers](#)

Explains how to back up and restore the admin server.

#### [Chapter 10 Backing Up and Restoring Image Files](#)

Explains how to back up and restore system images and cloning images.

## Part 4 Monitoring

### Chapter 11 Monitoring Resources

Explains how to monitor the configuration and status of managed resources.

### Chapter 12 Collecting Power Consumption Data and Displaying Graphs

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.

## Part 5 Modification

### Chapter 13 Changing Settings

Explains how to modify various setting information.

### Appendix A Notes on Operating ServerView Resource Orchestrator

Gives important reminders for the operation of Resource Orchestrator.

## Web Site URLs

URLs provided as reference sources within the main text are correct as of October 2020.

## Document Conventions

The notation in this manual conforms to the following conventions.

- When there is different information for the different versions of Resource Orchestrator, it is indicated as follows.

[All Editions]	Sections relevant for all editions
[Cloud Edition]	Sections related to Cloud Edition
[Virtual Edition]	Sections related to Virtual Edition

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

[Windows Manager]

Sections related to Windows manager

[Linux Manager]

Sections related to Linux manager

[Windows]

Sections related to Windows

[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

[Horizon View]

Sections related to VMware Horizon View

[Hyper-V]

Sections related to Hyper-V

[Xen]

Sections related to RHEL5-Xen

[KVM]

Sections related to RHEL-KVM

[Solaris Zones]

Sections related to Solaris Zones (Solaris 10) and Solaris Zones (Solaris 11)

[Solaris Zones (Solaris 10)]

Sections related to Solaris Zones with Solaris 10 VM hosts

[Solaris Zones (Solaris 11)]

Sections related to Solaris Zones with Solaris 11 VM hosts

[OVM for x86]

Sections related to Oracle VM Server for x86 2.2 and Oracle VM Server for x86 3.x

[OVM for x86 2.2]

Sections related to Oracle VM Server for x86 2.2

[OVM for x86 3.x]

Sections related to Oracle VM Server for x86 3.2 and Oracle VM Server for x86 3.3

[OVM for SPARC]

Sections related to Oracle VM Server for SPARC

[Citrix Xen]

Sections related to Citrix XenServer

[Physical Servers]

Sections related to physical servers

[Trend Micro OfficeScan]

Sections related to Trend Micro OfficeScan

[Symantec]

Sections related to Symantec Endpoint Protection

[McAfee]

Sections related to McAfee ePolicy Orchestrator

- 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.
- Oracle Solaris Zones may also be indicated as Solaris Containers or Solaris Container.
- Oracle VM Server for x86 may also be indicated as Oracle VM.
- In Resource Orchestrator, the following servers are referred to as SPARC Enterprise.
  - SPARC Enterprise M3000/M4000/M5000/M8000/M9000
  - SPARC Enterprise T5120/T5140/T5220/T5240/T5440

- In Resource Orchestrator, the following servers are referred to as SPARC M12.
  - SPARC M12-1/M12-2/M12-2S
- In Resource Orchestrator, the following servers are referred to as SPARC M10.
  - SPARC M10-1/M10-4/M10-4S
- Fujitsu SPARC M12 is the product name used for SPARC M12 when they are sold outside Japan.
- Fujitsu M10 is the product name used for SPARC M10 when they are sold outside Japan.
- In this manual, Fujitsu SPARC M12 is referred to as SPARC M12.
- In this manual, Fujitsu M10 is referred to as SPARC M10.
- In this manual, Fujitsu SPARC M12 and Fujitsu M10 are collectively referred to as SPARC M10/M12.
- In Resource Orchestrator, the following software is referred to as GLS.
  - PRIMECLUSTER GLS 4.4 or earlier
- In Resource Orchestrator, the following software is referred to as GDS.
  - PRIMECLUSTER GDS 4.4 or earlier
- References and character strings or values requiring emphasis are indicated using double quotes ( " ).
- GUI items are shown enclosed by 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.
- The ">" used in Windows is included in usage examples. When using Linux, read ">" as meaning "#".
- When using Resource Orchestrator on Windows 8 and Windows Server 2012, please note the following.  
When OS operations are explained in this manual, the examples assume OSs up to Windows 7 and Windows Server 2008. When using Resource Orchestrator on Windows 8 or Windows Server 2012, take explanations regarding the [Start] menu as indicating the [Apps] screen.  
The [Apps] screen can be displayed by right-clicking on the [Start] screen and then right-clicking [All apps].
- When using Resource Orchestrator on Windows 8.1 and Windows Server 2012 R2, please note the following.  
When OS operations are explained in this manual, the examples assume OSs up to Windows 7 and Windows Server 2008. When using Resource Orchestrator on Windows 8.1 or Windows Server 2012 R2, take explanations regarding the [Start] menu as indicating the [Apps] screen.  
The [Apps] screen can be displayed by swiping the [Start] screen from bottom to top, or clicking the downward facing arrow on the lower-left of the [Start] screen.

## 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.

## Regarding Installation Folder Paths

The installation folder path may be given as C:\Fujitsu\ROR in this manual.

Replace it as shown below.

[Virtual Edition]

- When using Windows 64-bit (x64)  
C:\Program Files (x86)\Resource Orchestrator
- When using Windows 32-bit (x86)  
C:\Program Files\Resource Orchestrator

[Cloud Edition]

C:\Program Files (x86)\Resource Orchestrator

## Command Examples

The paths used in command examples may be abbreviated. When using commands, execute them using the paths in the "Name" column in the "Reference Guide (Command) VE" and the "Reference Guide (Command/XML) CE".

## Abbreviations

The following abbreviations are use in this manual.

### Category

#### Abbreviation

- Products

### Windows

#### Windows

- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Essentials
- Microsoft(R) Windows Server(R) 2012 R2 Standard
- Microsoft(R) Windows Server(R) 2012 R2 Datacenter
- Microsoft(R) Windows Server(R) 2016 Standard
- Microsoft(R) Windows Server(R) 2016 Datacenter
- Microsoft(R) Windows Server(R) 2019 Standard
- Microsoft(R) Windows Server(R) 2019 Datacenter
- Windows(R) 7 Professional
- Windows(R) 7 Ultimate
- Windows(R) 8.1 Pro
- Windows(R) 8.1 Enterprise
- Windows(R) 10 Pro
- Windows(R) 10 Enterprise

#### Windows Server 2012

- Microsoft(R) Windows Server(R) 2012 Standard
- Microsoft(R) Windows Server(R) 2012 Datacenter
- Microsoft(R) Windows Server(R) 2012 R2 Essentials
- Microsoft(R) Windows Server(R) 2012 R2 Standard

- Microsoft(R) Windows Server(R) 2012 R2 Datacenter

#### Windows Server 2016

- Microsoft(R) Windows Server(R) 2016 Standard
- Microsoft(R) Windows Server(R) 2016 Datacenter

#### Windows Server 2019

- Microsoft(R) Windows Server(R) 2019 Standard
- Microsoft(R) Windows Server(R) 2019 Datacenter

#### Windows PE

- Microsoft(R) Windows(R) Preinstallation Environment

#### Windows 7

- Windows(R) 7 Professional
- Windows(R) 7 Ultimate

#### Windows 8.1

- Windows(R) 8.1 Pro
- Windows(R) 8.1 Enterprise

#### Windows 10

- Windows(R) 10 Pro
- Windows(R) 10 Enterprise

#### DOS

- Microsoft(R) MS-DOS(R) operating system, DR DOS(R)

#### MSFC

- Microsoft(R) Windows Server(R) 2012 Standard Failover Cluster
- Microsoft(R) Windows Server(R) 2012 Datacenter Failover Cluster

#### SCVMM

- Microsoft(R) System Center 2012 Virtual Machine Manager
- Microsoft(R) System Center 2012 R2 Virtual Machine Manager
- Microsoft(R) System Center 2016 Virtual Machine Manager

#### Linux

##### Linux

- Red Hat(R) Enterprise Linux(R) 6.0 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.0 (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(R) Enterprise Linux(R) 6.3 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.4 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.5 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.6 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.6 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.7 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.7 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.8 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.8 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.9 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.9 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.10 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.10 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.0 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.1 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.2 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.4 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.5 (for Intel64)
- SUSE(R) Linux Enterprise Server 10 Service Pack 2 for x86
- SUSE(R) Linux Enterprise Server 10 Service Pack 2 for AMD64 & Intel64
- SUSE(R) Linux Enterprise Server 10 Service Pack 3 for x86
- SUSE(R) Linux Enterprise Server 10 Service Pack 3 for AMD64 & Intel64
- SUSE(R) Linux Enterprise Server 11 for x86
- SUSE(R) Linux Enterprise Server 11 for AMD64 & Intel64
- SUSE(R) Linux Enterprise Server 11 Service Pack 1 for x86
- SUSE(R) Linux Enterprise Server 11 Service Pack 1 for AMD64 & Intel64
- Oracle Enterprise Linux Release 6.7 for x86 (32-bit)
- Oracle Enterprise Linux Release 6.7 for x86\_64 (64-bit)
- Oracle Enterprise Linux Release 7.2 for x86 (32-bit)
- Oracle Enterprise Linux Release 7.2 for x86\_64 (64-bit)

#### Red Hat Enterprise Linux

- Red Hat(R) Enterprise Linux(R) 6.0 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.0 (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(R) Enterprise Linux(R) 6.3 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.4 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.5 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.6 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.6 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.7 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.7 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.8 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.8 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.9 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.9 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.10 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.10 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.0 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.1 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.2 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.4 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.5 (for Intel64)

#### Red Hat Enterprise Linux 6

- Red Hat(R) Enterprise Linux(R) 6.0 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.0 (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(R) Enterprise Linux(R) 6.3 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.4 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.5 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.6 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.6 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.7 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.7 (for Intel64)

- Red Hat(R) Enterprise Linux(R) 6.8 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.8 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.9 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.9 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 6.10 (for x86)
- Red Hat(R) Enterprise Linux(R) 6.10 (for Intel64)

#### Red Hat Enterprise Linux 7

- Red Hat(R) Enterprise Linux(R) 7.0 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.1 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.2 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.4 (for Intel64)
- Red Hat(R) Enterprise Linux(R) 7.5 (for Intel64)

#### SUSE Linux Enterprise Server

- SUSE(R) Linux Enterprise Server 10 Service Pack 2 for x86
- SUSE(R) Linux Enterprise Server 10 Service Pack 2 for AMD64 & Intel64
- SUSE(R) Linux Enterprise Server 10 Service Pack 3 for x86
- SUSE(R) Linux Enterprise Server 10 Service Pack 3 for AMD64 & Intel64
- SUSE(R) Linux Enterprise Server 11 for x86
- SUSE(R) Linux Enterprise Server 11 for AMD64 & Intel64
- SUSE(R) Linux Enterprise Server 11 Service Pack 1 for x86
- SUSE(R) Linux Enterprise Server 11 Service Pack 1 for AMD64 & Intel64

#### Oracle Enterprise Linux

- Oracle Enterprise Linux Release 6.7 for x86 (32-bit)
- Oracle Enterprise Linux Release 6.7 for x86\_64 (64-bit)
- Oracle Enterprise Linux Release 7.2 for x86 (32-bit)
- Oracle Enterprise Linux Release 7.2 for x86\_64 (64-bit)

## KVM

### 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
- Red Hat(R) Enterprise Linux(R) 6.3 (for x86) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.4 (for x86) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.5 (for x86) Virtual Machine Function

- Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.6 (for x86) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.6 (for Intel64) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.7 (for x86) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.7 (for Intel64) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.8 (for x86) Virtual Machine Function
- Red Hat(R) Enterprise Linux(R) 6.8 (for Intel64) Virtual Machine Function

## Xen

### Xen

- Citrix XenServer(R) 5.5
- Citrix Essentials(TM) for XenServer 5.5, Enterprise Edition
- Citrix XenServer(R) 6.0
- Citrix Essentials(TM) for XenServer 6.0, Enterprise Edition

## Citrix

### Citrix XenServer

- Citrix XenServer(R) 6.0
- Citrix XenServer(R) 6.0.2
- Citrix XenServer(R) 6.1.0
- Citrix XenServer(R) 6.2.0
- Citrix XenServer(R) 7.1 LTSR
- Citrix XenServer(R) 7.2
- Citrix Hypervisor(R)

### XenServer 6

- Citrix XenServer(R) 6.0
- Citrix Essentials(TM) for XenServer 6.0, Enterprise Edition

### Citrix XenApp

- Citrix XenApp(R)
- Citrix Virtual Apps(R)

### Citrix XenDesktop

- Citrix XenDesktop(R)
- Citrix Virtual Apps and Desktops(R)

## Oracle Solaris

### Solaris

- Oracle Solaris 10 05/09 (Update7)
- Oracle Solaris 11 11/11
- Oracle Solaris 11.1

- Oracle Solaris 11.2
- Oracle Solaris 11.3

## Oracle VM

### OVM for x86 2.2

- Oracle(R) VM Server for x86 2.2

### OVM for x86 3.x

#### OVM for x86 3.2

- Oracle VM Server for x86 v3.2.x

#### OVM for x86 3.3

- Oracle VM Server for x86 v3.3.x

### OVM for SPARC

- Oracle(R) VM Server for SPARC

### Oracle VM Manager

- Oracle(R) VM Manager

## EMC

### Navisphere

- EMC Navisphere Manager

### Solutions Enabler

- EMC Solutions Enabler

## VMware

### VMware vSphere or vSphere

- VMware vSphere(R) 4
- VMware vSphere(R) 4.1
- VMware vSphere(R) 5
- VMware vSphere(R) 5.1
- VMware vSphere(R) 5.5
- VMware vSphere(R) 6
- VMware vSphere(R) 6.5
- VMware vSphere(R) 6.7

### VMware ESX

- VMware(R) ESX(R)

### VMware ESX 4

- VMware(R) ESX(R) 4

### VMware ESXi

- VMware(R) ESXi(TM)

### VMware ESXi 5.0

- VMware(R) ESXi(TM) 5.0

#### VMware ESXi 5.1

- VMware(R) ESXi(TM) 5.1

#### VMware ESXi 5.5

- VMware(R) ESXi(TM) 5.5

#### VMware ESXi 6.0

- VMware(R) ESXi(TM) 6.0

#### VMware ESXi 6.5

- VMware(R) ESXi(TM) 6.5

#### VMware ESXi 6.7

- VMware(R) ESXi(TM) 6.7

#### VMware Infrastructure Client

- VMware(R) Infrastructure Client

#### VMware Tools

- VMware(R) Tools

#### VMware vSphere 4.0 or vSphere 4.0

- VMware vSphere(R) 4.0

#### VMware vSphere 4.1 or vSphere 4.1

- VMware vSphere(R) 4.1

#### VMware vSphere 5 or vSphere 5

- VMware vSphere(R) 5

#### VMware vSphere 5.1 or vSphere 5.1

- VMware vSphere(R) 5.1

#### VMware vSphere 5.5 or vSphere 5.5

- VMware vSphere(R) 5.5

#### VMware vSphere 6.0 or vSphere 6.0

- VMware vSphere(R) 6.0

#### VMware vSphere 6.5 or vSphere 6.5

- VMware vSphere(R) 6.5

#### VMware vSphere 6.7 or vSphere 6.7

- VMware vSphere(R) 6.7

#### VMware vSphere Client or vSphere Client

- VMware vSphere(R) Client

#### VMware vCenter Server or vCenter Server

- VMware(R) vCenter(TM) Server

#### VMware vCenter Server Appliance or vCenter Server Appliance

- VMware(R) vCenter(TM) Server Appliance(TM)

#### VMware vClient

- VMware(R) vClient(TM)

#### VMware FT

- VMware(R) Fault Tolerance

#### VMware DRS

- VMware(R) Distributed Resource Scheduler

#### VMware DPM

- VMware(R) Distributed Power Management

#### VMware Storage VMotion

- VMware(R) Storage VMotion

#### VMware vDS

- VMware(R) vNetwork Distributed Switch

#### VMware Horizon View

- VMware Horizon View 5.2.x
- VMware Horizon View 5.3.x
- VMware Horizon 6.0 (with View)

#### VMware VSAN or vSAN

- VMware(R) Virtual SAN(TM)

#### VMware vSphere Web Client or vSphere Web Client

- VMware vSphere(R) Web Client

#### VMware NSX

- VMware NSX(R)
- VMware NSX(R) for vSphere(R)
- VMware NSX(R) for vSphere(R) 6.3

#### VMware NSX Controller or NSX Controller

- VMware NSX(R) Controller(TM)

#### VMware NSX Edge or NSX Edge

- VMware NSX(R) Edge(TM)

#### VMware NSX Manager or NSX Manager

- VMware NSX(R) Manager(TM)

### Excel

#### Excel

- Microsoft(R) Office Excel(R) 2007
- Microsoft(R) Office Excel(R) 2010
- Microsoft(R) Office Excel(R) 2013

#### Excel 2007

- Microsoft(R) Office Excel(R) 2007

#### Excel 2010

- Microsoft(R) Office Excel(R) 2010

#### Excel 2013

- Microsoft(R) Office Excel(R) 2013

### Browsers

#### Internet Explorer

- Windows(R) Internet Explorer(R) 9
- Internet Explorer(R) 10
- Internet Explorer(R) 11

#### Firefox

- Firefox(R)

### Antivirus Software

#### OfficeScan

- Trend Micro OfficeScan

#### McAfee ePolicy Orchestrator

- McAfee(R) ePolicy Orchestrator(R)

#### McAfee ePO

- McAfee(R) ePolicy Orchestrator(R)

#### McAfee Agent

- McAfee(R) Agent

#### McAfee Endpoint Security

- McAfee(R) Endpoint Security

#### Symantec Endpoint Protection

- Symantec(TM) Endpoint Protection

#### Symantec Endpoint Protection Manager

- Symantec(TM) Endpoint Protection Manager

### BMC

#### BladeLogic

- BMC BladeLogic Server Automation

### ETERNUS

#### ESC

- ETERNUS SF Storage Cruiser

### ServerView

#### ServerView Agent

- ServerView SNMP Agents for MS Windows (32-bit and 64-bit)

- ServerView Agents Linux
- ServerView Agents VMware for VMware ESX Server

#### VIOM

- ServerView Virtual-IO Manager

#### ISM

- ServerView Infrastructure Manager
- Infrastructure Manager

#### SVOM

- ServerView Operations Manager

#### SVFAB

- ServerView Fabric Manager

#### RCVE

- ServerView Resource Coordinator VE

#### ROR

- FUJITSU Software ServerView Resource Orchestrator

#### ROR VE

- FUJITSU Software ServerView Resource Orchestrator Virtual Edition

#### ROR CE

- FUJITSU Software ServerView Resource Orchestrator Cloud Edition

#### Resource Coordinator

- Systemwalker Resource Coordinator
- Systemwalker Resource Coordinator Virtual server Edition

#### Resource Coordinator VE

- ServerView Resource Coordinator VE
- Systemwalker Resource Coordinator Virtual server Edition

#### Resource Orchestrator

- FUJITSU Software ServerView Resource Orchestrator

## Export Administration Regulation Declaration

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

## Trademark Information

- BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries.
- Citrix, Citrix Virtual Apps and Desktops, Citrix Virtual Apps, Citrix Hypervisor, XenApp, XenDesktop, XenServer, Citrix Essentials 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(R) is a trademark or registered trademark of Linus Torvalds in the United States and other countries.
- McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the United States and other countries.
- Microsoft, Windows, MS-DOS, Windows Server, Windows Vista, Excel, Active Directory, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- Firefox is a trademark or registered trademark of the Mozilla Foundation in the United States and other countries.
- Oracle and Java are registered trademarks of Oracle 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 and the SUSE logo are trademarks of SUSE IP Development Limited or its subsidiaries or affiliates.
- Symantec and the Symantec logo are trademarks or registered trademarks of the Symantec Corporation or its subsidiaries in the United States and other countries.
- TREND MICRO and OfficeScan are registered trademarks of Trend Micro, Inc.
- 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.

## Revision History

Month/Year Issued, Edition	Manual Code
November 2011, First Edition	J2X1-7605-01ENZ0(00)
December 2011, Edition 1.1	J2X1-7605-01ENZ0(01)
January 2012, Edition 1.2	J2X1-7605-01ENZ0(02)
February 2012, Edition 1.3	J2X1-7605-01ENZ0(03)
March 2012, Edition 1.4	J2X1-7605-01ENZ0(04)
April 2012, Edition 1.5	J2X1-7605-01ENZ0(05)
July 2012, Second Edition	J2X1-7605-02ENZ0(00)
October 2012, Third Edition	J2X1-7605-03ENZ0(00)
December 2012, Fourth Edition	J2X1-7605-04ENZ0(00)
January 2013, Fifth Edition	J2X1-7605-05ENZ0(00)
January 2013, Edition 5.1	J2X1-7605-05ENZ0(01)
January 2013, Edition 5.2	J2X1-7605-05ENZ0(02)
March 2013, Edition 5.3	J2X1-7605-05ENZ0(03)

Month/Year Issued, Edition	Manual Code
June 2013, Edition 5.4	J2X1-7605-05ENZ0(04)
August 2013, Edition 5.5	J2X1-7605-05ENZ0(05)
December 2013, Sixth Edition	J2X1-7605-06ENZ0(00)
February 2014, Edition 6.1	J2X1-7605-06ENZ0(01)
April 2014, Edition 6.2	J2X1-7605-06ENZ0(02)
June 2014, Edition 6.3	J2X1-7605-06ENZ0(03)
April 2015, Seventh Edition	J2X1-7605-07ENZ0(00)
July 2015, Edition 7.1	J2X1-7605-07ENZ0(01)
September 2015, Edition 7.2	J2X1-7605-07ENZ0(02)
December 2015, Edition 7.3	J2X1-7605-07ENZ0(03)
January 2016, Edition 7.4	J2X1-7605-07ENZ0(04)
June 2016, Edition 7.5	J2X1-7605-07ENZ0(05)
September 2016, Edition 7.6	J2X1-7605-07ENZ0(06)
December 2016, Edition 7.7	J2X1-7605-07ENZ0(07)
February 2017, Edition 7.8	J2X1-7605-07ENZ0(08)
April 2017, Eighth Edition	J2X1-7605-08ENZ0(00)
May 2017, Edition 8.1	J2X1-7605-08ENZ0(01)
August 2017, Edition 8.2	J2X1-7605-08ENZ0(02)
September 2017, Edition 8.3	J2X1-7605-08ENZ0(03)
December 2017, Edition 8.4	J2X1-7605-08ENZ0(04)
February 2018, Edition 8.5	J2X1-7605-08ENZ0(05)
March 2018, Edition 8.6	J2X1-7605-08ENZ0(06)
October 2018, Ninth Edition	J2X1-7605-09ENZ0(00)
December 2018, Edition 9.1	J2X1-7605-09ENZ0(01)
December 2018, Edition 9.2	J2X1-7605-09ENZ0(02)
October 2020, Edition 9.3	J2X1-7605-09ENZ0(03)

## Copyright

Copyright 2011-2020 FUJITSU LIMITED

# Contents

---

Part 1 Overview.....	1
Chapter 1 Overview of Operations, Maintenance, and Monitoring.....	2
Part 2 Operation.....	3
Chapter 2 Starting and Stopping Managers and Agents.....	4
2.1 Starting and Stopping Managers.....	4
2.2 Starting and Stopping Agents.....	6
Chapter 3 Managing User Accounts.....	8
Chapter 4 Server Switchover.....	9
4.1 Overview.....	9
4.2 Switchover.....	9
4.3 Post-Switchover Operations.....	12
4.3.1 Operations after Server Switchover.....	12
4.3.2 Recovery of OVM for SPARC Environments.....	14
Chapter 5 Event Handling.....	16
Part 3 Maintenance.....	20
Chapter 6 Hardware Maintenance.....	21
6.1 Overview.....	21
6.2 Blade Server Maintenance.....	22
6.2.1 Maintenance LED.....	22
6.2.2 Reconfiguration of Hardware Properties.....	23
6.2.3 Replacing Servers.....	25
6.2.4 Replacing Server Components.....	27
6.2.5 Replacing Non-server Hardware.....	28
6.3 Maintenance for Servers Other Than Blade Servers.....	30
6.3.1 Reconfiguration of Hardware Properties.....	30
6.3.2 Replacing Servers.....	32
6.3.3 Replacing and Adding Server Components.....	37
6.3.4 Replacing Non-server Hardware and Upgrading Firmware.....	39
6.4 Network Device Maintenance.....	40
6.4.1 Common Maintenance Procedure of Network Devices.....	40
6.4.1.1 When the Network Device to Replace Has Failed.....	41
6.4.1.2 When the Network Device to Replace Has Not Failed.....	42
6.4.1.3 Regular Maintenance Procedure of Network Devices.....	42
6.4.1.4 Procedure for Addition or Modification of Connection Destinations of Network Devices.....	43
6.4.2 Maintenance Procedures of Network Devices (Firewalls, Server Load Balancers, and L2 Switches).....	44
6.4.2.1 Adding L2 Switches to Handle Insufficient Numbers of Ports when Adding Servers.....	44
6.4.3 Maintenance Procedures of Network Devices (Ethernet Fabrics).....	46
6.4.3.1 Adding Switches to an Ethernet Fabric to Handle Insufficient Numbers of Ports when Adding Servers.....	46
6.4.3.2 Migrating an Ethernet Fabric (Converged Fabric) to a Multiple VFAB Environment.....	48
6.4.3.3 Reflecting a Modified Domain Switch Configuration on the Ethernet Fabric.....	48
6.5 Storage Device Maintenance.....	49
6.6 Power Monitoring Device (PDU or UPS) Maintenance.....	49
Chapter 7 Maintaining Software with Cloning [Physical Servers].....	51
7.1 Overview.....	51
7.2 Software Maintenance Procedure.....	51
Chapter 8 Backup and Restoration of Managed Servers.....	53
Chapter 9 Backup and Restoration of Admin Servers.....	54

9.1 Overview.....	54
9.1.1 Resources Managed by This Product and Timing of Update.....	54
9.1.2 Backup.....	55
9.1.3 Restore.....	55
9.1.4 Backup and Restore Commands.....	56
9.2 Backup.....	56
9.2.1 Backing Up All Management Information.....	58
9.2.2 Backing Up Configuration Definition Information.....	60
9.3 Restoration.....	61
<b>Chapter 10 Backing Up and Restoring Image Files.....</b>	<b>65</b>
10.1 Configuration of Folders and Files.....	65
10.2 Backing Up Image Files.....	66
10.3 Restoring Image Files.....	66
<b>Part 4 Monitoring.....</b>	<b>68</b>
<b>Chapter 11 Monitoring Resources.....</b>	<b>69</b>
11.1 Overview.....	69
11.2 Resource Status.....	70
11.3 Addressing Resource Failures.....	73
<b>Chapter 12 Collecting Power Consumption Data and Displaying Graphs.....</b>	<b>75</b>
12.1 Overview.....	75
12.2 Exporting Power Consumption Data.....	75
12.3 Power Consumption Data File (CSV Format).....	75
12.4 Displaying Power Consumption Data Graphs.....	76
<b>Part 5 Modifying.....</b>	<b>77</b>
<b>Chapter 13 Changing Settings.....</b>	<b>78</b>
13.1 When Configuring Single Sign-On.....	78
13.1.1 Reconfiguration Procedure.....	78
13.1.1.1 Confirming Certificates.....	78
13.1.1.2 Registering Certificates.....	78
13.1.1.3 Checking Directory Service Connection Information.....	79
13.1.2 Modifying Directory Service Connection Information.....	79
13.1.3 When Certificates Have Expired.....	80
<b>Appendix A Notes on Operating ServerView Resource Orchestrator.....</b>	<b>81</b>

# Part 1 Overview

---

---

Chapter 1 Overview of Operations, Maintenance, and Monitoring.....	2
--	---

# **Chapter 1 Overview of Operations, Maintenance, and Monitoring**

This chapter provides an overview of operation, maintenance, and monitoring of Resource Orchestrator.

For additional information on the operation, maintenance, and monitoring of this product, refer to the configuration information in the "Setup Guide VE".

# Part 2 Operation

---

---

Chapter 2 Starting and Stopping Managers and Agents.....	4
Chapter 3 Managing User Accounts.....	8
Chapter 4 Server Switchover.....	9
Chapter 5 Event Handling.....	16

## Chapter 2 Starting and Stopping Managers and Agents

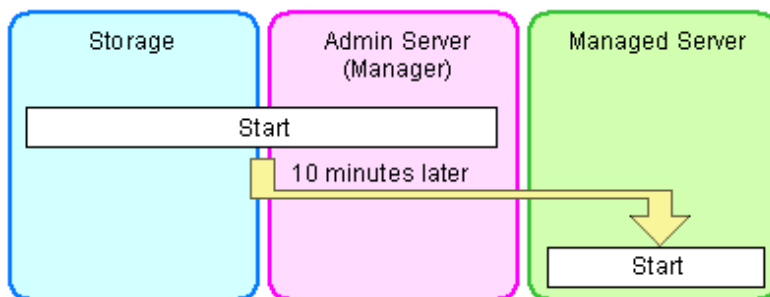
This chapter explains how to manually start or stop managers and agents.

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 "2.1 Starting and Stopping Managers" and "2.2 Starting and Stopping Agents".

### Note

When using HBA address rename, ensure managed servers are started after starting the manager. 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. The managed server does not start, if managed servers are started before the manager is. Make sure that the manager is running before starting managed servers.



When using HBA address rename, start the HBA address rename setting service, and always keep the power on. For details on starting, stopping, and confirming the state of the HBA address rename setup service, refer to "6.1 Settings for the HBA address rename Setup Service" in the "Setup Guide VE".

## 2.1 Starting and Stopping Managers

The Resource Orchestrator manager starts automatically on the admin server.

This section explains how to manually start or stop the manager and how to check its running state.

[Windows Manager]

The manager is made up of the following two groups of Windows services:

- Manager Services

- Resource Coordinator Manager
- Resource Coordinator Task Manager
- Resource Coordinator Web Server (Apache)
- Resource Coordinator Sub Web Server (Mongrel)
- Resource Coordinator Sub Web Server (Mongrel2)
- Resource Coordinator DB Server (PostgreSQL)

- Related Services

- Deployment Service
- TFTP Service
- PXE Services
- DHCP Server (\*)

\* Note: Required when managed servers belonging to different subnets from the admin server exist.

From the Windows Control Panel, open [Administrative Tools]. Then, open the [Services] window to check the state of each service.



Services are started and stopped using the rcxadm mgrctl command (start and stop subcommands).

Using this command, manager services and related services can be started or stopped at the same time.

For details on the command, refer to "5.11 rcxadm mgrctl" in the "Reference Guide (Command) VE".

To start or stop a manager in a clustered configuration, right-click the manager application shown under the failover cluster manager tree, and select either [Bring this service or application online] or [Take this service or application offline].

[Linux Manager]

The manager is made up of the following two groups of Linux services:

- Manager Services

rcvmr

Manager services also include the following daemons.

rcxmanager

rcxtaskmgr

rcxmongrel1

rcxmongrel2

rcxhttpd

- Database (PostgreSQL)

rcxdb

- Related Services

scwdepsvd

scwpxesvd

scwftpd

dhcpcd (\*)

\* Note: Required when managed servers belonging to different subnets from the admin server exist.

The status of each of those services can be confirmed from the service command, as shown below.

```
# service rcvmr status <RETURN>
# service scwdepsvd status <RETURN>
# service scwpxesvd status <RETURN>
# service scwftpd status <RETURN>
# service dhcpcd status <RETURN>
```

Services are started and stopped using the rcxadm mgrctl command (start and stop subcommands).

Using this command, manager services and related services can be started or stopped at the same time.

For details on the command, refer to "5.11 rcxadm mgrctl" in the "Reference Guide (Command) VE".

To start or stop a manager in a clustered configuration, use the cluster administration view (Cluster Admin).

For details, refer to the PRIMECLUSTER manual.

 Note

- When using ServerView Deployment Manager on an admin LAN, all services related to Resource Orchestrator will be automatically disabled. To prevent conflicts with ServerView Deployment Manager, do not start these services in order. For details, refer to "B.2 Co-Existence with ServerView Deployment Manager" in the "Setup Guide VE".
- Resource Orchestrator cannot be operated if any of the manager services are stopped. Ensure that all services are running when Resource Orchestrator is running.

- If the manager is unable to communicate on the admin LAN when started up (because of LAN cable disconnections or any other causes), PXE Services may not start automatically. If PXE Services are stopped, investigate the network interface used for the admin LAN and confirm whether it can communicate with other nodes on the admin LAN.

If the manager cannot communicate with admin LAN nodes, restore the admin LAN itself and restart the manager.

## 2.2 Starting and Stopping Agents

The Resource Orchestrator agent starts automatically on managed servers. This section explains how to manually start or stop an agent and how to check its power state.



### Note

To prevent conflicts, related services are uninstalled from the Resource Orchestrator agent when using ServerView Deployment Manager on the admin LAN. In such cases, there is no need to start or stop those services when starting or stopping the Resource Orchestrator agent.

[Windows] [Hyper-V]

The agent consists of the following two Windows services:

- Agent Service
  - Resource Coordinator Agent
- Related Services
  - Deployment Agent

From the Windows Control Panel, open [Administrative Tools]. Then, open the [Services] window to check the state of each service. The following explains how to start and stop each service.

- Agent Service
  - Agents can be started and stopped using the start and stop subcommands of the `rcxadm agtctl` command. For details of the command, refer to "5.2 `rcxadm agtctl`" in the "Reference Guide (Command) VE".

- Related Services

From the Windows Control Panel, open [Administrative Tools]. Then, open the [Services] window to stop or start the following service.

- Deployment Agent

[Linux] [VMware] [Xen] [KVM]

The agent consists of the following services.

- Agent Service
- Related Services
  - Deployment Agent

For VMware vSphere 4.0 or later version, Deployment Agent is not automatically started, as backup and restore, and cloning functions cannot be used. It is not necessary to start up.

Execute the following commands to determine whether the agent is running or not. If those commands show that the processes for the agent and deployment services are running, then the agent can be asserted to be running.

- Agent Service

```
# /bin/ps -ef | grep FJSVssagt <RETURN>
```

- Related Services

```
# /bin/ps -ef | grep scwagent <RETURN>
```

The following explains how to start and stop each service.

- Agent Service

Agents can be started and stopped using the start and stop subcommands of the `rcxadm agtctl` command. For details of the command, refer to "5.2 `rcxadm agtctl`" in the "Reference Guide (Command) VE".

- Related Services

Execute the following command to start or stop the collection of image files, deployment of image files, and server startup control.

- When using Red Hat Enterprise Linux 5 and Red Hat Enterprise Linux 6

**Start**

```
# /etc/init.d/scwagent start <RETURN>
```

**Stop**

```
# /etc/init.d/scwagent stop <RETURN>
```

- When using Red Hat Enterprise Linux 7

**Start**

```
# systemctl start scwagent.service <RETURN>
```

**Stop**

```
# systemctl stop scwagent.service <RETURN>
```

[Solaris] [Solaris Zones] [OVM for SPARC]

The agent consists of the following services.

- Agent Service

Execute the following commands to determine whether the agent is running or not. If those commands show that the processes for the agent and deployment services are running, then the agent can be asserted to be running.

```
# /bin/ps -ef | grep FJSVrcvat <RETURN>
```

The following explains how to start and stop each service.

Agents can be started and stopped using the start and stop subcommands of the `rcxadm agtctl` command.

For details of the command, refer to "5.2 `rcxadm agtctl`" in the "Reference Guide (Command) VE".

## Chapter 3 Managing User Accounts

This chapter explains the management of user accounts.

Managing users of Resource Orchestrator prevents operational errors by end users' and enables stable operation of systems.

For details on user accounts, refer to "Chapter 5 Defining User Accounts" in the "Design Guide VE".

For the functions available for user accounts of Resource Orchestrator, refer to "A.2.1 List of Menus" in the "User's Guide VE".

# Chapter 4 Server Switchover

This chapter explains how to use the server switchover function.

## 4.1 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 18 Settings for Server Switchover" in the "User's Guide VE".

When performing server switchover or failback using the backup and restore method, it is necessary to create a Windows PE in advance. For details, refer to the "Windows PE Creation Script Guide".



- 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.

- When the switchover method is storage affinity

- If switchover to spare servers is performed, the storage settings of the spare servers will be deleted. Perform restoration referring to "[4.3 Post-Switchover Operations](#)".

- After switchover to spare servers is performed, even if failback is performed the storage settings for the spare servers are not automatically restored.

Restore the zoning and host affinity settings for storage units of spare servers following the procedure listed in the "Information" in "[4.3 Post-Switchover Operations](#)".

## 4.2 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 "[4.3 Post-Switchover Operations](#)".

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

For details, refer to the "Functions Available for Agents" in "6.2.1 All Editions" in the "Overview".



- 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 or failback of a server, if the source and destination servers are both running at the same time, there is a risk that the OSs of those servers may be damaged.

To prevent this, shut down the switchover source or failback source server, and then confirm that the relevant server has been powered off. For each of these operations, the following server management units must be running:

- For server switchover
  - The server management unit of the switchover destination server
  - The server management unit of the switchover source server
- For server failback
  - The server management unit of the failback destination server
  - The server management unit of the failback source server
- During switchover, server restarts and configuration changes may trigger SNMP Traps (which are shown in the Event Log). For details, refer to "Part 1 Messages Displayed by Virtual Edition and Cloud Edition" in "Messages".
- 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.
- After shutting down a spare server, if the power is not turned off within 15 minutes, the spare server will be forcibly powered off.
- When performing server switchover using the backup and restore method in a SAN data server environment that uses local boot, configure a target disk for image operations on both the primary server and the spare server.
 

If the switchover is performed without configuring the target disk for image operations, data may be overwritten on an unintended disk. For details, refer to "9.1.13 Changing Target Disks of Image Operations" in the "User's Guide VE".
- If switchover or failback of a server fails, a message is displayed, and then the automatic recovery process (rollback) is performed automatically. In this case, wait a few minutes and then perform the failed operation again, targeting the relevant server.

#### [VMware] [Hyper-V]

- 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.

#### [OVM for SPARC]

- In OVM for SPARC environments, the XML files of the OVM configuration information used during server switchover are saved in the following location. Delete them if necessary.

##### Placeholder for the File

[Control domain]  
/etc/opt/FJSVrcvat/config

##### File name

ovm\_config`year_month_minute_second`.xml

The `year_month_minute_second` at the end of the file name is UTC.

- Before performing server switchover, if the XML file of the domain configuration information has not been saved in the control domain, the domain configuration cannot be recovered after server switchover. In this case, it will be necessary to reconfigure the domain configuration.

This is also true for the spare server that is being used as OVM for SPARC.

For details on how to save the XML files of the OVM configuration information, refer to "18.5.4 XML File of OVM Configuration Information" in the "User's Guide VE".

---

## Auto-Recovery

- For PRIMERGY BX servers

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 servers, tower servers, SPARC Enterprise, and SPARC M10/M12

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 "9.4 Conditions Required for Auto-Recovery" in the "Setup 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 performed either 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 "9.3 Server Switchover Conditions" in the "Setup 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 the [OK] button.

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 the [Cancel] button 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 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
- 

## 4.3 Post-Switchover Operations

---

### 4.3.1 Operations after Server Switchover

---

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 6 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 "ETERNUS SF Storage Cruiser Operation 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".

For details on the recovery of spare servers when using an OVM for SPARC environment as a spare server, refer to "[4.3.2 Recovery of OVM for SPARC Environments](#)".

- 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.

For details on the recovery of spare servers when using an OVM for SPARC environment as a spare server, refer to "[4.3.2 Recovery of OVM for SPARC Environments](#)".



---

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 Operation 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 "9.3 Server Switchover Conditions" in the "Setup 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 the [OK] button.

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 the [Cancel] button 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 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.

### When using backup and restore for the server switchover method

- Do not start up the original spare server during or after a 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 it is necessary to transfer newly generated data from the spare server to the primary server, back up the spare server before performing failback.  
Refer to "Backing Up a System Image" in "16.2 Backup" in the "User's Guide VE", 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 a hard disk is replaced in a failed server, configure the target disks of image operations again.  
If the switchover is performed without configuring the target disk for image operations, data may be overwritten on an unintended

disk.

For details, refer to "9.1.13 Changing Target Disks of Image Operations" in the "User's Guide VE".

## 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 the [OK] button.

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 (\*)

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)

\* Note: 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.

## 4.3.2 Recovery of OVM for SPARC Environments

When using an OVM for SPARC environment as a spare server, use the following procedure to perform recovery.

1. Configure the same domain configuration as the factory default. Execute the following Resource Orchestrator command on XSCF.

```
XSCF> setdomainconfig -p 0 -c default <RETURN>
```

2. Configure "true" for "auto boot" in the domain control, and "disk" for "boot-device".

```
XSCF> setpparam -y -p 0 -s bootscript 'setenv auto-boot? true <RETURN>
setenv boot-device Disk name' <RETURN>
```

3. Configure "off" for Autoboot (Guest Domain) of the physical partition operation mode on XSCF.

```
XSCF> setpparmode -p 0 -m guestboot=off <RETURN>
```

4. 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.
5. Use the `storageadm zone info` command to confirm the zoning and host affinity configurations.
6. 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 Operation Guide".
7. Start the OS of the control domain.
8. When using the ZFS storage pool in the control domain, import it.

When "18.5.2 ZFS Storage Pool Definition Files [Solaris] [Solaris Zones] [OVM for SPARC]" in the "User's Guide VE" has already been configured using the spare server of the control domain, it is not necessary to automatically import it.

- a. Check the status of the ZFS storage pool.

```
primary# zpool list <RETURN>
```

- b. Import the target ZFS storage pool.

```
primary# zpool import ZFS storage pool name <RETURN>
```

9. Restore all domain configurations on the system from the XML files of the domain configuration saved before server switchover.

```
primary# ldm init-system -r -i XML domain configuration information <RETURN>
```

10. Configure the physical I/O device allocated to the control domain and the IO domain.

The physical I/O device may be configured in both the control domain and the IO domain in the OVM specifications. Reconfigure the allocation of the physical I/O device.

11. Configure the port number used for the console of the domain.

The port number of the console configured in the guest domain may be invalid in the OVM specifications. Configure the port number used for the console of the domain.

12. When an IO domain is used, the IO domain starts before startup of the guest domain.

13. When using the ZFS storage pool in the guest domain, import it.

When "18.5.2 ZFS Storage Pool Definition Files [Solaris] [Solaris Zones] [OVM for SPARC]" in the "User's Guide VE" has already been configured using the spare server of the guest domain, it is not necessary to automatically import it.

- a. Log in to the guest domain.
- b. Check the status of the ZFS storage pool.

```
# zpool list <RETURN>
```

- c. Import the target ZFS storage pool.

```
# zpool import ZFS storage pool name <RETURN>
```

14. When using the guest domain as a Solaris Zone, restore the non-global zone.

- a. Check the status of the non-global zone.

```
# zoneadm list -vc <RETURN>
```

- b. If necessary, execute "attach" and "boot" to start the non-global zones.

15. Save the configuration information for the service processor. Saving is not possible when configuration information with the same name has already been saved in the service processor.

```
# ldm add-spconfig Configuration information name <RETURN>
```

## Chapter 5 Event Handling

This chapter 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 Manager]

*Installation\_folder*\SVROR\Manager\etc\trapop.bat Argument 1 Argument 2 Argument 3 Argument 4 Argument 5 Argument 6

[Linux Manager]

/etc/opt/FJSVrcvnr/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 Manager]

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\SVROR\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 Manager]

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/FJSVrcvnr/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.  
.....

# Part 3 Maintenance

---

---

Chapter 6 Hardware Maintenance.....	21
Chapter 7 Maintaining Software with Cloning [Physical Servers].....	51
Chapter 8 Backup and Restoration of Managed Servers.....	53
Chapter 9 Backup and Restoration of Admin Servers.....	54
Chapter 10 Backing Up and Restoring Image Files.....	65



# Chapter 6 Hardware Maintenance

This chapter explains how to perform hardware maintenance.

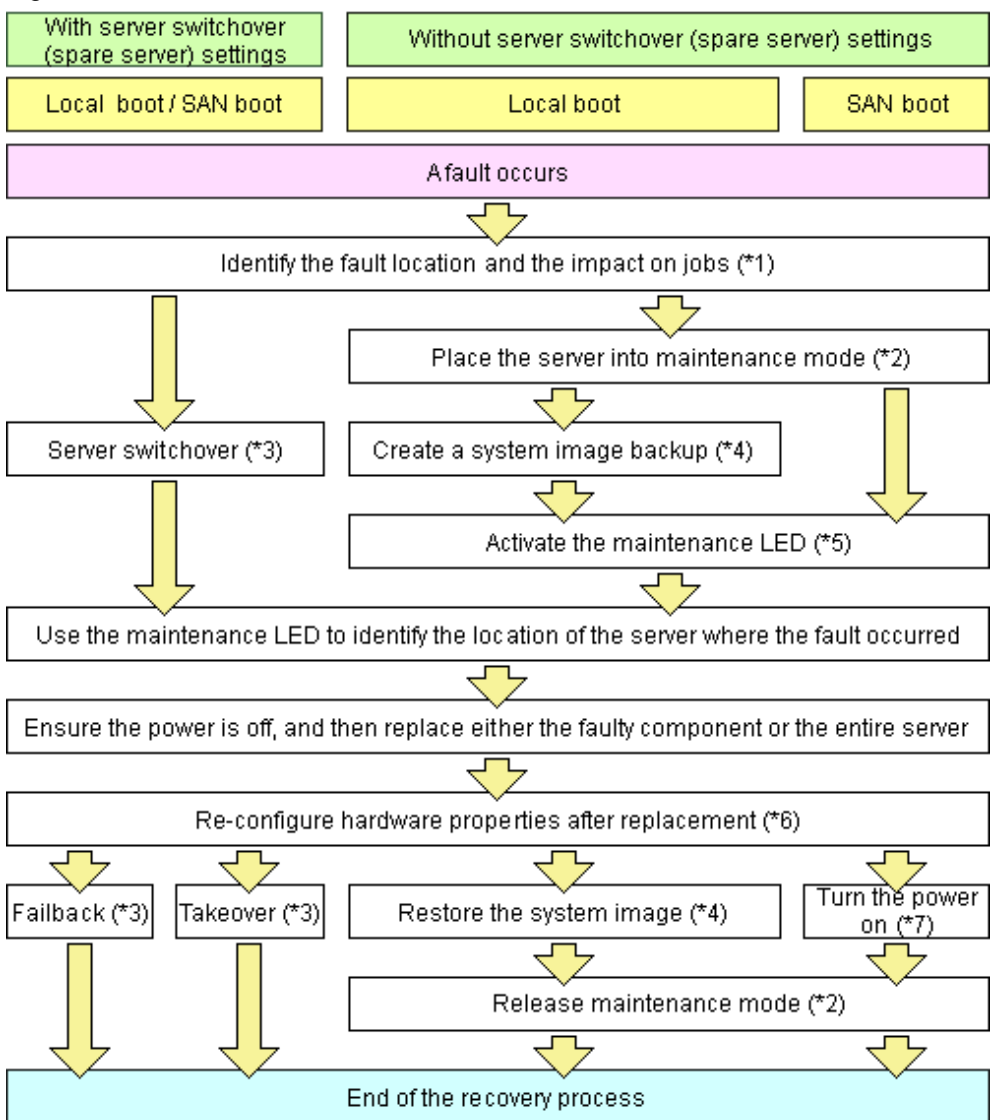
## 6.1 Overview

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

### Flow of Hardware Maintenance when a Server Fails

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

Figure 6.1 Flow of Hardware Maintenance when a Server Fails



\*1: For details on how to identify failures, refer to "11.3 Addressing Resource Failures".

\*2: For details on how to configure and release maintenance mode, refer to "Appendix C Maintenance Mode" in the "User's Guide VE".

\*3: For details on server switchover, failback, and takeover, refer to "Chapter 4 Server Switchover".

\*4: For details on backing up and restoring system images, refer to "Chapter 16 Backup and Restore" in the "User's Guide VE".

\*5: For details on maintenance LED operations, refer to "6.2.1 Maintenance LED". Note that maintenance LED operations are only supported for PRIMERGY BX servers.

\*6: For details on reconfiguring hardware properties, refer to the following sections:

- For blade servers: Refer to "6.2.3 Replacing Servers".

- For servers other than blade servers: Refer to "[6.3.2 Replacing Servers](#)".

\*7: For details on power control, refer to "Chapter 14 Power Control" in the "User's Guide VE".

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 the following sections:

- For blade servers: Refer to "[6.2.3 Replacing Servers](#)".
- For servers other than blade servers: Refer to "[6.3.2 Replacing Servers](#)".

- Replacing Server Components

Replace hardware components (such as a NIC, HBA, or hard disk) of a registered server.  
For details on replacing server components, refer to the following sections:

- For blade servers: Refer to "[6.2.4 Replacing Server Components](#)".
- For servers other than blade servers: Refer to "[6.3.3 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 hardware other than servers, refer to the following sections:

- For blade servers: Refer to "[6.2.5 Replacing Non-server Hardware](#)".
- For servers other than blade servers: Refer to "[6.3.4 Replacing Non-server Hardware and Upgrading Firmware](#)".

## 6.2 Blade Server Maintenance

---

This section explains the maintenance of blade servers.

### 6.2.1 Maintenance LED

---

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 maintenance mode, refer to "Appendix C Maintenance Mode" in 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 of flashing 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. Configure the settings correctly, referring to "6.2 Configuring the Server Environment" in the "Design 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 the [OK] button.

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 the [OK] button.

The maintenance LED is turned off.

## 6.2.2 Reconfiguration of Hardware Properties

---

This section explains how to reconfigure hardware properties for replaced hardware.

After hardware replacement, it is necessary to reconfigure Resource Orchestrator with the new hardware properties.

For PRIMERGY BX servers for which hardware replacement including the admin LAN NIC has been performed, the hardware properties are automatically reconfigured.



- When replacing a server itself or the NIC used for either the admin or public LAN, be sure to perform this operation after the replacement.  
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 reconfiguring the hardware properties from the server.
- When certain components are replaced, such as the management blade itself, a midplane, etc., it is necessary for the management blade to restart. When replacing such a component at the same time as a server blade, an error may occur when reconfiguring the hardware properties.

To replace the management blade, a midplane, etc. at the same time as a server blade, perform the following procedure:

1. Disable automatic reconfiguration of hardware properties.

For details, refer to "[When Not Performing Reconfiguration of Hardware Properties Automatically](#)".

2. Replace the hardware.

The management blade will restart automatically.

3. After the management blade has restarted, manually reconfigure the hardware properties.

For details, refer to "[Reconfiguring Hardware Properties after Server Replacement](#)".

## 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 reconfigured 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 for which hardware replacement including the admin LAN NIC has been performed, the hardware properties are automatically reconfigured.

## When Not Performing Reconfiguration of Hardware Properties Automatically

This section explains when not performing reconfiguration of hardware properties automatically.

Configuring the values in the following definition file in advance makes it possible to select whether to perform reconfiguration of hardware information automatically.

Placeholder for the Definition File

[Windows Manager]  
*Installation\_folder*\SVROR\Manager\etc\customize\_data

[Linux Manager]  
/etc/opt/FJSVrcvnr/customize\_data

Name of the Definition File

auto\_replace.rcxprop

Format of the Definition File

<i>Key = Value</i>
--------------------

Items in the Definition File

Table 6.1 List of Specified Items

Items	Key	Value	Remarks
Automatic execution of hardware property reconfiguration	auto_replace	true false	<p>Select whether to perform reconfiguration of hardware information automatically.</p> <ul style="list-style-type: none"> <li>- When specifying "true" Reconfiguration of hardware information is executed automatically.</li> <li>- When specifying "false" Reconfiguration of hardware information is not executed automatically.</li> </ul>

Items	Key	Value	Remarks
			The default value is "true". When a character string other than "true" is specified, or the definition file is deleted, "false" is configured.

## Reconfiguring Hardware Properties after Server Replacement

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 reconfigure 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

After the message is displayed, shut down the server if it is still powered on.

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 the [OK] button.

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.

### 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 "[2.2 Starting and Stopping Agents](#)"

## 6.2.3 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.

- Replacing a Server with Spare Servers Assigned

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 4 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 "6.2 Configuring the Server Environment" in the "Design Guide VE".  
Shut down the server after completing BIOS settings.

### 3. Reconfigure Hardware Properties after Replacement

After replacing the server, reconfigure Resource Orchestrator with the latest hardware properties.

For details on how to reconfigure hardware properties, refer to "[6.2.2 Reconfiguration of Hardware Properties](#)".

After hardware properties have been reconfigured, 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 "[4.3 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 maintenance mode, refer to "Appendix C Maintenance Mode" in the "User's Guide VE".

### 2. Place the Server into VM Maintenance Mode

When the primary server is a VM host, and can be placed into VM maintenance mode, place it into VM maintenance mode.

For details on VM maintenance mode, refer to "15.2 VM Maintenance Mode of VM Hosts" in the "User's Guide VE".

### 3. Create a System Image Backup

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

For details on backing up system images, refer to "Chapter 16 Backup and Restore" in the "User's Guide VE".

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

### 4. 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 "[6.2.1 Maintenance LED](#)".

### 5. 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 "6.2 Configuring the Server Environment" in the "Design Guide VE".

Shut down the server after completing BIOS settings.

### 6. Reconfigure Hardware Properties after Replacement

After replacing the server, reconfigure Resource Orchestrator with the latest hardware properties.

For details on how to reconfigure hardware properties, refer to "[6.2.2 Reconfiguration of Hardware Properties](#)".

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

### 7. 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.

When the image operation target disk is configured, configure the image operation target disk before performing restoration.

For details, refer to "9.1.13 Changing Target Disks of Image Operations" in the "User's Guide VE".

Refer to "16.3 Restore" in the "User's Guide VE" 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.

## 8. Release VM Maintenance Mode

When the primary server was placed into VM maintenance mode, release the replaced server from VM maintenance mode. For details on VM maintenance mode, refer to "15.2 VM Maintenance Mode of VM Hosts" in the "User's Guide VE".

## 9. Release the Reference Server from Maintenance Mode

Release the replaced server from maintenance mode.

For details on maintenance mode, refer to "Appendix C Maintenance Mode" in 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 "6.2.1 Maintenance LED".

#### 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 "6.2 Configuring the Server Environment" in the "Design Guide VE".

Shut down the server after completing BIOS settings.

#### 3. Reconfigure Hardware Properties after Replacement

After replacing the server, reconfigure Resource Orchestrator with the latest hardware properties.

For details on how to reconfigure hardware properties, refer to "6.2.2 Reconfiguration of Hardware Properties".

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

## 6.2.4 Replacing Server Components

---

This section explains how to replace and add server components.

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

The procedure used to replace, add, and delete network interfaces is the same as the one described in "6.2.3 Replacing Servers".

For details, refer to "6.2.3 Replacing Servers".

When adding or removing network interfaces, if the target server is running Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, or Citrix XenServer, after completing the steps described in "6.2.3 Replacing Servers", log in with administrative privileges on the managed server and execute the following command.

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

[Citrix Xen]

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

[Xen]

When using Red Hat Enterprise Linux 5 Virtualization (Xen-Based) and not using I/O Virtualization (VIOM), 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 "Check the Network Interface Definition File" in "2.2.1.1 Software Preparation and Checks" in the "Setup 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 "6.2.3 Replacing Servers", modify the configuration file.

For details, refer to "Check the Network Interface Definition File" in "2.2.1.1 Software Preparation and Checks" in the "Setup Guide VE".

- **Replacing an HBA**

- 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 reconfigure access paths on the storage side.
- When configuring WWN information, it is necessary to change WWN information settings to the replaced HBA WWN values. For details on how to change WWN information, refer to "9.1.12 Changing WWN Settings for ETERNUS SF Storage Cruiser Integration" in the "User's Guide VE".

- **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.

When the image operation target disk is configured, configure the image operation target disk before performing restoration. For details, refer to "9.1.13 Changing Target Disks of Image Operations" in the "User's Guide VE".



## Information

The backup and restore functions available in Resource Orchestrator can be used to restore the boot disk contents. For details, refer to "Chapter 16 Backup and Restore" in the "User's Guide VE".

- **Replacing a System Board**

The procedure used to replace a system board is the same as that described in "6.2.3 Replacing Servers". For details, refer to "6.2.3 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.

## 6.2.5 Replacing Non-server Hardware

---

This section explains how to replace hardware external to servers.

- **Replacing Chassis**

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

- **Replacing Management Blades**

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

- **Replacing LAN Switch Blades**

No specific action is required in Resource Orchestrator for PRIMERGY BX900/BX400 LAN switch blades in either IBP mode or Converged Fabric mode and for PY CB 10Gb FEX Nexus B22 LAN switch blades.

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.

For LAN switch blades (PY CB DCB SW 10Gb 18/6/6), the Automatic Migration of Port Profile (AMPP) configuration of all ports and VLAN settings of external ports must be restored manually.

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 the [OK] button.

VLAN settings are applied to the specified LAN switch blade.

For LAN switch blades (PY CB DCB SW 10Gb 18/6/6), only the VLAN settings of internal ports for which an Automatic Migration of Port Profile (AMPP) has not been configured are restored.

### Information

#### **When Restoration is Necessary when Replacing LAN Switch Blades**

When a replaced LAN switch blade is detected, the following message is displayed in the [General] tab in [Resource Details].

The LAN switch has been replaced. Check that the unit status is normal, and then perform restoration.

Perform restoration after this message is displayed.

Detection of replaced LAN switch blades may take some time.

### 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 "7.3.4 Configuring VLANs on LAN Switch Blades" in the "User's Guide VE".

When the following configurations before and after replacement of a PRIMERGY BX900/BX400 series LAN switch blade are different, delete the registered LAN switch blade and register it again.

- Operation mode (IBP, VCS, or Converged Fabric mode, and another mode)
  - VCS ID
  - RBridge ID
  - Fabric ID
  - Domain ID
  - Switch ID
- When replacing LAN switch blades, acquisition of the VLAN information by regular update stops.  
When Resource Orchestrator is restored, acquisition of the VLAN information starts again.

- When operations are continued without performing restoration, the VLAN information managed with Resource Orchestrator and the VLAN settings of the LAN switch blades may be different, since acquisition of the VLAN information by regular update will not occur.

Clear the checkbox in the restoration dialog, and then perform restoration. As a result, VLAN settings retained by Resource Orchestrator will be discarded and acquisition of VLAN information from the LAN switch blade can be resumed.

#### - Replacing Fibre Channel Switch Blades

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

In Resource Orchestrator, the settings for Fibre Channel switch blades are not restored.

Restore the settings for Fibre Channel switch blades based on the information in hardware manuals.

#### - 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.

When the image operation target disk is configured, configure the image operation target disk before performing restoration. For details, refer to "9.1.13 Changing Target Disks of Image Operations" in the "User's Guide VE".

#### Information

The backup and restore functions available in Resource Orchestrator can be used to restore the boot disk contents. For details, refer to "Chapter 16 Backup and Restore" in the "User's Guide VE".

## 6.3 Maintenance for Servers Other Than Blade Servers

This section explains server maintenance for servers other than blade servers.

### 6.3.1 Reconfiguration of Hardware Properties

This section explains how to reconfigure hardware properties for replaced hardware.

When replacing hardware or adding or removing server components, it is necessary to reconfigure Resource Orchestrator with the new hardware properties.

#### Note

- When replacing a server itself or the NIC used for either the admin or public LAN, be sure to perform this operation after the replacement.  
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.  
\* Note: For the PRIMEQUEST 2000 series, take GSPB as meaning IOU.
- After replacing the hardware, the server status becomes "unknown". The appropriate status can be restored by reconfiguring the hardware properties from the server.
- For PRIMEQUEST, after IOU replacement or immediately after powering on, the MAC Address for each partition that is obtained from the MMB becomes FF:FF:FF:FF:FF:FF. After each partition is powered on, the MAC Address of the correct LAN is obtained from the MMB. Reconfigure the hardware properties after powering on partitions.

- A MAC address used for configuring public LAN (MAC address) information cannot be specified as the MAC address of the admin LAN. To specify that MAC address for the admin LAN, first delete it from the public LAN (MAC address) information settings. For details, refer to "11.10 Deleting the Public LAN (MAC Address) Information" in the "User's Guide VE".
- 

## 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.

- 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.

## Reconfiguring Hardware Properties after Hardware Replacement or Addition or Removal of Server Components

- For Rack Mount and Tower Servers

Use the following procedure to reconfigure properties for replaced hardware.

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

However, when the MAC address of the admin LAN has been virtualized, after checking the physical MAC address using the procedure in [Additional Information](#), stop the server.

For servers virtualized using VIOM or ISM, check the physical MAC address with the profile in an unapplied state.

### Additional Information

With the HBA address rename method, when a server using SAN boot has a hardware exchange that results in the MAC address used for the admin LAN being changed, the OS and an agent cannot be started.

In this case, the server should be started once, and the MAC address confirmed on the BIOS (hardware) screen. After the MAC address is confirmed, power off the server again.

2. In the ROR console server resource tree, right-click the target server and select [Hardware Maintenance]-[Reconfigure] from the popup menu.
3. Enter MAC addresses for the network interfaces used on the admin LAN.

Enter the value for the physical MAC address.

- Admin LAN (MAC Address (NIC1))

This is necessary when the admin LAN MAC address has been virtualized or an agent has not been registered.

### Additional Information

When a server is powered off for the reason given in the [Additional Information](#) in step 1, the item for input of the value of NIC1 is displayed. In this case, input the MAC address confirmed in the [Additional Information](#) in step 1.

- 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 the [OK] button.

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 reconfigure hardware properties after replacement of hardware or addition or removal of server components:

1. Replace the system board or GSPB, or add or remove server components.

For the PRIMEQUEST 2000 series, take GSPB as meaning IOU.

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 the [OK] button.

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

- For SPARC M10/M12 and SPARC Enterprise Servers

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



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 "[2.2 Starting and Stopping Agents](#)"

## 6.3.2 Replacing Servers

---

This section details the procedure to follow when replacing servers.



- 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 Rack Mount and Tower Servers

- Replacing a Server with Spare Servers Assigned

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 4 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 "6.2 Configuring the Server Environment" in the "Design 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. Reconfigure Hardware Properties After Replacement

After replacing the server, reconfigure Resource Orchestrator with the latest hardware properties.

For details on how to reconfigure hardware properties, refer to ["6.3.1 Reconfiguration of Hardware Properties"](#).

When using VIOM, refer to the manual of ServerView Virtual-IO Manager and perform inventory boot on ServerView Virtual-IO Manager.

When using I/O virtualization using ISM, restart ISM.

When public LAN (MAC address) information is configured, it is necessary to reconfigure the information. Perform reconfiguration after completing ["6.3.2 Replacing Servers"](#).

For details, refer to ["7.4.3 Registering the Public LAN \(MAC Address\) Information"](#) in the ["User's Guide for VE"](#).

### 4. Perform Post-server Switchover Operations

For details on the operations that must be performed after a server switchover, refer to ["4.3 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 maintenance mode, refer to ["Appendix C Maintenance Mode"](#) in the ["User's Guide VE"](#).

#### 2. Place the Server into VM Maintenance Mode

When the primary server is a VM host, and can be placed into VM maintenance mode, place it into VM maintenance mode.

For details on VM maintenance mode, refer to ["15.2 VM Maintenance Mode of VM Hosts"](#) in the ["User's Guide VE"](#).

#### 3. Create a System Image Backup

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

For details on backing up system images, refer to ["Chapter 16 Backup and Restore"](#) in the ["User's Guide VE"](#).

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

#### 4. Power the Server Off

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

For details on shutting down servers, refer to ["Chapter 14 Power Control"](#) in the ["User's Guide VE"](#).

#### 5. 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 ["6.2 Configuring the Server Environment"](#) in the ["Design 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.

### 6. Reconfigure Hardware Properties After Replacement

After replacing the server, reconfigure Resource Orchestrator with the latest hardware properties.

For details on how to reconfigure hardware properties, refer to ["6.3.1 Reconfiguration of Hardware Properties"](#).

When using VIOM, refer to the manual of ServerView Virtual-IO Manager and perform inventory boot on ServerView Virtual-IO Manager.

When using I/O virtualization using ISM, restart ISM.

When public LAN (MAC address) information is configured, it is necessary to reconfigure the information. Perform reconfiguration after completing ["6.3.2 Replacing Servers"](#).

For details, refer to ["7.4.3 Registering the Public LAN \(MAC Address\) Information"](#) in the ["User's Guide for VE"](#).

## 7. 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.

When the image operation target disk is configured, configure the image operation target disk before performing restoration.

For details, refer to "9.1.13 Changing Target Disks of Image Operations" in the "User's Guide VE".

Refer to "16.3 Restore" in the "User's Guide VE" 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.

## 8. Release VM Maintenance Mode

When the primary server was placed into VM maintenance mode, release the replaced server from VM maintenance mode.

For details on VM maintenance mode, refer to "15.2 VM Maintenance Mode of VM Hosts" in the "User's Guide VE".

## 9. Release the Reference Server from Maintenance Mode

Release the replaced server from maintenance mode.

For details on maintenance mode, refer to "Appendix C Maintenance Mode" in 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 the Server Off

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

For details on shutting down servers, refer to "Chapter 14 Power Control" in the "User's Guide VE".

#### 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 "6.2 Configuring the Server Environment" in the "Design 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. Reconfigure Hardware Properties After Replacement

After replacing the server, reconfigure Resource Orchestrator with the latest hardware properties.

For details on how to reconfigure hardware properties, refer to "[6.3.1 Reconfiguration of Hardware Properties](#)".

When using VIOM, refer to the manual of ServerView Virtual-IO Manager and perform inventory boot on ServerView Virtual-IO Manager.

When using I/O virtualization using ISM, restart ISM.

When public LAN (MAC address) information is configured, it is necessary to reconfigure the information. Perform reconfiguration after completing "[6.3.2 Replacing Servers](#)".

For details, refer to "7.4.3 Registering the Public LAN (MAC Address) Information" in the "User's Guide for VE".

## For SPARC M10/M12 and SPARC Enterprise Servers

### - Replacing a Server with Spare Servers Assigned

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 4 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 "6.2 Configuring the Server Environment" in the "Design 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 "[4.3 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 4 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 "6.2 Configuring the Server Environment" in the "Design 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 "[4.3 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 "6.2 Configuring the Server Environment" in the "Design 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 "ETERNUS SF Storage Cruiser Operation 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 "ETERNUS SF Storage Cruiser Operation Guide".

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



## Information

[OVM for SPARC]

When replacing servers, it is necessary to restore the OVM for SPARC environment.

For details, refer to ["4.3.2 Recovery of OVM for SPARC Environments"](#).

### - When SPARC M10-4S/M12-2S are in a Building Block Configuration

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

## For PRIMEQUEST Servers

### - 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 maintenance mode, refer to "Appendix C Maintenance Mode" in the "User's Guide VE".

#### 2. Place the Server into VM Maintenance Mode

When the primary server is a VM host, and can be placed into VM maintenance mode, place it into VM maintenance mode.

For details on VM maintenance mode, refer to "15.2 VM Maintenance Mode of VM Hosts" in the "User's Guide VE".

#### 3. Create a System Image Backup

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

For details on backing up system images, refer to "Chapter 16 Backup and Restore" in the "User's Guide VE".

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

#### 4. Power the Server Off

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

For details on shutting down servers, refer to "Chapter 14 Power Control" in the "User's Guide VE".

#### 5. 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 "6.2 Configuring the Server Environment" in the "Design Guide VE".

Shut down the server after completing BIOS settings.



## 6. Reconfigure Hardware Properties after Replacement

After replacing the server, reconfigure Resource Orchestrator with the latest hardware properties.

For details on how to reconfigure hardware properties, refer to "[6.3.1 Reconfiguration of Hardware Properties](#)".

## 7. 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 "16.3 Restore" in the "User's Guide VE" 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.

## 8. Release VM Maintenance Mode

When the primary server was placed into VM maintenance mode, release the replaced server from VM maintenance mode.

For details on VM maintenance mode, refer to "15.2 VM Maintenance Mode of VM Hosts" in the "User's Guide VE".

## 9. Release the Reference Server from Maintenance Mode

Release the replaced server from maintenance mode.

For details on maintenance mode, refer to "Appendix C Maintenance Mode" in 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 the Server Off

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

For details on shutting down servers, refer to "Chapter 14 Power Control" in the "User's Guide VE".

#### 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 "6.2 Configuring the Server Environment" in the "Design Guide VE".

Shut down the server after completing BIOS settings.

#### 3. Reconfigure Hardware Properties after Replacement

After replacing the server, reconfigure Resource Orchestrator with the latest hardware properties.

For details on how to reconfigure hardware properties, refer to "[6.3.1 Reconfiguration of Hardware Properties](#)".

## 6.3.3 Replacing and Adding Server Components

---

This section explains how to replace and add server components.

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

The procedure used to replace, add, and delete network interfaces is the same as the one described in "[6.3.2 Replacing Servers](#)".

For details, refer to "[6.3.2 Replacing Servers](#)".

When adding or removing network interfaces, if the target server is running Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, or Citrix XenServer, after completing the steps described in "[6.3.2 Replacing Servers](#)", log in with administrative privileges on the managed server and execute the following command.

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

When Public LAN (MAC Address) Information Is Configured on a Rack Mount Server or a Tower Server

When public LAN (MAC address) information is configured, it is necessary to reconfigure the information.

Perform configuration after completing "6.3.2 Replacing Servers".

For details, refer to "7.4.3 Registering the Public LAN (MAC Address) Information" in the "User's Guide VE".

[Citrix Xen]

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

[Xen]

When using Red Hat Enterprise Linux 5 Virtualization (Xen-Based) and not using I/O virtualization using VIOM or ISM, 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 "Check the Network Interface Definition File" in "2.2.1.1 Software Preparation and Checks" in the "Setup 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 "6.3.2 Replacing Servers", modify the configuration file.

For details, refer to "Check the Network Interface Definition File" in "2.2.1.1 Software Preparation and Checks" in the "Setup 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

- 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 reconfigure access paths on the storage side.
- When configuring WWN information, it is necessary to change WWN information settings to the replaced HBA WWN values. For details on how to change WWN information, refer to "9.1.12 Changing WWN Settings for ETERNUS SF Storage Cruiser Integration" in the "User's Guide VE".

#### - 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.

When the image operation target disk is configured, configure the image operation target disk before performing restoration.

For details, refer to "9.1.13 Changing Target Disks of Image Operations" in the "User's Guide VE".

## Information

The backup and restore functions available in Resource Orchestrator can be used to restore the boot disk contents. For details, refer to "Chapter 16 Backup and Restore" in the "User's Guide VE".

### - **Replacing a System Board**

The procedure used to replace a system board is the same as that described in "6.3.2 Replacing Servers". For details, refer to "6.3.2 Replacing Servers".

### - **Replacing an IO Board**

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

### - **Addition and Deletion of Server Parts for the PRIMEQUEST 2000 Series**

When performing operations from MMB, or when performing addition or deletion of SBs and IOUs using Dynamic Reconfiguration, reconfigure the latest hardware information in Resource Orchestrator. For details on how to reconfigure hardware properties, refer to "6.3.1 Reconfiguration of Hardware Properties".

For details on how to add or delete server parts, refer to the operation management manuals for the PRIMEQUEST 2000 series.

### - **Replacing Other Server Components**

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

## **6.3.4 Replacing Non-server Hardware and Upgrading Firmware**

---

This section explains how to replace hardware external to servers and upgrade firmware.

### - **Replacing Management Blades**

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

No specific action is required when updating firmware.

When performing replacements or upgrading firmware, the status of the chassis and server blades mounted in the chassis may change to "unknown".

### - **Replacing Management Boards**

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

No specific action is required when updating firmware.

When performing replacements or upgrading firmware, the status of servers may change to "unknown".

### - **Replacing LAN Switches**

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

No specific action is required when updating firmware.

When performing replacements or upgrading firmware, the status of LAN switches may change to "unknown".

### - **Upgrading Firmware of PRIMEQUEST Chassis**

#### 1. Place the Server into Maintenance Mode

Place the server to upgrade the firmware of into maintenance mode.

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

#### 2. Place the Server into VM Maintenance Mode

When the primary server for firmware upgrade is a VM host, and can be placed into VM maintenance mode, place it into VM maintenance mode.

For details on VM maintenance mode, refer to "15.2 VM Maintenance Mode of VM Hosts" in the "User's Guide VE".

#### 3. Power the Server Off

Shut down the server for firmware upgrade if it is still powered on.

For details on shutting down servers, refer to "Chapter 14 Power Control" in the "User's Guide VE".

#### 4. Upgrading Firmware of PRIMEQUEST Chassis

Perform upgrade of the firmware of PRIMEQUEST chassis.

#### 5. Release VM Maintenance Mode

When the server of which the firmware was upgraded was placed into VM maintenance mode, release it from VM maintenance mode.

For details on VM maintenance mode, refer to "15.2 VM Maintenance Mode of VM Hosts" in the "User's Guide VE".

#### 6. Release the Reference Server from Maintenance Mode

Release the server of which the firmware was upgraded from maintenance mode.

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



See

When using ISM, refer to the manuals of ServerView Infrastructure Manager.

## 6.4 Network Device Maintenance

---

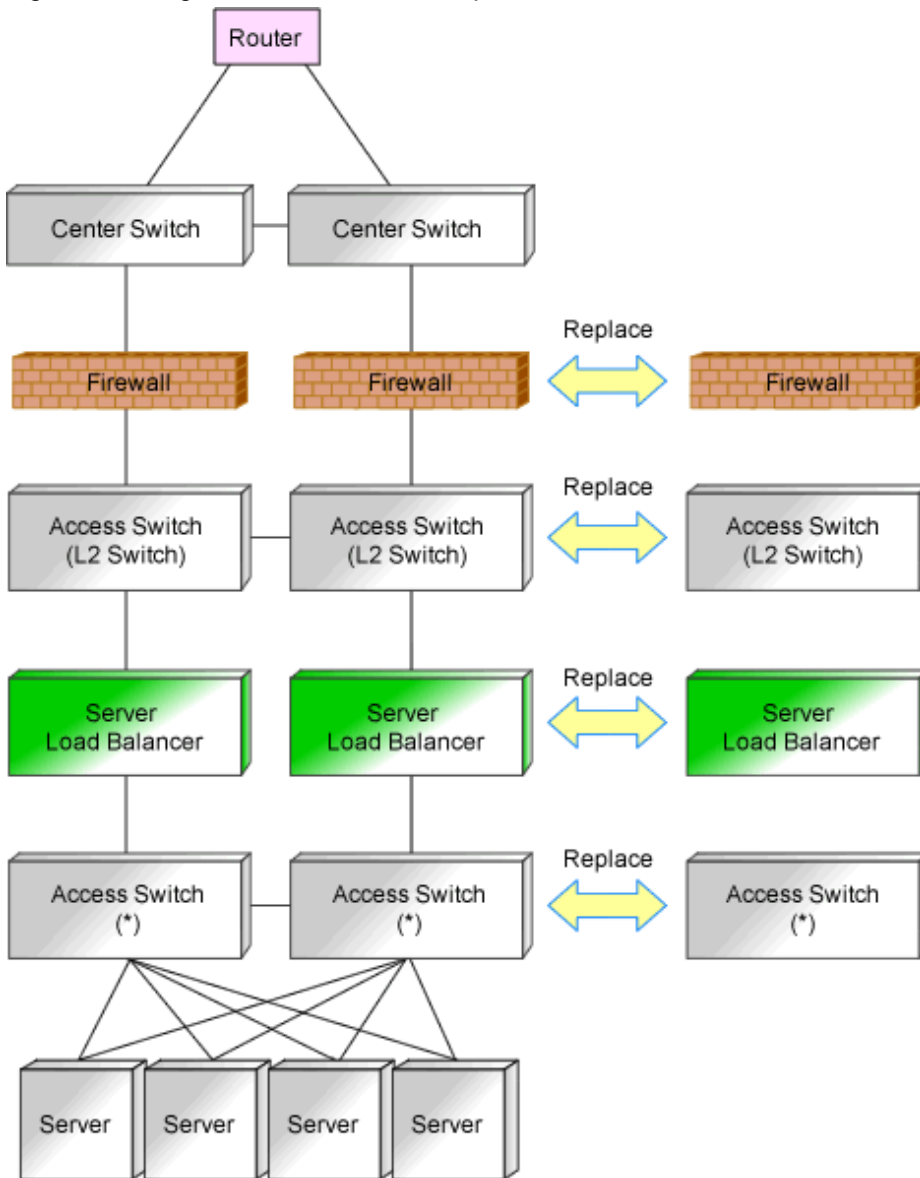
This section explains how to maintain network devices that are the target of management in Resource Orchestrator.

### 6.4.1 Common Maintenance Procedure of Network Devices

---

This section explains the procedure to replace network devices when it becomes necessary due to failure.

Figure 6.2 Image of Network Device Replacement



\* Note: L2 switches or switches that comprise the Ethernet Fabric.

It is assumed that you perform replacement while continuing operations using the network devices of redundancy configurations of an active and standby switch configuration.

When there is no description, the operations are performed by an administrator.

In Resource Orchestrator, there are no functions to back up the environment information (definitions, etc.) of network devices. Therefore, it is recommended to perform backup of the environment information for the network devices at timing such as after completion of the environment configuration or modification of the definition.

For details on backup, refer to the network device manuals.

### 6.4.1.1 When the Network Device to Replace Has Failed

This section explains the replacement procedure when the device to replace has failed.

1. Announcement of planned maintenance operations.
2. Change the target network device to "maintenance mode".
3. Replace the network devices. (Hardware maintenance person)

4. Restore configuration of replaced network devices following the maintenance procedure for the network device.
5. Release the "maintenance mode" of network devices, when problems with network devices after replacement have been solved.
6. Notification that maintenance operations are complete.

### Information

When the replaced network device is a member switch in an Ethernet Fabric configuration (Fujitsu PRIMERGY Converged Fabric switch blade (10 Gbps 18/8+2) or Fujitsu Converged Fabric switch), setting and releasing of maintenance mode is not necessary. Follow the maintenance procedure for that device.

## 6.4.1.2 When the Network Device to Replace Has Not Failed

This section explains the replacement procedure when the network device that is the target of replacement has not failed.

1. Announcement of planned maintenance operations.
2. Log in the network device directly to check if the target network device of replacement is in active status or standby status.  
When the target network device of replacement is in active status, switch over the device with the standby network device of redundancy configuration, and change the status of target network device for replacement from active status to standby status.
3. Change the target network device to "maintenance mode".
4. Back up the current environment (such as definitions) from the network devices that are switched to "maintenance mode".
5. Replace the network devices. (Hardware maintenance person)
6. Restore the configuration of the replaced network device using the environment backed up in step 4, following the maintenance procedure for the network device.
7. Back up the current definitions from the network devices with operational status.
8. Check that there are no differences in the definitions in the redundancy configurations using environments backed up in step 7 and environment definitions backed up in step 4.  
When there is difference that is a problem, log in to the network device directly after replacement, and resolve the difference.
9. Release the "maintenance mode" of network devices, when problems with network devices after replacement have been solved.
10. Notification that maintenance operations are complete.

### Information

When the replaced network device is a member switch in an Ethernet Fabric configuration (Fujitsu PRIMERGY Converged Fabric switch blade (10 Gbps 18/8+2) or Fujitsu Converged Fabric switch), setting and releasing of maintenance mode is not necessary. Follow the maintenance procedure for that device.

## 6.4.1.3 Regular Maintenance Procedure of Network Devices

This section explains the procedure of regular maintenance (patch application or firmware update) of network devices.

Use the following procedure when performing maintenance operations while continuing operations using the network devices of redundancy configurations by switching between active and standby.

1. Announce that regular maintenance operations are being started.
2. Confirm that the network device that is the target of regular maintenance is in standby status, by directly logging in to the network device.
3. Back up the current network device configuration file from the network device with standby status.

Back up the configuration files from network devices.

For information about the backup method, refer to the network device manuals.

4. Change the target network device in standby status to "maintenance mode".
5. A hardware maintenance person performs the regular maintenance operations for network devices (patch application or firmware update).
6. Back up the current network device configuration files from the network devices with operational status.  
 Back up the configuration files from network devices.  
 For information about the backup method, refer to the network device manuals.
7. Check that there are no differences between the network device configuration files backed up in step 3 and those backed up in step 6.  
 Export the network device file from the network device and check it for difference. When there is difference that is a problem, log in to the network device with standby status, and resolve the difference.  
 For information about how to export, refer to the network device manuals.  
 For information about login to network devices, refer to the network device manuals.
8. Release the network device from "maintenance mode", after checking that problems with network devices with standby status have been solved.
9. Switch over the network device in active status that is the target of regular maintenance and the network device of the redundancy configuration which is in standby status.
10. Then change the status of the remaining network device that is the target of regular maintenance from operational status to standby status, and perform steps 3 to 8.
11. Announce that maintenance operations are complete.

 See

- For details on how to configure and release the maintenance mode, refer to "20.1 Switchover of Maintenance Mode" in the "User's Guide VE".

 Note

- Regular maintenance may not be able to be performed using the described procedure depending on the maintenance details for individual network devices. Before performing regular maintenance operations, ensure you check the information provided from the network device vendors regarding the maintenance operations of network devices.
- Confirm the following items, using the manuals of network devices, in advance.
  - The operations for network devices (status check, switchover and backup methods)
  - Environmental differences which become problems due to redundancy configurations
- When performing regular maintenance for multiple network devices of redundancy configurations simultaneously, perform replacement operations in units of the same redundancy configurations.

 Information

- When the replaced network device is a member switch in an Ethernet Fabric configuration (Fujitsu PRIMERGY Converged Fabric switch blade (10 Gbps 18/8+2) or Fujitsu Converged Fabric switch), setting and releasing of maintenance mode is not necessary. Follow the maintenance procedure for that device.

#### 6.4.1.4 Procedure for Addition or Modification of Connection Destinations of Network Devices

This section explains the procedure for adding or modifying destinations for network device connection.

1. Notify your administrator about the addition or modification of the destination for network device connection. (Network device administrator)
2. Create network configuration information (XML definition) using the acquired network device information.
3. Confirm there are no differences besides the link information (under Links tag) regarding the added or modified destinations for connection, by comparing the network configuration information of network devices registered in Resource Orchestrator and the network configuration information created in step 2.

If there is any difference, check with the system administrator that network device configurations have not been modified, and change the network configuration information if necessary.

The network configuration information of network devices registered in Resource Orchestrator can be obtained using the `rcxadm netconfig export` command.

4. Modify the network device by setting the confirmed network configuration information as the input information.  
Use the `rcxadm netconfig import` command to modify network devices.
5. Confirm from the ROR console that the network device information has changed, and the status is normal.



See

- For details on how to create network configuration information (XML definition), refer to "8.1 Network Configuration Information" in the "Reference Guide (Command) VE".
- For details on the `rcxadm netconfig` command, refer to "3.2 `rcxadm netconfig`" in the "Reference Guide (Command) VE".

## 6.4.2 Maintenance Procedures of Network Devices (Firewalls, Server Load Balancers, and L2 Switches)

---

This section explains the maintenance procedures of network devices (firewalls, server load balancers, and L2 switches).

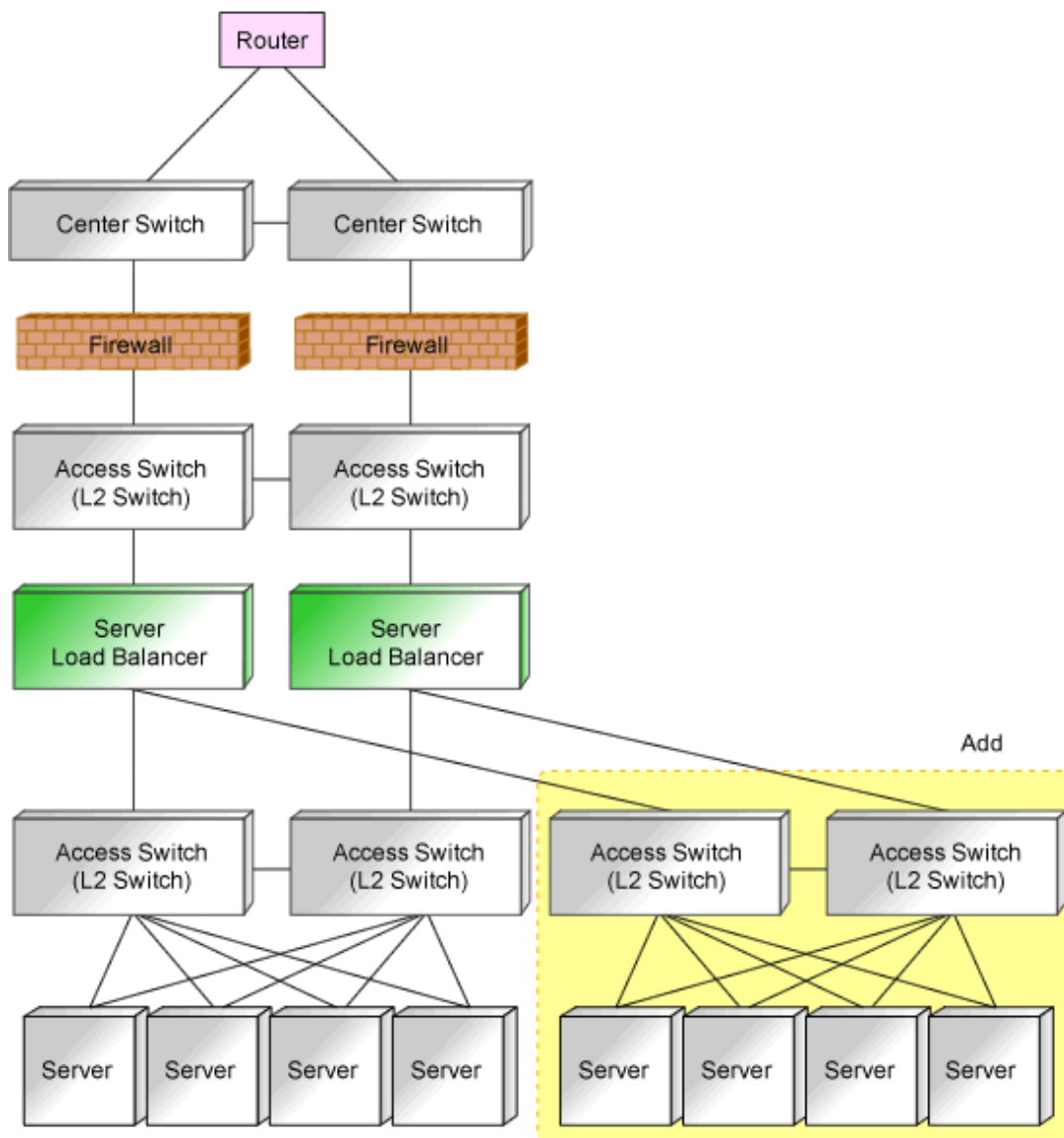
### 6.4.2.1 Adding L2 Switches to Handle Insufficient Numbers of Ports when Adding Servers

This section explains the procedure for addition, assuming a case where it is necessary to add L2 switches, since the LAN ports of the L2 switch to connect to are insufficient when adding servers.

The explanation is mainly about operations related to L2 switches.



Figure 6.3 Image of L2 Switches to Add



1. Design additional configurations. (Network device administrator)
2. Provide the additional network device information to the administrator. (Network device administrator)
  - Add a network device in the state where the following operations have been completed.
    - Initial configuration
    - Operation test
    - Integration of the device into a physical network configuration
3. Register the resources of the server.
  - It is necessary to register chassis or LAN switch blades for a blade server.
4. Create network configuration information (XML definition) using the acquired network device information.
5. Register an additional L2 switch as a network device.
  - Use the `rcxadm netdevice create` command to register as a network device.



See

- For details on the initial configurations of network devices, refer to "7.7.1 Settings for Managed Network Devices" in the "Design Guide VE".
- For details on how to create network configuration information (XML definition), refer to "8.1 Network Configuration Information" in the "Reference Guide (Command) VE".
- For details on the rcxadm netdevice command, refer to "3.3 rcxadm netdevice" in the "Reference Guide (Command) VE".

## **6.4.3 Maintenance Procedures of Network Devices (Ethernet Fabrics)**

---

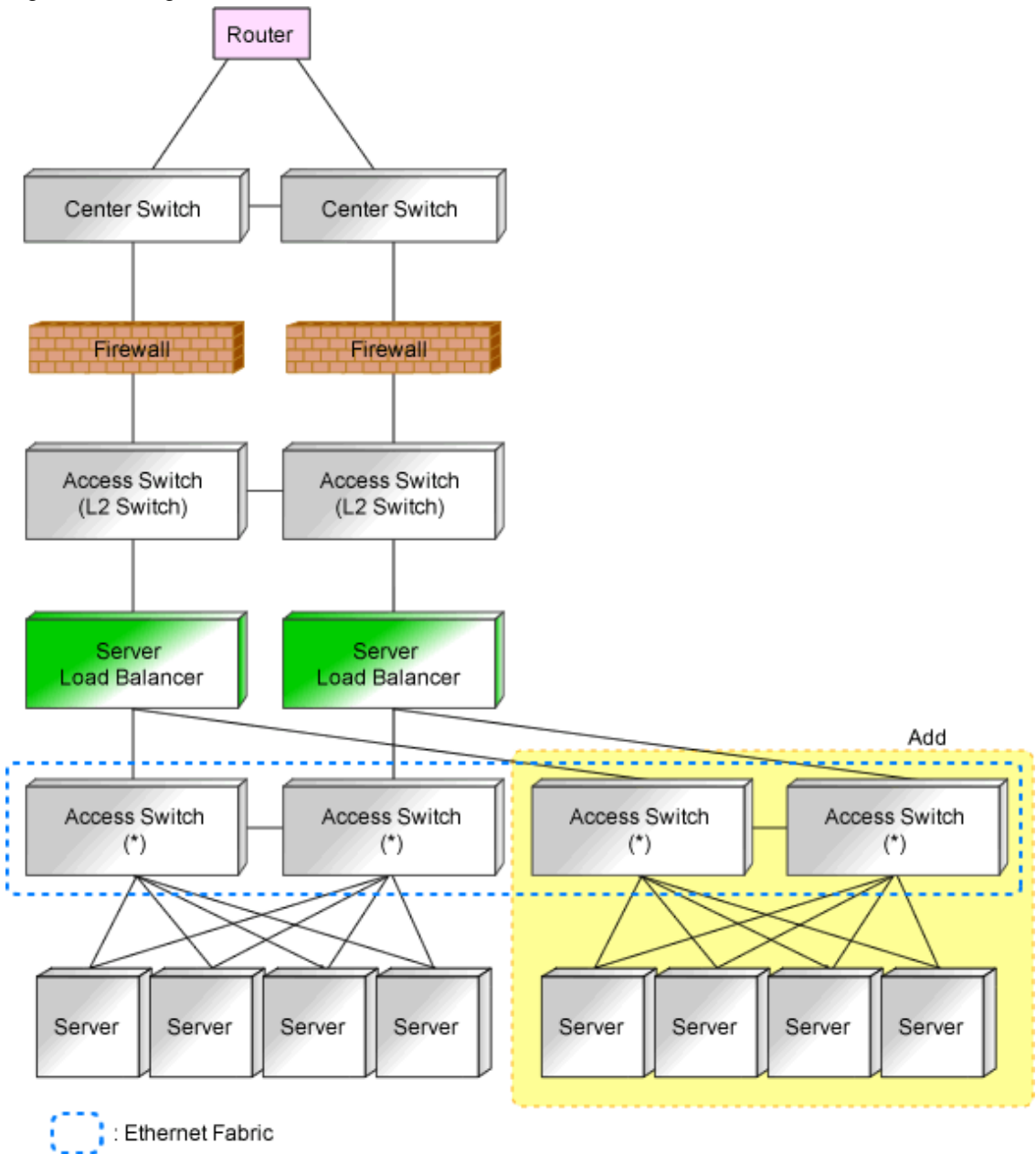
This section explains the maintenance procedures of network devices (Ethernet Fabrics).

### **6.4.3.1 Adding Switches to an Ethernet Fabric to Handle Insufficient Numbers of Ports when Adding Servers**

This section explains the procedure for addition, assuming a case where it is necessary to add switches due to a shortage of LAN ports of the Ethernet Fabric to connect to when adding servers.

The explanation is mainly about operations related to the Ethernet Fabric.

Figure 6.4 Image of Ethernet Fabric Switches Addition



\* Note: Switches that comprise the Ethernet Fabric.

1. Design additional configurations. (Network device administrator)
2. Provide an administrator with the link information of the server connection port to add to the Ethernet Fabric. (Network device administrator)  
Add switches according to the maintenance procedure of the Ethernet Fabric.
3. Register the resources of the server.  
For a blade server, it is necessary to register chassis or LAN switch blades.
4. Create network configuration information (XML definition) using the acquired link information of the server connection port.

 **Information**

When the destination server is a blade server, it is not necessary to create the link information.

5. Register the modified network configuration information.  
Use the `rcxadm netconfig import` command to register network configuration information.



- For details on how to create network configuration information (XML definition), refer to "8.1 Network Configuration Information" in the "Reference Guide (Command) VE".
- For details on the `rcxadm netconfig` command, refer to "3.2 `rcxadm netconfig`" in the "Reference Guide (Command) VE".

### 6.4.3.2 Migrating an Ethernet Fabric (Converged Fabric) to a Multiple VFAB Environment

This section explains the procedure to migrate a single Ethernet Fabric (Converged Fabric) to multiple VFABs in an environment where an Ethernet Fabric is installed.

1. Configure maintenance mode on the network device for Converged Fabric, log in to the target Converged Fabric using SSH, and perform the following.
  - a. Configure a VFAB and its VFAB operation mode.
  - b. Configure the port type of the port to connect with the external network used in the VFAB added in step a as CIR.
  - c. When the operation mode of the VFAB is network mode, configure the VLAN ID specified for the network resource in the tenant corresponding to the VFAB in the CIR port configured in step b. At this time, also configure the identifier of the added VFAB.
  - d. When there are no modifications for external connection ports for the network resource described in step c when performing step 3, perform the following configuration.
    - Modify the configuration of the relationship between the port profile and the MAC address corresponding to the VLAN ID of the network resource.

2. Update the network device information.

Use the `rcxadm netdevice refresh -recreate` command to update the network device information.

3. Configure maintenance mode on the network device for Converged Fabric, log in to the target Converged Fabric using SSH, and perform the following.
  - a. Configure a VFAB and its VFAB operation mode.
  - b. Configure the port type of the port to connect with the external network used in the VFAB added in step a as CIR.
  - c. When the operation mode of the VFAB is network mode, configure the VLAN ID specified for the network resource in the tenant corresponding to the VFAB in the CIR port configured in step b. At this time, also configure the identifier of the added VFAB.
  - d. When there are no modifications for external connection ports for the network resource described in step c when performing step 3, perform the following configuration.
    - Modify the configuration of the relationship between the port profile and the MAC address corresponding to the VLAN ID of the network resource.

4. Update the network device information.

Use the `rcxadm netdevice refresh -recreate` command to update the network device information.

### 6.4.3.3 Reflecting a Modified Domain Switch Configuration on the Ethernet Fabric

This section explains the procedure for operations when modifying the domain switch configuration of an Ethernet Fabric registered in Resource Orchestrator.

When there is no description, the following operations are performed by an infrastructure administrator.

1. When the following operations are performed, it is necessary to update the port information of network devices.
  - Switches are added or deleted
  - When the fabric ID, domain ID, switch ID, or port type is changed for Converged Fabric
  - When the VCS ID or RBridge ID is changed for VCS

Use the `rcxadm netdevice refresh -recreate` command to update the port information of network devices.

2. When modifying the links of uplink ports, re-register the link information.  
For details, refer to "[6.4.1.4 Procedure for Addition or Modification of Connection Destinations of Network Devices](#)".
3. When modifying the fabric ID, domain ID or the switch ID of a LAN switch blade PY CB Eth Switch 10/40Gb 18/8+2, it is necessary to update the information of the LAN switch blade by registering it again.  
  
Delete the registered LAN switch blade after modifying network resource settings for external ports so as not to use the LAN switch blade.



See

For details on the `rcxadm netdevice` command, refer to "3.3 `rcxadm netdevice`" in the "Reference Guide (Command) VE".

## 6.5 Storage Device Maintenance

---

This section explains how to maintain storage devices.

### - Replacing storage devices

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

In Resource Orchestrator, the settings for storage devices are not restored.

Restore the settings for storage devices based on the information in hardware manuals.

### - Replacing Fibre Channel switches

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

In Resource Orchestrator, the settings for Fibre Channel switches are not restored.

Restore the settings for Fibre Channel switches based on the information in hardware manuals.

## 6.6 Power Monitoring Device (PDU or UPS) Maintenance

---

This section explains how to maintain power monitoring devices (PDU or UPS).

### - Replacing power monitoring devices (PDU or UPS)

After replacing a power monitoring device, reconfigure the hardware properties of the power monitoring device (PDU or UPS).

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. Reconfigure 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 the [OK] button.

The target power monitoring device's hardware properties are reconfigured.

# Chapter 7 Maintaining Software with Cloning [Physical Servers]

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

## 7.1 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 reconfiguring the network interfaces used for the public LAN following deployment of a cloning image.

For details on the cloning function, refer to "Chapter 17 Cloning [Physical Servers]" in the "User's Guide VE".



### Note

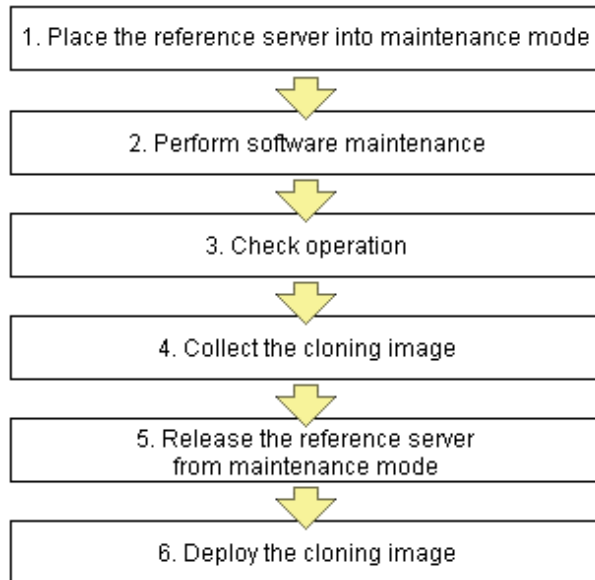
- Software maintenance tasks performed using the cloning function only apply to servers that share the same hardware and software configuration.
- Deployment of a cloning image will reset the VLAN settings used for the public LAN of each target server. Those settings need to be restored either manually 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

## 7.2 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 7.1 Software Maintenance Procedure Using Cloning



Each of these steps is explained below.

1. Place the 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 C Maintenance Mode" in 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 "17.2 Collecting" in 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 C Maintenance Mode" in 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 "17.3 Deploying" in the "User's Guide VE".



## **Chapter 8 Backup and Restoration of Managed Servers**

This chapter explains how to back up and restore managed servers.

This function enables backing up and restoration of system images of physical OS's and VM hosts.

For details, refer to "Chapter 16 Backup and Restore" in the "User's Guide VE".

# Chapter 9 Backup and Restoration of Admin Servers

This chapter explains how to back up and restore admin servers.

## Point

In addition to the Resource Orchestrator admin server and managed servers, be sure to back up other servers in the system as well.

## 9.1 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).

### 9.1.1 Resources Managed by This Product and Timing of Update

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 9.1 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.	No action is necessary	-
Session encryption keys	rcxkeydefbackup	Yes	After password saving (after execution of the rcxlogin -save command)	No action is necessary	-
System images and cloning images	scwbackup	Yes	After addition, deletion, and modification of physical server images	No action is necessary	-
Configuration definition information	rcxbackup	Yes	After creation, registration, modification, unregistration, and deletion of resources	No action is necessary	-
Information related to image files	scwbackup	Yes	After the registration and unregistration of VM hosts	No action is necessary	-
Definition files	rcxkeydefbackup	Yes	Modification of definition files	No action is necessary	-
Image management information	rcxkeydefbackup	Yes	After rcxadm imagemgr command operations	No action is necessary	-

Backup operations are necessary at the timing listed in "[Table 9.1 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, is it possible to perform restoration.

When performing hardware configuration or configuration changes, perform backup again.

- Replacement of a chassis, LAN switch, managed server, or power monitoring device hardware
- Replacement of the NIC of a managed server
- LAN connections between managed servers and LAN switches
- Server switchover or takeover (\*)
- Modification of the configuration of image operation target disks of managed servers

\* Note: If failback has been performed after server switchover, restore can be performed.



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.

## 9.1.2 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 "[9.2.1 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 "[9.2.2 Backing Up Configuration Definition Information](#)".

## 9.1.3 Restore

---

Restore backed up resources to the admin server using the following procedure.

For details, refer to "[9.3 Restoration](#)".

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 clustered manager configurations, 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 to 6 in "[9.3 Restoration](#)", and restore system images, cloning images, and configuration definition information.

---

## 9.1.4 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 immediately after the backup operation.

For details on the command, refer to "Chapter 6 Backup and Restoration Operations for Configuration Definition Information" in the "Reference Guide (Command) VE".

### Note

---

#### **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.

---

## 9.2 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 "[9.2.1 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 "[9.2.2 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.

### Example

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 system configuration 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 "[9.2.1 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 Manager]

*Installation\_folder*\SVROR\Manager\etc\customize\_data

[Linux Manager]

/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 Manager]

*Installation\_folder*\SVROR\Manager\var\backup

[Linux Manager]

/var/opt/FJSVrcvmr/backup

For details, refer to "[9.2.2 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 necessary 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 C Manager Cluster Operation Settings and Deletion" in the "Setup Guide VE".

## 9.2.1 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 of the `rcxkeydefbackup` command, refer to "6.2 `rcxkeydefbackup`" in the "Reference Guide (Command) VE".

[Windows Manager]

`Installation_folder\SVROR\Manager\bin\rcxkeydefbackup`

[Linux Manager]

`/opt/FJSVrcvnr/bin/rcxkeydefbackup`

```
>rcxkeydefbackup [-dir directory] [[-immediate]][[-timeout value]] <RETURN>
```

Backup files are created in the specified folder, using the following format:

Format

[Windows Manager]

`Host_name_keydef_YYYYMMDD_HHMM.jar`

[Linux Manager]

`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 10 KB requires less than 1 MB. 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 of the scwbackup command, refer to "6.5 scwbackup" in the "Reference Guide (Command) VE".

[Windows Manager]

*Installation\_folder*\SVROR\Manager\bin\scwbackup

[Linux Manager]

/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 "6.1.1.7 Dynamic Disk Space" in the "Overview".

## 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 of the rcxbackup command, refer to "6.1 rcxbackup" in the "Reference Guide (Command) VE".

[Windows Manager]

*Installation\_folder*\SVROR\Manager\bin\rcxbackup

[Linux Manager]

/opt/FJSVrcvmr/bin/rcxbackup

```
>rcxbackup [-dir directory] [[-immediate]][-timeout value] <RETURN>
```

Backup files are created in the specified folder, using the following format:

Format

[Windows Manager]

*Host\_name\_YYYYMMDD\_HHMM.jar*

[Linux Manager]

*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 2 MB. 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.

## 9.2.2 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 of the `rcxbackup` command, refer to "6.1 `rcxbackup`" in the "Reference Guide (Command) VE".

[Windows Manager]

*Installation\_folder\SVROR\Manager\bin\rcxbackup*

[Linux Manager]

*/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.



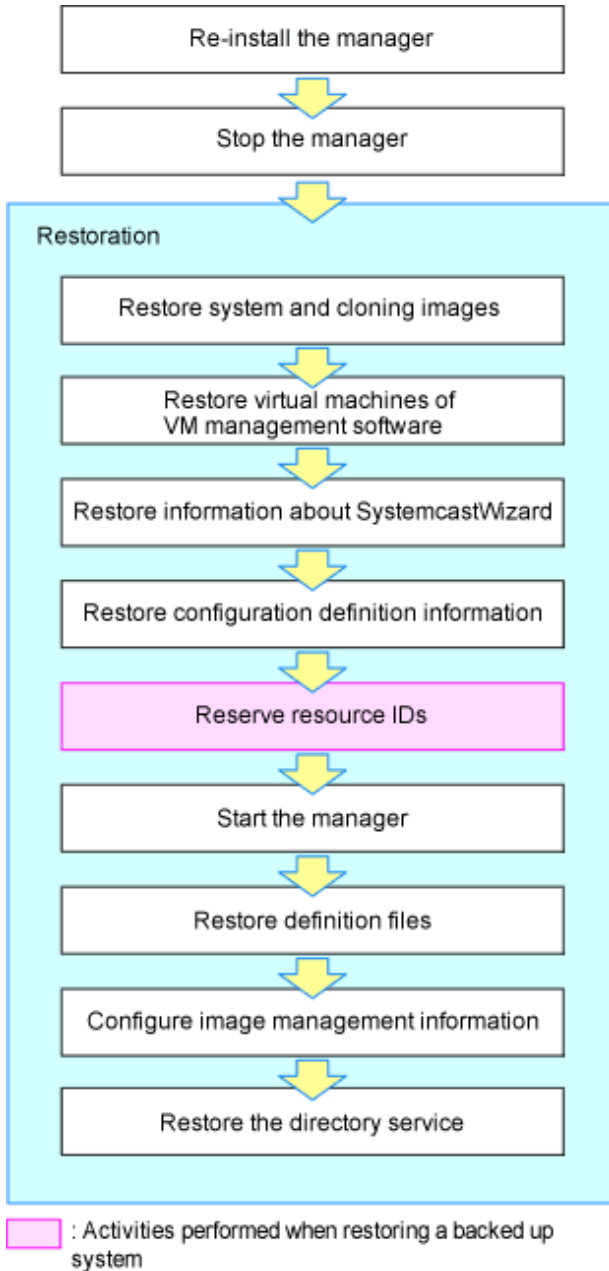
## 9.3 Restoration

---

This section explains how to restore the admin server.

Restore the admin server using the following procedure:

Figure 9.1 Flow of Admin Server Restoration



### 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 C Manager Cluster Operation Settings and Deletion" in the "Setup 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 "11.1.1 Preparations" in the "Setup Guide VE".

Stop the manager after re-installation.

For details on how to stop the manager, refer to ["2.1 Starting and Stopping Managers"](#).

- b. Execute the rcxkeydefrestore command to restore certificates, session encryption keys, definition files, and image management information.

For details of the rcxkeydefrestore command, refer to "6.3 rcxkeydefrestore" in the "Reference Guide (Command) VE".

[Windows Manager]

*Installation\_folder*\SVROR\Manager\bin\rcxkeydefrestore

[Linux Manager]

/opt/FJSVrcvmr/bin/rcxkeydefrestore

```
>rcxkeydefrestore -file filename <RETURN>
```

As 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 home directory contents 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 of the scwrestore command, refer to "6.6 scwrestore" in the "Reference Guide (Command) VE".

[Windows Manager]

*Installation\_folder*\SVROR\Manager\bin\scwrestore

[Linux Manager]

/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 ["9.2.2 Backing Up Configuration Definition Information"](#).

Execute the command shown below.

For details of the rcxrestore command, refer to "6.4 rcxrestore" in the "Reference Guide (Command) VE".

[Windows Manager]

*Installation\_folder*\SVROR\Manager\bin\rcxrestore

[Linux Manager]

/opt/FJSVrcvmr/bin/rcxrestore

```
>rcxrestore -file filename <RETURN>
```

## Note

Specify the command using an absolute path.

### 5. Starting the manager

For details on how to start the manager, refer to ["2.1 Starting and Stopping Managers"](#).

### 6. 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.

When operating Active Directory using the Single Sign-On function of ServerView Operations Manager in a redundancy configuration, and when restoring by reinstalling Resource Orchestrator, reconfigure the settings using Active Directory in the redundant configuration.

For details on configurations, refer to ["Appendix F Migration Procedure when Using Active Directory with a Redundant Configuration"](#) in the ["Setup Guide VE"](#).

## 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 C Manager Cluster Operation Settings and Deletion"](#) in the ["Setup 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
      - Replacement of the NIC of a managed server
      - LAN connections between managed servers and LAN switch blades
    - Snapshot collection
      - Server switchover or takeover (\*)
    - When backing up of configuration definition information again is necessary
- \* Note: 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 restoration. 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 "[2.2 Starting and Stopping Agents](#)"
- LAN switches registered using LAN switch discovery, and the link information of those switches, cannot be backed up.

After registering the LAN switch, acquire the link information.

For details on how to register LAN switches, refer to "7.11 Registering LAN Switches" in the "User's Guide VE".

For details on how to acquire the link information, refer to "13.4 Advisory Notes" in the "User's Guide VE".

- VIOM and ISM coordination user names and passwords cannot be backed up. Register VIOM and ISM coordination before performing restoration. For details on operation methods, refer to "7.1 Registering VIOM/ISM Coordination" in the "User's Guide VE".



# Chapter 10 Backing Up and Restoring Image Files

This chapter 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.

## 10.1 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 Manager]

```
"Installation_folder"\SVROR\ScwPro\depot\Cloneimg
```

[Linux Manager]

```
/var/opt/FJSVscw-deploysv/depot/CLONEIMG
```

- When the image files storage destination is changed after installation, using the rcxadm imagemgr command

[Windows Manager]

```
"Specified_folder"\Cloneimg
```

[Linux Manager]

```
"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. File

The following two files are stored in each resource folder for system images and cloning images.

- diskimg.fc2
- diskimg.ini

## 10.2 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. Stopping the manager

For details on how to stop the manager, refer to "[2.1 Starting and Stopping Managers](#)".



Confirm whether both the "Manager Services" and "Related Services" have been stopped.

### 3. Back Up Image Files

Copy the resource folders corresponding to the items confirmed in step 1.

The backup 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 backup operation of image files should be performed for each resource folder.

Starting the manager

For details on how to start the manager, refer to "[2.1 Starting and Stopping Managers](#)".



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.

## 10.3 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 "6.2.7 Configuring BIOS Settings of Managed Servers" in the "Design 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. Stopping the manager

For details on how to stop the manager, refer to "2.1 Starting and Stopping Managers".



#### Note

Confirm whether both the "Manager Services" and "Related Services" have been stopped.

#### 4. Restore 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. Starting the manager

For details on how to start the manager, refer to "2.1 Starting and Stopping Managers".



#### 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.

# Part 4 Monitoring

---

---

Chapter 11 Monitoring Resources.....	69
Chapter 12 Collecting Power Consumption Data and Displaying Graphs.....	75



# Chapter 11 Monitoring Resources

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

## 11.1 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

Resource Orchestrator can centrally monitor the configuration and status of servers and other managed resources (Chassis, servers, L2 switches, LAN switch blades, network devices, physical OSs, VM hosts and guests, power monitoring devices, etc.) directly from the ROR console.

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 11.1 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 blade	Yes	Yes
Network device	Yes	No
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 11.2 List of Regularly Updated Resources and Their Related Resources

Resources Subject to Regular Update	Related Resources	Data Source
Chassis	Chassis	Server management unit
Server	Server Physical OS VM host (*1) VM guest (*1)	ServerView Agents (*2) Server management unit Server virtualization software
LAN switch blade	LAN switch blade	LAN switch blade Server management unit (*3)
Network device	L2 switch Ethernet Fabric Firewall Server load balancer Management host	L2 switch Ethernet Fabric Firewall Server load balancer Management host
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.

## 11.2 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 11.3 Resource Icons


Icon	Meaning
	Server resource
	Chassis
	Server
	Physical OS
	VM host
	Guest domain of OVM for SPARC registered as a VM host
	VM guest
	LAN switch blade L2 switch
	Management Host
	Ethernet Fabric
	VFAB
	Firewall
	Server load balancer
	Integrated network device
	Power monitoring device (*)
	PDU (*)
	UPS (*)
	Management software

\* Note: 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 11.4 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.	Action must be taken
	unknown	Unknown The status of the resource cannot be obtained. (*1, *2)	Action must be taken
	stop	Stop The resource has stopped and cannot be used.	No action is necessary

Icon	Status	Meaning	Corrective Action
	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 VM guest is in "unknown" status, check the operation status of the VM host on which the VM guest is running.

\*2: When a network device is in "unknown" status, check the physical connection between the network device and admin LAN as well as the operation status of the network device.

### 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.
- For LAN switch blades operating in Converged Fabric mode, or LAN switch blade PY CB 10Gb FEX Nexus B22, statuses are not be obtained from LAN switch blades using SNMP. Therefore, "unknown" status is not detected.

Table 11.5 Physical Server Icons



Icon	Meaning
	Spare server
	Server in maintenance mode

Table 11.6 OS Icons
















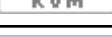

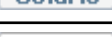

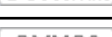

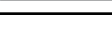
Icon (Tree)	Icon (List)	Meaning
		Windows OS
		Linux OS
		Solaris OS
		VMware host OS
		Hyper-V host OS
		Citrix XenServer host OS
		Linux Xen host OS
		KVM host OS
		Solaris Zone host OS
		OVM for SPARC host OS
		Host OS of OVM for x86

Table 11.7 Relations between Network Device Unit Status and Maintenance Mode (An Example of the Ethernet Fabric)

Unit Status	Maintenance Mode (active)	Maintenance Mode (maintenance)
normal	#	🟡 #
warning	⚠️ #	🟡 ⚠️ #
unknown		
error	-: (Not supported)	🟡 🚫

### 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 "9.2.2 Functional Differences between Products" in the "Design Guide VE".
- For LAN switch blades, "error", "fatal", "warning", "normal", or "unknown" is displayed.
- For LAN switches, "normal", "warning", or "unknown" is displayed.
 

However, when the network device management function is enabled, "normal", "warning", "unknown", or "error" is displayed.  
For details on enabling the network device management function, refer to "7.5.1 Enabling the Network Device Management Function" in the "User's Guide VE".
- For network devices, "normal", "warning", "unknown", or "error" is displayed.

## 11.3 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 "11.2 Resource Status" and "A.3 Status Panel" in 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 OSs, 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 "[4.2 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 "[6.3.2 Replacing Servers](#)".

#### 5. Perform Post-recovery Verification

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

# Chapter 12 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.

## 12.1 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 " $\theta$ ", 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.

## 12.2 Exporting Power Consumption Data

For details of how to export power consumption data, refer to "19.1 Exporting Power Consumption Data" in the "User's Guide VE".

## 12.3 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.

## 12.4 Displaying Power Consumption Data Graphs

For details of how to display graphs of power consumption data, refer to "19.2 Displaying Power Consumption Data Graphs" in the "User's Guide VE".



# Part 5 Modifying

---

---

<a href="#">Chapter 13 Changing Settings</a> .....	78
--	----

# Chapter 13 Changing Settings

This chapter explains how to change settings.

## 13.1 When Configuring Single Sign-On

This section explains how to reconfigure Single Sign-On.

### 13.1.1 Reconfiguration Procedure

If you cannot log in to the ROR console after installation, the environment setup may have failed. Stop the manager and then reconfigure the environment.

#### 13.1.1.1 Confirming Certificates

Check the CA Certificate registered with Resource Orchestrator using the following procedure.

1. Execute the following command:

```
rcxadm authctl diffcert<RETURN>
```

The difference of the CA certificate (keystore) of ServerView Operations Manager and the registered CA certificate (keystore) of Resource Orchestrator is displayed.

2. Check the displayed difference information.

The information is displayed as follows:

```
svs_cms  
ldaphost.fujitsu.com
```

When difference is displayed, registration of a CA certificate (keystore) may have failed. In this case, register the CA certificate referring to "[13.1.1.2 Registering Certificates](#)".

#### 13.1.1.2 Registering Certificates

Use the following procedure to register CA certificates to Resource Orchestrator.

1. Check the content of the CA certificate for updating.

Refer to "[13.1.1.1 Confirming Certificates](#)", and check the content of the CA certificate to update.

2. Update the CA certificate.

Execute the following command:

```
rcxadm authctl refreshcert -alias alias<RETURN>
```

Specify the alias of the certificate displayed by executing "Confirming Certificates" as *alias*.

When importing two or more certificates to Resource Orchestrator, repeat this procedure for each certificate.



.....  
If the root certificate has been registered in the CA certificate (keystore) of ServerView Operations Manager, import a root certificate to Resource Orchestrator.  
.....

3. Check the difference of the CA certificate.

Perform step 1 again, and check that the updated certificate is not displayed.

### 13.1.1.3 Checking Directory Service Connection Information

Check if the connection information of the directory service to be used has been correctly registered in Resource Orchestrator.

1. Execute the following command:

```
rcxadm authctl show <RETURN>
```

The connection information registered in Resource Orchestrator is displayed.

2. Check the displayed connection information.

The information is displayed as follows:

```
host: hostx.fujitsu.com
port: 1474
base: dc=fujitsu,dc=com
bind: cn=Directory Manager
method: SSL
```

Check if the directory service settings and the displayed connection information are the same. In particular, note the following information:

- If port is the port for SSL communications
- If bind is the directory service administrator

(Check if the administrator is a directory service administrator, not a privileged user of Resource Orchestrator)

For details on how to check the connection settings of the directory service provided with ServerView Operations Manager, refer to the following manual.

- ServerView Operations Manager V7.0 or earlier  
"ServerView user management with OpenDJ" in "User Management in ServerView 6.30"
- ServerView Operations Manager V7.1 or later  
"ServerView user management with Apache DS" in "User Management in ServerView 7.10"

3. When there is an error in the connection information, use the following procedure to register the correct information:
  - a. Stop the manager.
  - b. Execute the `rcxadm authctl sync` command and configure the correct connection information.
  - c. Start the manager.

For details on the `rcxadm authctl` command, refer to "5.3 `rcxadm authctl`" in the "Reference Guide (Command) VE".

## 13.1.2 Modifying Directory Service Connection Information

---

When a directory server's coordinator name (connected user name), a password, etc. have been changed, use the following procedure to reconfigure Single Sign-On.

1. Change the settings for the directory service of ServerView Operations Manager.

For details on how to change the directory service settings of ServerView Operations Manager, refer to the manuals of ServerView Operations Manager.

- "Configuring directory service access" in "ServerView Suite User Management in ServerView"

2. Refer to "[13.1.1.1 Confirming Certificates](#)" and check whether the CA certificate of ServerView Operations Manager has been imported correctly to the Resource Orchestrator keystore.
3. When the certificate has not been imported to the keystore, refer to "[13.1.1.2 Registering Certificates](#)" and register a certificate.
4. Execute the `rcxadm authctl sync` command and change the directory service connection information. For details on the `rcxadm authctl sync` command, refer to "5.3 `rcxadm authctl`" in the "Reference Guide (Command) VE".

### **13.1.3 When Certificates Have Expired**

---

When the CA certificate of ServerView Operations Manager or the directory server has expired, re-register the CA certificates after obtaining new certificates. For details on how to register the CA certificates, refer to "[13.1.1.2 Registering Certificates](#)".

# 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 "9.3 Server Switchover Conditions" in the "Setup Guide VE".
- Auto-Recovery cannot be performed if maintenance mode has not been released.  
Ensure maintenance mode is released once maintenance operations are complete.
- When performing server switchover using the profile switchover method, it is necessary to use VIOM or ISM to assign a virtual MAC address to the NIC of the managed server that will be used to connect to the admin LAN.
- 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.

## [OVM for SPARC]

- The status of an OVM for SPARC environment after switchover is as shown below.
  - When performing switchover for OVM for SPARC, start all domains after switchover.
  - When using the guest domain as the Solaris Zone, the non-global zone is powered on according to the auto-boot? configuration.
  - For switchover, the primary server is shut down using the poweroff command of the service processor (XSCF). When configuring the IO domain, configure the shutdown group of each domain giving consideration to the stopping order.
  - When the number of guest domains in an OVM for SPARC environment is increased, the time necessary for power operations of SPARC M10-4S/M12-2S is also increased. Perform power operations using the actual system to estimate the timeout value based on the actual measured values. For details on how to modify the timeout value, refer to "6.1.5 Setting Values for SPARC Enterprise M4000/M5000/M8000/M9000 and SPARC M10-4S/M12-2S" in the "Design Guide VE".
  - In OVM for SPARC server switchover, only the boot-device OBP settings are taken over to the SPARC M10-4S/M12-2S that is the switchover destination. The other OBP settings return to the default values.
  - When performing server switchover on OVM for SPARC, configure off for Autoboot (Guest Domain) of the physical partition operation mode on XSCF in the spare server.
  - During server switchover, configure the same domain configuration for the spare server as the factory default. When configuring the spare server on OVM for SPARC, perform the following operations before switchover.
    - Save the configuration information of the spare server in an XML file
    - Record the OBP settings of the control domain and the IO domain

For details on how to save and restore the domain configuration, refer to the "Oracle VM Server for SPARC Administration Guide" provided by Oracle.

## 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
- Collection and deployment of cloning images
- Server switchover and fallback

## 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 details on how to delete servers, refer to "11.2 Deleting Managed Servers" in 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 "11.2 Deleting Managed Servers" in 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.

For details on how to restart the manager, refer to "2.1 Starting and Stopping Managers".

## Restarting Managers

By default, the manager services restart at 3:45 am every day for stable system operation.

The settings for restarting can be changed depending on the authority level. To change the configuration, perform the following:

- Settings file

[Windows Manager]

*Installation\_folder*\SVROR\Manager\rails\config\rcx\rcx\_manager\_params.rb

[Linux Manager]

/opt/FJSVrcvnr/rails/config/rcx/rcx\_manager\_params.rb

- Configuration Parameters

Table A.1 Configuration Parameters

Parameter	Meaning	Initial Value
RESTART_ENABLE	Select the restart operation status. Specify one of the following: - When restarting	true

Parameter	Meaning	Initial Value
	Specify "true". - When not restarting Specify "false".	
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 "[2.1 Starting and Stopping Managers](#)".



**Note**

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.

For the stable operation of systems, configure the restarting of managers to occur on a daily basis.

When upgrading managers, check the setting details in advance, and re-set them after the upgrade is complete.

## Changing Multiple Operations of Managers

When executing multiple operations simultaneously, the upper limit is set for the number of simultaneous operations.

The upper limit of the number of simultaneous operations can be changed depending on the usage environment. To change the configuration, edit the following definition file.

When there is no definition file, create one.

### Placeholder for the Definition File

[Linux Manager]

/etc/opt/FJSVrcvnr/customize\_data

[Windows Manager]

Installation\_folder\SVROR\Manager\etc\customize\_data

### Definition File Name

rcx\_base.rcxprop

### Format of the Definition File

Describe the definition file in individual lines as below:

<i>Key = Value</i>
--------------------

### Items in the Definition File

Specify the following items.

Table A.2 Items in the Definition File

Items	Key	Value	Remarks
Multiplicity	TASK_WORKER_COUNT	Specify the multiplicity from 5 - 30.	The initial value is "5".

Items	Key	Value	Remarks
			Operates by default, when there are no definition files.

### Example of the Definition File

An example definition file is indicated below. In this example, the multiplicity is set to "10".

```
TASK_WORKER_COUNT=10
```

### Changing Procedures of Definition Files

- When the manager is operating in a normal environment
  1. Stop the manager.
  2. Change the TASK\_WORKER\_COUNT value in the rcx\_base.rcxprop file.  
When there is no rcx\_base.rcxprop file, create one.
  3. Restart the manager.

- When the manager is operating in a cluster environment

[Windows Manager]

1. Stop the manager.
2. Place the shared disk of the manager online. Place other cluster resources offline.
3. Change the TASK\_WORKER\_COUNT values for rcx\_base.rcxprop files on the shared disk.  
When there is no rcx\_base.rcxprop file, create one.

Placeholder for the Definition File

*Drive\_name\Fujitsu\ROR\SVROR\customize\_data\rcx\_base.rcxprop*

4. Restart the manager.

[Linux Manager]

1. Stop the manager.
2. Mount the shared disk of the admin server on the primary node or the secondary node.
3. Change the TASK\_WORKER\_COUNT values for rcx\_base.rcxprop files in the shared disk.  
When there is no rcx\_base.rcxprop file, create one.

Placeholder for the Definition File

*Destination\_to\_mount\_shared\_disk/Fujitsu/ROR/SVROR/etc/opt/FJSVrcvmr/customize\_data/rcx\_base.rcxprop*

4. Unmount the shared disk for the admin server from the node mounted in step 2.
5. Restart the manager.

For details on how to start and stop the manager, refer to "[2.1 Starting and Stopping Managers](#)".



### 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 using the values in the table and the memory size required for the manager operations described in "6.1.1.8 Memory Size" in the "Overview", and then add memory if necessary.

**Table A.3 Increased Memory Use with Multiple Operations**

Multiplicity	Increase in Memory Use (in MB)
5	-



Multiplicity	Increase in Memory Use (in MB)
6 - 14	1080 + ( <i>Multiplicity</i> * 40)
15 - 30	2104 + ( <i>Multiplicity</i> * 40)

## Modification of Extended Partitioning Mode when Using the PRIMEQUEST 2000 Series

When modifying Extended Partitioning Mode of the partition on which the business server/host operate when using PRIMEQUEST 2000 series, re-register the partition used in the following procedure with Resource Orchestrator.

- When the currently used partition is a PPAR partition, and when using an Extended Partition with "Enable" configured for PPAR [Extended Partitioning Mode]
  1. Delete the relevant managed server in the server tree.  
For information on deleting managed servers, refer to "11.2 Deleting Managed Servers" in the "User's Guide VE".
  2. Modify the settings of [Extended Partitioning Mode] from the management console of the PRIMEQUEST MMB.  
For details on how to modify Extended Partitioning Mode, refer to the operation management manuals for the PRIMEQUEST 2000 series.
  3. Register the relevant Extended Partition in the server tree.  
For details on how to register managed servers, refer to "7.6.2 Registering PRIMEQUEST Servers" in the "User's Guide VE".
- When the currently used partition is an Extended Partition, and when using an Extended Partition with "Disable" configured for PPAR [Extended Partitioning Mode]
  1. Delete the relevant managed server in the server tree.  
For information on deleting managed servers, refer to "11.2 Deleting Managed Servers" in the "User's Guide VE".
  2. Modify the settings of [Extended Partitioning Mode] from the management console of the PRIMEQUEST MMB.  
For details on how to modify Extended Partitioning Mode, refer to the operation management manuals for the PRIMEQUEST 2000 series.
  3. Register the relevant PPAR partition in the server tree.  
For details on how to register managed servers, refer to "7.6.2 Registering PRIMEQUEST Servers" in the "User's Guide VE".

## Modification of PPAR Extended Partition Configurations when Using the PRIMEQUEST 2000 Series

When modifying PPAR Extended Partition configurations of the partition on which the business server/host operate when using PRIMEQUEST 2000 series, re-register the partition used in the following procedure with Resource Orchestrator.

1. Delete the relevant managed server in the server tree.  
For information on deleting managed servers, refer to "11.2 Deleting Managed Servers" in the "User's Guide VE".
2. Modify the settings of "Partition Configuration" from the management console of the PRIMEQUEST MMB.  
For details on how to modify the PRIMEQUEST 2000 series, refer to the operation management manuals for the PRIMEQUEST 2000 series.
3. Register the relevant Extended Partition in the server tree.  
For details on how to register managed servers, refer to "7.6.2 Registering PRIMEQUEST Servers" in the "User's Guide VE".

## Modification of Building Block Configurations when Using SPARC M10-4S/M12-2S

When modifying a building block configuration when using SPARC M10-4S/M12-2S, use the following procedure to re-register the partition with Resource Orchestrator.

1. Delete the relevant managed server in the server tree.  
For information on deleting managed servers, refer to "11.2 Deleting Managed Servers" in the "User's Guide VE".

2. Modify the settings of the building block configuration.

For details on modifying building block configurations, refer to the following manuals:

- For SPARC M12

Refer to the "Fujitsu SPARC M12-2S Installation Guide".

- For SPARC M10

Refer to the "Fujitsu M10-4S/SPARC M10-4S Installation Guide".

3. Register the relevant managed server in the server tree.

For details on registering managed servers, refer to "Registering Chassis (SPARC Enterprise M4000/M5000/M8000/M9000) or SPARC M10-4S/M12-2S in the "User's Guide VE".

## Changing Monitoring Timeout Values of Physical Server Power Operations

The time elapsed from the start to finish of a power operation of a physical server may exceed the timeout value for power operations. Therefore, perform power operations using the actual system to estimate the timeout value based on the actual measured values.

In the definition files, timeout values are specified for different server models. As a result, changes in the timeout values for each model of server managed by the manager are reflected on the manager.

When changing a timeout value, create the following definition file.

### Placeholder for the Definition File

[Windows Manager]

*Installation\_folder*\SVROR\Manager\etc\customize\_data

[Linux Manager]

/etc/opt/FJSVrcvmr/customize\_data

### Definition File Name

power\_timeout.rcxprop

### Format of the Definition File

In the definition file, each line contains configuration information for a model of server (model name, timeout values for powering the server on, rebooting it, powering it off, etc.), separated using commas (","). Each line is exported in the following format.

<i>model,boot_timeout,shutdown_timeout</i>
--

- Any blank spaces before or after the commas are ignored.
- When adding comments, start the line with a number sign ("#").

### Items in the Definition File

Specify the following items.

#### model

Describe the model name of the server to modify the timeout value for.

The value is displayed in [General]-[Model name] of the [Resource Details] tab in the [ROR Console]

For SPARC M10-4S, enter "M10-4S".

#### boot\_timeout

Describe the timeout value of powering on and rebooting the server.

This value is also used for as the timeout value when starting or rebooting a managed server in image operations.

Specify a value in seconds using an integer greater than 0.

If any other value is specified, the default timeout value is used.

## Point

A timeout value of less than 5940 seconds is recommended.

Table A.4 Default Timeout Values (boot\_timeout)

Model	Powering On or Rebooting (in Seconds)	Image Operation	
		Start (in Seconds)	Reboot (in Seconds)
RX4770 M1 or later	5700	5700	5700
SPARC M10-1/M10-4/ M12-1/M12-2	1800	(*)	(*)
SPARC M10-4S/M12-2S	2700	(*)	(*)
PRIMEQUEST 2000 series	900	3600	3600
Other models	900	900	1800

\* Note: Image operations of SPARC M10/M12 model servers are not supported.

### shutdown\_timeout

Specify the timeout value for powering off of the server.

Specify a value in seconds using an integer greater than 0.

If any other value is specified, the default timeout value is used.

Table A.5 Default Timeout Values (shutdown\_timeout)

Model	Power the Server Off (in Seconds)
SPARC M10-1/M10-4/ M12-1/M12-2	900
SPARC M10-4S/M12-2S	1200
Other models	900

## Example

```
PRIMERGY RX4770 M2,5700,900
```

### Changing Procedures of Definition Files

It is not necessary to restart the manager after creating or modifying a definition file. Changes are reflected on the manager after the definition file is changed.