ServerView Resource Orchestrator Virtual Edition V3.1.0

Operation Guide

Windows/Linux
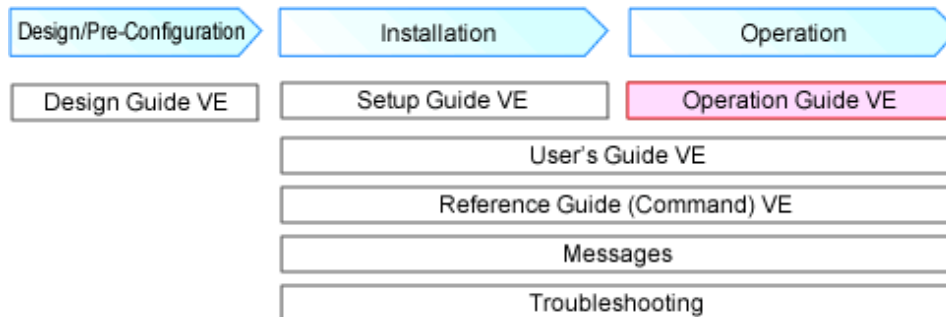
Preface

Resource Orchestrator Documentation Road Map

The documentation road map for Resource Orchestrator is as shown below.

Resource Orchestrator Documentation Road Map

For information about the documents for Resource Orchestrator, refer to "Chapter 1 Documentation Road Map" in the "Design Guide VE".

Purpose

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

Target Readers

This manual is written for people who will operate Resource Orchestrator.
An overview of the functions provided in Resource Orchestrator can be found in "Chapter 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 Overview of Resource Management" in the "User's Guide VE".

Organization

This manual is composed as follows:

Section 1 Overview

Chapter 1 Overview of Operations, Maintenance, and Monitoring

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

Section 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.

Section 3 Maintenance

Section 4 Monitoring

Notational Conventions

The notation in this manual conforms to the following conventions.

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

[Windows Manager]	Sections related to Windows manager
[Linux Manager]	Sections related to Linux manager
[Windows]	Sections related to Windows (When not using Hyper-V)
[Linux]	Sections related to Linux
[Red Hat Enterprise Linux]	Sections related to Red Hat Enterprise Linux
[Solaris]	Sections related to Solaris or Solaris Containers
[VMware]	Sections related to VMware
[Hyper-V]	Sections related to Hyper-V
[Xen]	Sections related to Xen
[KVM]	Sections related to RHEL-KVM
[Solaris Containers]	Sections related to Solaris containers

[Physical Servers]	Sections related to physical servers
[VM host]	Sections related to VMware, Windows Server 2008 with Hyper-V enabled, Xen, RHEL-KVM, and Solaris containers

- Unless specified otherwise, the blade servers mentioned in this manual refer to PRIMERGY BX servers.

- Oracle Solaris may also be indicated as Solaris, Solaris Operating System, or Solaris OS.

- References and character strings or values requiring emphasis are indicated using double quotes (").

- Window names, dialog names, menu names, and tab names are shown enclosed by brackets ([ ]).

- Button names are shown enclosed by angle brackets (< >) or square brackets ([ ]).

- The order of selecting menus is indicated using [ ]-[ ].

- Text to be entered by the user is indicated using bold text.

- Variables are indicated using italic text and underscores.

- The ellipses ("...") in menu names, indicating settings and operation window startup, are not shown.

- The ">" used in Windows is included in usage examples. When using Linux, read ">" as meaning "#".

- The URLs in this manual were correct when the manual was written.

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.

When using Windows 64-bit (x64)

C:\Program Files (x86)\Resource Orchestrator

When using Windows 32-bit (x86)

C:\Program Files\Resource Orchestrator

Abbreviations

The following abbreviations are used in this manual:

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

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

Abbreviation	Products
	Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (for Intel64) Red Hat(R) Enterprise Linux(R) 6 (for x86) Red Hat(R) Enterprise Linux(R) 6 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.1 (for x86) Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64) SUSE(R) Linux Enterprise Server 10 Service Pack2 for x86 SUSE(R) Linux Enterprise Server 10 Service Pack2 for EM64T SUSE(R) Linux Enterprise Server 10 Service Pack3 for x86 SUSE(R) Linux Enterprise Server 10 Service Pack3 for EM64T SUSE(R) Linux Enterprise Server 11 for x86 SUSE(R) Linux Enterprise Server 11 for EM64T SUSE(R) Linux Enterprise Server 11 Service Pack1 for x86 SUSE(R) Linux Enterprise Server 11 Service Pack1 for EM64T Oracle Enterprise Linux Release 5 Update 4 for x86 (32 Bit) Oracle Enterprise Linux Release 5 Update 4 for x86_64 (64 Bit) Oracle Enterprise Linux Release 5 Update 5 for x86 (32 Bit) Oracle Enterprise Linux Release 5 Update 5 for x86_64 (64 Bit)
Red Hat Enterprise Linux	Red Hat(R) Enterprise Linux(R) AS (v.4 for x86) Red Hat(R) Enterprise Linux(R) ES (v.4 for x86) Red Hat(R) Enterprise Linux(R) AS (v.4 for EM64T) Red Hat(R) Enterprise Linux(R) ES (v.4 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.5 for x86) Red Hat(R) Enterprise Linux(R) ES (4.5 for x86) Red Hat(R) Enterprise Linux(R) AS (4.5 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.5 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.6 for x86) Red Hat(R) Enterprise Linux(R) ES (4.6 for x86) Red Hat(R) Enterprise Linux(R) AS (4.6 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.6 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.7 for x86) Red Hat(R) Enterprise Linux(R) ES (4.7 for x86) Red Hat(R) Enterprise Linux(R) AS (4.7 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.7 for EM64T) Red Hat(R) Enterprise Linux(R) AS (4.8 for x86) Red Hat(R) Enterprise Linux(R) ES (4.8 for x86) Red Hat(R) Enterprise Linux(R) AS (4.8 for EM64T) Red Hat(R) Enterprise Linux(R) ES (4.8 for EM64T) Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86)

Abbreviation	Products
	Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (for Intel64) Red Hat(R) Enterprise Linux(R) 6 (for x86) Red Hat(R) Enterprise Linux(R) 6 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.1 (for x86) Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)
Red Hat Enterprise Linux 5	Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.1 (for x86) Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.2 (for x86) Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.8 (for x86) Red Hat(R) Enterprise Linux(R) 5.8 (for Intel64)
Red Hat Enterprise Linux 6	Red Hat(R) Enterprise Linux(R) 6 (for x86) Red Hat(R) Enterprise Linux(R) 6 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.1 (for x86) Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64)
RHEL-KVM	Red Hat(R) Enterprise Linux(R) 6.1 (for x86) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64) Virtual Machine Function
Xen	Citrix XenServer(TM) 5.5 Citrix Essentials(TM) for XenServer 5.5, Enterprise Edition Citrix XenServer(TM) 6.0 Citrix Essentials(TM) for XenServer 6.0, Enterprise Edition Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Linux Virtual Machine Function

Abbreviation	Products
	Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.8 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.8 (for Intel64) Linux Virtual Machine Function
XenServer 6	Citrix XenServer(TM) 6.0 Citrix Essentials(TM) for XenServer 6.0, Enterprise Edition
DOS	Microsoft(R) MS-DOS(R) operating system, DR DOS(R)
SUSE Linux Enterprise Server	SUSE(R) Linux Enterprise Server 10 Service Pack2 for x86 SUSE(R) Linux Enterprise Server 10 Service Pack2 for EM64T SUSE(R) Linux Enterprise Server 10 Service Pack3 for x86 SUSE(R) Linux Enterprise Server 10 Service Pack3 for EM64T SUSE(R) Linux Enterprise Server 11 for x86 SUSE(R) Linux Enterprise Server 11 for EM64T SUSE(R) Linux Enterprise Server 11 Service Pack1 for x86 SUSE(R) Linux Enterprise Server 11 Service Pack1 for EM64T
Oracle Enterprise Linux	Oracle Enterprise Linux Release 5 Update 4 for x86 (32 Bit) Oracle Enterprise Linux Release 5 Update 4 for x86_64 (64 Bit) Oracle Enterprise Linux Release 5 Update 5 for x86 (32 Bit) Oracle Enterprise Linux Release 5 Update 5 for x86_64 (64 Bit)
Solaris	Solaris(TM) 10 Operating System
SCVMM	System Center Virtual Machine Manager 2008 R2 System Center 2012 Virtual Machine Manager
VMware	VMware(R) Infrastructure 3 VMware vSphere(R) 4 VMware vSphere(R) 4.1 VMware vSphere(R) 5
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 Infrastructure 3	VMware(R) Infrastructure 3
VMware Infrastructure Client	VMware(R) Infrastructure Client
VMware vSphere 4.0	VMware vSphere(R) 4.0
VMware vSphere 4.1	VMware vSphere(R) 4.1
VMware vSphere 5	VMware vSphere(R) 5
VMware vSphere Client	VMware vSphere(R) Client
VMware vCenter Server	VMware(R) vCenter(TM) Server
VMware vClient	VMware(R) vClient(TM)
VIOM	ServerView Virtual-IO Manager
BladeLogic	BMC BladeLogic Server Automation
ServerView Agent	ServerView SNMP Agents for MS Windows (32bit-64bit) ServerView Agents Linux ServerView Agents VMware for VMware ESX Server

Abbreviation	Products
Excel	Microsoft(R) Office Excel(R) 2010 Microsoft(R) Office Excel(R) 2007 Microsoft(R) Office Excel(R) 2003
Excel 2010	Microsoft(R) Office Excel(R) 2010
Excel 2007	Microsoft(R) Office Excel(R) 2007
Excel 2003	Microsoft(R) Office Excel(R) 2003
RCVE	ServerView Resource Coordinator VE
ROR	ServerView Resource Orchestrator
ROR VE	ServerView Resource Orchestrator Virtual Edition
ROR CE	ServerView Resource Orchestrator Cloud Edition
Resource Coordinator	Systemwalker Resource Coordinator
Resource Coordinator VE	ServerView Resource Coordinator VE Systemwalker Resource Coordinator Virtual server Edition
Resource Orchestrator	ServerView Resource Orchestrator

Export Administration Regulation Declaration

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

Trademark Information

- BMC, BMC Software, the BMC logos, and other BMC marks are trademarks or registered trademarks of BMC Software, Inc. in the U.S. and/or certain other countries.

- Citrix(R), Citrix XenServer(TM), Citrix Essentials(TM), and Citrix StorageLink(TM) are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

- Dell is a registered trademark of Dell Computer Corp.

- HP is a registered trademark of Hewlett-Packard Company.

- IBM is a registered trademark or trademark of International Business Machines Corporation in the U.S.

- Linux is a trademark or registered trademark of Linus Torvalds in the United States and other countries.

- Microsoft, Windows, MS, MS-DOS, Windows XP, Windows Server, Windows Vista, Windows 7, Excel, Active Directory, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

- Oracle and Java are registered trademarks of Oracle and/or its affiliates in the United States and other countries.

- Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

- Red Hat, RPM and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.

- Spectrum is a trademark or registered trademark of Computer Associates International, Inc. and/or its subsidiaries.

- SUSE is a registered trademark of SUSE LINUX AG, a Novell business.

- VMware, the VMware "boxes" logo and design, Virtual SMP, and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

- ServerView and Systemwalker are registered trademarks of FUJITSU LIMITED.

- All other brand and product names are trademarks or registered trademarks of their respective owners.

Notices

- The contents of this manual shall not be reproduced without express written permission from FUJITSU LIMITED.

- The contents of this manual are subject to change without notice.

Month/Year Issued, Edition	Manual Code
November 2011, First Edition	J2X1-7605-01ENZ0(00)
December 2011, 1.1	J2X1-7605-01ENZ0(01)
December 2011, 1.2	J2X1-7605-01ENZ0(02)
February 2012, 1.3	J2X1-7605-01ENZ0(03)
March 2012, 1.4	J2X1-7605-01ENZ0(04)
April 2012, 1.5	J2X1-7605-01ENZ0(05)
July 2012, 2	J2X1-7605-02ENZ0(00)
October 2012, Third Edition	J2X1-7605-03ENZ0(00)

Contents

Part 1   Overview

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

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 the Manager" and "2.2 Starting and Stopping an Agent".

Note

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

Managed servers will not boot up properly if they are started before the manager. Make sure that the manager is running before starting managed servers.
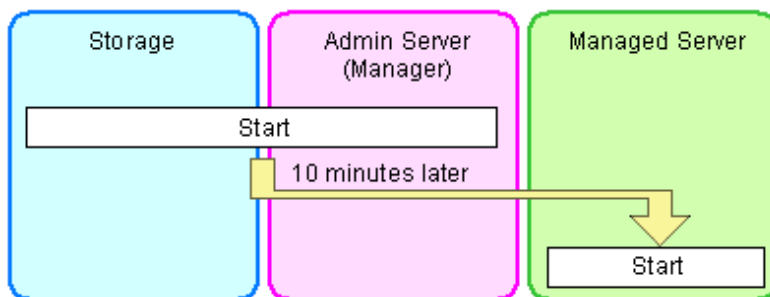
Additionally, when using the HBA address rename function, the HBA address rename setup service should be started on a dedicated server (HBA address rename server) and left running continuously. For details on starting, stopping, and confirming the state of the HBA address rename setup service, refer to "Chapter 6 Settings for the HBA address rename Setup Service" in the "Setup Guide VE".

2.1 Starting and Stopping the Manager

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 Orchestrator Sub Web Server (Mongrel)
    Resource Orchestrator 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
  scwtftpd
  dhcpd (*)

  * 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 scwtftpd status <RETURN>
# service dhcpd 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 "Appendix B 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 an Agent

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>

To check the running state of the service of Systemwalker SQC DCM, execute the following command:

```
# /etc/rc0.d/K00ssqcdcm <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.

  Starting an L-Server

```
# /etc/init.d/scwagent start <RETURN>
# /etc/rc2.d/S99ssqcdcm start <RETURN>
```

  Stop

```
# /etc/init.d/scwagent stop <RETURN>
# /etc/rc0.d/K00ssqcdcm stop <RETURN>
```

[Solaris]
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 Server Switchover Settings" in the "User's Guide VE".

Note

- When the switchover method is backup and restore

  When backing up or restoring system images, or collecting and deploying cloning images, up to four processes can be executed simultaneously. If four processes are already being executed, any system image restore triggered by a switchover or failback operation will enter a standby state.
  Any process put under standby state will be resumed after one of the already running processes completes.

- When the MAK method is used for license authentication

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

- 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 "Note" in "2.5 Hardware Environment" in the "Design Guide VE".

Note

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

- During switchover, server restarts and configuration changes may trigger SNMP Traps (which are shown in the Event Log).
  For details, refer to "Section 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.

- 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. [VMware] [Hyper-V]

- After shutting down a spare server, if the power is not turned off within 15 minutes, the spare server will be forcibly powered off.

Auto-Recovery

- For PRIMERGY BX servers and PRIMEQUEST

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

- For rack mount, tower servers, and SPARC Enterprise

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

For the decision criteria for whether an OS has stopped, refer to "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 <OK>.

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

🕭 Note

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

- Manual switchover can be performed regardless of the status of the primary server.

- If "Automatic allocation" is selected for Auto-Recovery or manual switchover, the spare server to be allocated will be selected based on the following order of priority:

    1. Physical servers with no settings configured

    2. Physical servers for which HBA address rename information or a VIOM server profile is configured

    3. Physical servers with no agents registered

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

    1. "-"

    2. Numbers

    3. Uppercase letters

    4. Lowercase letters

4.3 Post-Switchover Operations

After a switchover was performed (either manually or automatically), perform either one of the following post-switchover recovery procedures.
For details on how to replace hardware, refer to "Chapter 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 ESC users guide.

- When performing "Failback"

    Perform the following operations.

    1. Replace failed server hardware to recover.

    2. Perform "Failback" to keep the configuration created before server switchover.

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

- When performing "Takeover"

    Perform the following operations.

    1. Replace failed server hardware to recover.

    2. Perform "Takeover" to keep the configuration created by a server switchover.

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

Information

For a server takeover procedure, server hardware can be replaced either before or after the "Takeover" operation.

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

1. Check the zoning and host affinity configurations for spare servers using the zoning and host affinity information displayed in "WWN Settings" of the [Resource Details] tab.

2. Use the storageadm zone info command to confirm the zoning and host affinity configurations.

3. Use the storageadm zone add/delete command to confirm the zoning of spare servers and host affinity configurations.

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

Note

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

Failback

Use the following procedure to return to a pre-switchover configuration.
For details on the conditions for server failback, refer to "Conditions for Server Failback" in "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 <OK>.

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

Note

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

- When using the backup and restore switchover method, do not start up the original spare server during or after the failback operation. As the primary server and spare server both run the same system image, having the two servers running together will cause conflicts of IP addresses and other information. This can adversely affect the applications switched back to the spare server.
  If it becomes necessary to start the primary server, for maintenance or other tasks, ensure that it does not start up from the same system image as that of the spare server. This can be done by turning off the primary server first, or by stopping the spare server at its BIOS screen (before startup of the OS).

- When using the backup and restore switchover method, and it is necessary to transfer newly generated data from the spare server to the primary server, back up the spare server before performing the failback.
  Refer to "Backing Up a System Image" in "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 using PRIMERGY BX servers, the maintenance LED of a primary server is automatically deactivated after a server failback.

- When the spare server is using I/O virtualization, the spare server will be powered on after failback.

Takeover

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

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

    The [Takeover] dialog is displayed.

2. Click <OK>.

    The spare server continues operating as the primary server and the server that functioned as the primary server before switchover becomes a spare server.
    If the spare server was originally shared by multiple primary servers, all those servers will now use the original primary server as their spare server.

    💡 Example

    1. Status before switchover

        Application 1: Server A (active) - Server B (spare)
        Application 2: Server C (active) - Server B (spare)

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

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

    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.

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

Chapter 5 Event Handling

This appendix explains the event handling function.

This function allows execution of a pre-defined file whenever the admin server receives SNMP Traps (events) from a registered device. This function works with the following devices.

- Chassis (Management Blade, Management Board)

- Managed Servers (ServerView)

- Remote Management Controller

- LAN Switch

The following file is executed each time an event occurs.

[Windows Manager]
Installation_folder\SVROR\Manager\etc\trapop.bat Argument 1 Argument 2 Argument 3 Argument 4 Argument 5 Argument 6

[Linux Manager]
/etc/opt/FJSVrcvmr/trapop.sh Argument 1 Argument 2 Argument 3 Argument 4 Argument 5 Argument 6

The default-installed file will log each event, but will not trigger any action based on those events.
However, it is possible to trigger operations such as email notifications or calls to external management software (command calls or event notifications) by providing a custom-script to use in place of the default script.

- The following information is passed as arguments:

  - Argument 1

    Message describing the event

  - Argument 2

    IP address of the device in which the event occurred

  - Argument 3

    Host name (FQDN) inferred from the IP address received in Argument 2 (when the name cannot be inferred, this is set to the device's IP address)

  - Argument 4

    Number of milliseconds counted from 01/01/1970 00:00:00 GMT until the current time

  - Argument 5

    Event level ("INFO", "WARNING", or "ERROR")

  - Argument 6

    Name of the device in which the event occurred

For the following events, however, only the event log is displayed. The file is not executed.

- Events logged during ROR console operations, command execution, or automatic server switchovers due to Auto-Recovery

  - Start of processing, in-progress status, end of processing

  - Changes in resource status during a running process

  - Errors that occur within Resource Orchestrator

- Errors detected from regular monitoring (when no SNMP Trap is sent, or when SNMP traps do not reach the manager because of communication errors or an abnormally high load on the system)

📗 Note

. . . .

In a clustered manager configuration, it is necessary to store the same file on both the primary and secondary nodes for this function to work properly.

. . . .

E-Mail Notification Sample

Below is a sample program that will send e-mail notifications for each event received.
To customize e-mail contents and adapt the program to your practical configuration, it is recommended to create your own version using this sample as a reference.

[Windows 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/FJSVrcvmr/trapop.sh)

```
#!/bin/sh


# MAIL_FROM=from_your@e-mail.address  <- sender address
# MAIL_TO=to_your@e-mail.address      <- destination address


# HOSTNAME=`/bin/uname -n`
# MAILCMD="/usr/sbin/sendmail -t"


# $MAILCMD <<ENDMAIL
# From: $MAIL_FROM
# To: $MAIL_TO
# Subject: Resource Coordinator VE($HOSTNAME) event mail


# ---------------------------------------------
# Resource Coordinator VE: event mail
# ---------------------------------------------
# $1


# ENDMAIL
```

When actually using this script, remove all comments and enter appropriate addresses.

```
#!/bin/sh


MAIL_FROM=from_your@e-mail.address  <- sender address
MAIL_TO=to_your@e-mail.address      <- destination address


HOSTNAME=`/bin/uname -n`
MAILCMD="/usr/sbin/sendmail -t"


$MAILCMD <<ENDMAIL
From: $MAIL_FROM
To: $MAIL_TO
Subject: Resource Coordinator VE($HOSTNAME) event mail


---------------------------------------------
Resource Coordinator VE: event mail
```

```
------------------------------------------------
$1


ENDMAIL
```

Information

The above sample assumes that the sendmail command is available on the admin server. Adapt the path to the sendmail command to your own environment. The outgoing SMTP server can be defined by changing the sendmail command's configuration files.

Part 3   Retention

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
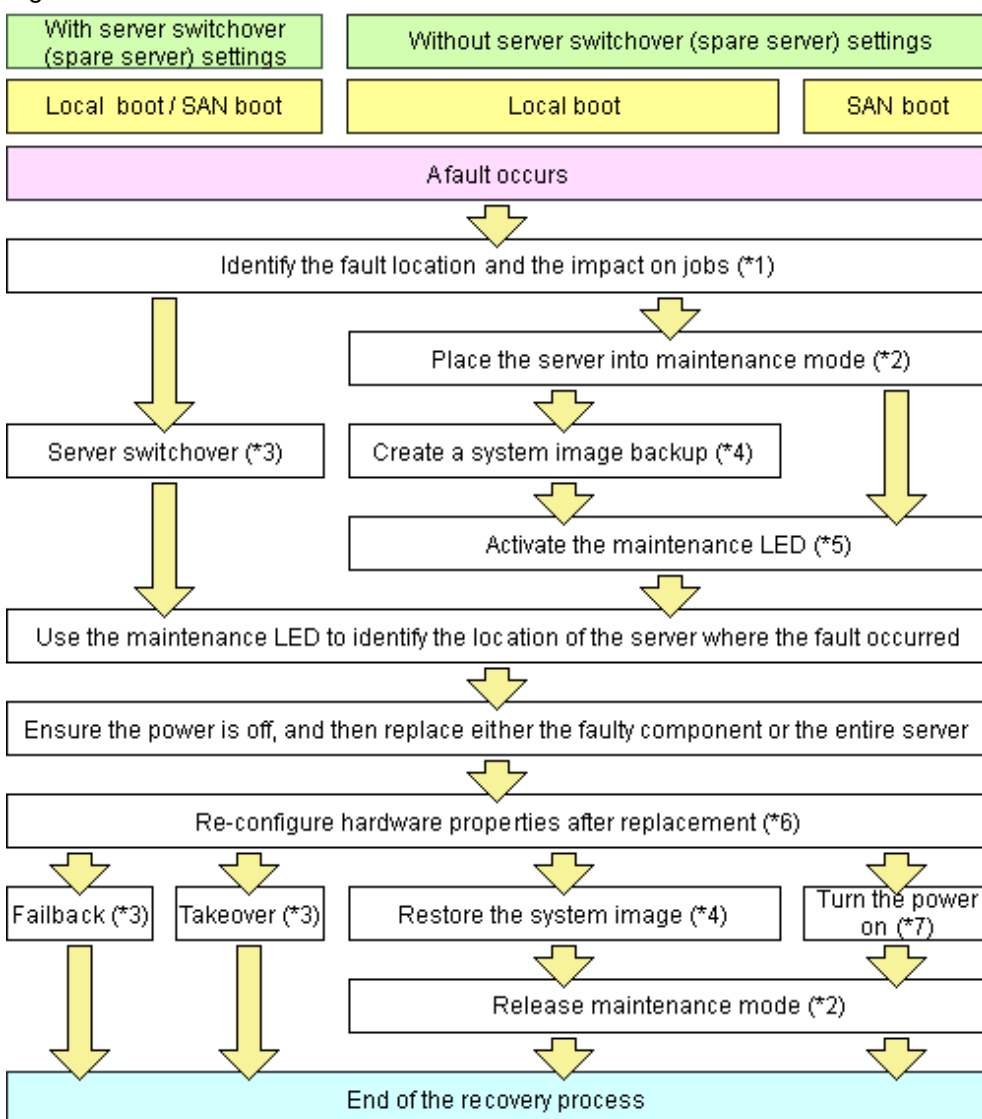
*1: For details on how to identify failures, refer to "11.3 Addressing Resource Failures".
*2: For details on how to configure and release the maintenance mode, refer to "Appendix C Maintenance Mode" in the "User's Guide VE".
*3: For details on server switchover, failback, and takeover, refer to "Chapter 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". Please note that maintenance LED operations are only supported for PRIMERGY BX servers.
*6: For details on re-configuring hardware properties, refer to "6.3.1 Reconfiguration of Hardware Properties".
*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 "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 or adding server components, 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 non-server hardware, refer to "6.3.4 Replacing Non-server Hardware".

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".

🛑 Note

- Maintenance LED control is only available for PRIMERGY BX servers. The actual LED used as an identification LED differs between server models.

   - For PRIMERGY BX600 servers, the power LED is used (blinks when activated).

   - For PRIMERGY BX900 servers, the ID indicator is used (lit when activated).

- If SNMP agent settings within the management blade configuration are incorrect, maintenance LED operations in Resource Orchestrator will end successfully, but the state of the identification LED will not change. 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 <OK>.

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

Note

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

Deactivating a Maintenance LED

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

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

    The [Turning off Maintenance LED] dialog is displayed.

2. Click <OK>.

    The maintenance LED is turned off.

6.2.2 Reconfiguration of Hardware Properties

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

After hardware replacement, it is necessary to re-configure Resource Orchestrator with the new hardware properties.
For PRIMERGY BX servers, the hardware properties are automatically re-configured.

Note

-   Ensure this operation is performed only after the replacement of one of the following: a server itself, the NIC used for either the admin or public LAN, or the HBA.
    If it is not, there is a possibility that operations on the server will not run correctly.

-   After replacing the hardware, the server status becomes "unknown". The appropriate status can be restored by re-configuring the hardware properties from the server.

Prerequisites

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

-   Both the replaced server and replacement server must be the same model

    A warning message is shown if the model of the replacement server differs from that of the replaced server.

-   When replacing a PRIMERGY BX server, the replacement server must be inserted into the same slot as used for the replaced server

    Hardware properties cannot be re-configured from a server inserted in a different slot. An error occurs if no server is inserted in the slot occupied by the previous server.

-   The replaced server and replacement server must both be of the same blade type

    If the blade types of the replaced and replacement servers are different, an error will occur.

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

Pre-Configuration

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

If automatic re-configuration is not necessary for PRIMERGY BX servers, delete the following file, and then restart the manager.

Placeholder for the Definition File

[Windows Manager]
Installation_folder\SVROR\Manager\etc\customize_data

[Linux Manager]
/etc/opt/FJSVrcvmr/customize_data

Name of the Definition File

auto_replace.rcxprop

Re-configuring 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 re-configure properties for replaced hardware.

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

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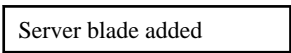
   After the message is displayed, shut down the server if it is still powered on.

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 <OK>.

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

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 an Agent"

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 Assigned with Spare Servers

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

  1. Perform Server Switchover

     Switch over the server to replace with its spare server.
     For details on the switchover function, refer to "Chapter 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 Configure the Server Environment" in the "Design Guide VE".
   Shut down the server after completing BIOS settings.

3. Re-configure Hardware Properties after Replacement

   After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.
   For details on how to re-configure hardware properties, refer to "6.3.1 Reconfiguration of Hardware Properties".
   After hardware properties have been re-configured, the maintenance LED is automatically turned off in the ROR console.

4. Perform Post-server Switchover Operations

   For details on the operations that must be performed after a server switchover, refer to "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. 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.

3. Activate the Maintenance LED

   Activate the maintenance LED on the server that is to be replaced before shutting it down.
   For details on how to activate maintenance LEDs, refer to "6.2.1 Maintenance LED".

4. Replace the Server

   Replace the server whose maintenance LED is activated.
   Change the BIOS settings of the replacement server to match the operating environment.
   For details on BIOS settings, refer to "6.2 Configure the Server Environment" in the "Design Guide VE".
   Shut down the server after completing BIOS settings.

5. Re-configure Hardware Properties after Replacement

   After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.
   For details on how to re-configure hardware properties, refer to "6.3.1 Reconfiguration of Hardware Properties".
   After hardware properties have been re-configured, the maintenance LED is automatically turned off in the ROR console.

6. Restore the Boot Disk

   - Local Boot

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

     If the boot disk was replaced and a system image backup was collected, restore that backup.
     Refer to "16.3 Restoring a System Image" 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.

7. Release 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 Configure the Server Environment" in the "Design Guide VE".
     Shut down the server after completing BIOS settings.

  3. Re-configure Hardware Properties after Replacement

     After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.
     For details on how to re-configure hardware properties, refer to "6.3.1 Reconfiguration of Hardware Properties".
     After hardware properties have been re-configured, the maintenance LED is automatically turned off in the ROR console.

6.2.4 Replacing Non-Server Hardware

This section explains how to replace hardware external to servers.

- **Replacing Chassis**

  No specific action is required in Resource Orchestrator.

- **Replacing Management Blades**

  No specific action is required in Resource Orchestrator.

- **Replacing LAN Switch Blades**

  No specific action is required for PRIMERGY BX900/BX400 LAN switch blades in IBP mode.
  For other LAN switch blades of PRIMERGY BX models, after replacing a switch blade, update the new LAN switch blade with the VLAN settings that were previously configured in Resource Orchestrator.
  Use the following procedure to replace a LAN switch blade.

  1. Replace the faulty LAN switch blade.

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

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

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

  3. Update the new LAN switch blade with the latest VLAN settings configured in Resource Orchestrator.

     a. In the ROR console server resource tree, right-click the target LAN switch, and select [Restore] from the popup menu.

        The [Restore LAN Switch] dialog is displayed.

     b. Click <OK>.

        VLAN settings are applied to the specified LAN switch blade.

 Note
. . . .

To replace LAN switch blades with different models, first delete the registered LAN switch blade, and then register the replacement LAN switch blade.
After the LAN switch blade is registered, the VLAN settings must be configured for the internal and external ports.
For details on the VLAN settings, refer to "7.3.4 Configuring VLANs on LAN Switch Blades" in the "User's Guide VE".

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

- **Replacing Fibre Channel Switch Blades**

No specific action is required in Resource Orchestrator.

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.

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 other than blade servers.

6.3.1 Reconfiguration of Hardware Properties

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

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

Note

- Ensure this operation is performed only after the replacement of one of the following: a server itself, the NIC used for either the admin or public LAN, or the HBA.
  If it is not, there is a possibility that operations on the server will not run correctly.

- When the system board or GSPB of a PRIMEQUEST server has been changed, ensure that this operation is performed.
  If it is not, there is a possibility that operations on the server will not run correctly.

- After replacing the hardware, the server status becomes "unknown". The appropriate status can be restored by re-configuring the hardware properties from the server.

Prerequisites

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

- Both the replaced server and replacement server must be the same model

  A warning message is shown if the model of the replacement server differs from that of the replaced server.

- 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 SPARC Enterprise servers, the hardware properties are automatically re-configured.

Re-configuring Hardware Properties after Server Replacement

- For Rack Mount and Tower Servers

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

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

        Additional Information

        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]-[Re-configure] from the popup menu.

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

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

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

        - Admin LAN MAC Address (NIC1)

            Required only if the agent is not registered.

            Additional Information

            When a server is powered off for the reason given in the Additional Information in 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 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 <OK>.

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

- For PRIMEQUEST Servers

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

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

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

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

    3. Click <OK>.

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

- For SPARC Enterprise Servers

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

Note

....

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

- Restart the managed server after reconfiguring the hardware properties

- Restart the related services described in "2.2 Starting and Stopping an Agent"

....

6.3.2 Replacing Servers

This section details the procedure to follow when replacing servers.

Information

....

- Follow the same procedure when replacing servers where VM hosts are running.

- No specific action is required in Resource Orchestrator when replacing admin servers or HBA address rename setup service servers.

....

For Rack Mount and Tower Servers

- Replacing a Server Assigned with Spare Servers

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

1. Perform Server Switchover

   Switch over the server to replace with its spare server.
   For details on the switchover function, refer to "Chapter 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 Configure 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. Re-configure Hardware Properties after Replacement

   After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.
   For details on how to re-configure hardware properties, refer to "6.3.1 Reconfiguration of Hardware Properties".

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. 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.

3. Power 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".

4. Replace the Server

   Replace the server.
   Change the BIOS settings of the replacement server to match the operating environment.
   For details on BIOS settings, refer to "6.2 Configure 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.

5. Re-configure Hardware Properties after Replacement

   After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.
   For details on how to re-configure hardware properties, refer to "6.3.1 Reconfiguration of Hardware Properties".

6. Restore the Boot Disk

   - Local Boot

     There is no need to restore the boot disk if the original disk is installed on the replaced server. Simply power on the replacement server.
     If the boot disk was replaced and a system image backup was collected, restore that backup.
     Refer to "16.3 Restoring a System Image" 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.

7. Release 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 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 Configure 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. Re-configure Hardware Properties after Replacement

     After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.
     For details on how to re-configure hardware properties, refer to "6.3.1 Reconfiguration of Hardware Properties".

For SPARC Enterprise Servers

- Replacing a server assigned with spare servers

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

- When Replacing an HBA

1. Perform Server Switchover

Switch over the server to replace with its spare server.
For details on the switchover function, refer to "Chapter 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 Configure 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 icon] **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 Configure 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 Configure 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 ESC users guide.

3. Change the WWN Information Settings

Change the WWN information settings for after server replacement to the WWN value of the HBA after server replacement.
When the target CA was deleted in step 1., configure a new target CA.
After configuration, restart the server.
After starting the server, check the status of the server's HBA from ESC.
When the HBA status is "unknown", delete it.
When the HBA status is displayed as "access path inheritance is required" (yellow icon), perform access path inheritance.
For details, refer to the ESC users guide.
When the target CA was not deleted in step 1., configure the target CA as a hyphen ("-").

For PRIMEQUEST Servers

- Replacing a Server Assigned with Spare Servers

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

1. Perform Server Switchover

Switch over the server to replace with its spare server.
For details on the switchover function, refer to "Chapter 4 Server Switchover".
The server is automatically powered off after switchover.

2. Replace the Server

Replace the server.
Use the Maintenance Wizard of the Management Board Web-UI to perform replacement.
For details on the Maintenance Wizard, refer to the PRIMEQUEST manual.
Also, change the BIOS settings of the replacement server to match the operating environment.
For details on BIOS settings, refer to "6.2 Configure the Server Environment" in the "Design Guide VE".
Shut down the server after completing BIOS settings.

3. Re-configure Hardware Properties after Replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.
For details on how to re-configure hardware properties, refer to "6.3.1 Reconfiguration of Hardware Properties".

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. 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.

3. Power 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".

4. Replace the Server

Replace the server.
Use the Maintenance Wizard of the Management Board Web-UI to perform replacement.
For details on the Maintenance Wizard, refer to the PRIMEQUEST manual.
Also, change the BIOS settings of the replacement server to match the operating environment.
For details on BIOS settings, refer to "6.2 Configure the Server Environment" in the "Design Guide VE".
Shut down the server after completing BIOS settings.

5. Re-configure Hardware Properties after Replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.
For details on how to re-configure hardware properties, refer to "6.3.1 Reconfiguration of Hardware Properties".

6. Restore the Boot Disk

- Local Boot

There is no need to restore the boot disk if the original disk is installed on the replaced server. Simply power on the replacement server.
If the boot disk was replaced and a system image backup was collected, restore that backup.
Refer to "16.3 Restoring a System Image" 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.

7. Release 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 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 Configure the Server Environment" in the "Design Guide VE".
Shut down the server after completing BIOS settings.

3. Re-configure Hardware Properties after Replacement

After replacing the server, re-configure Resource Orchestrator with the latest hardware properties.
For details on how to re-configure hardware properties, refer to "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 and Adding Network Interfaces (Admin LAN, Public LAN)**

  The procedure used to replace and add network interfaces is the same as that 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 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>

  [Xen]
  When using Citrix XenServer, reinstall XenServer referring to the Citrix XenServer manual.

  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 temporally disable automatic startup of the xend daemon and then restart the managed server.

     > # **chkconfig xend off** <RETURN>

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

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

  [Linux]
  When the configuration of server components has been changed, check the configuration file of the OS, and make any necessary corrections. For details, refer to "Configuration File Check" in "2.1.1.1 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 "Configuration File Check" 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**

  The procedure used to replace an HBA is the same as that described in "6.3.2 Replacing Servers".

  - When using I/O virtualization, the replacement HBA will automatically inherit the WWN originally set on the replaced HBA. Therefore, there is no need to re-configure access paths on the storage side.

  - When configuring WWN information, it is necessary to change WWN information settings to the replaced HBA WWN values. 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.

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".

- **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.

  [Solaris Containers]
  When replacing, adding or removing CPU, Add replaced, added or removed CPU to the resource pool for Solaris Containers or remove it depending on your environment.

  For details, refer to "C.7 Solaris Containers" in the "Setup Guide CE".

6.3.4 Replacing Non-server Hardware

This section explains how to replace hardware external to servers.

- **Replacing Management Blades**

  No specific action is required in Resource Orchestrator.

- **Replacing Management Boards**

  No specific action is required in Resource Orchestrator.

- **Replacing LAN Switches**

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

6.4 Storage Device Maintenance

This section explains how to maintain storage devices.

- **Replacing storage devices**

  No specific action is required in Resource Orchestrator.

  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.

  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.

6.5 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, re-configure 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. Re-configure the power monitoring device's hardware properties.

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

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

     b. Click <OK>.

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

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 re-configuring the network interfaces used for the public LAN following deployment of a cloning image.

For details on the cloning function, refer to "Chapter 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
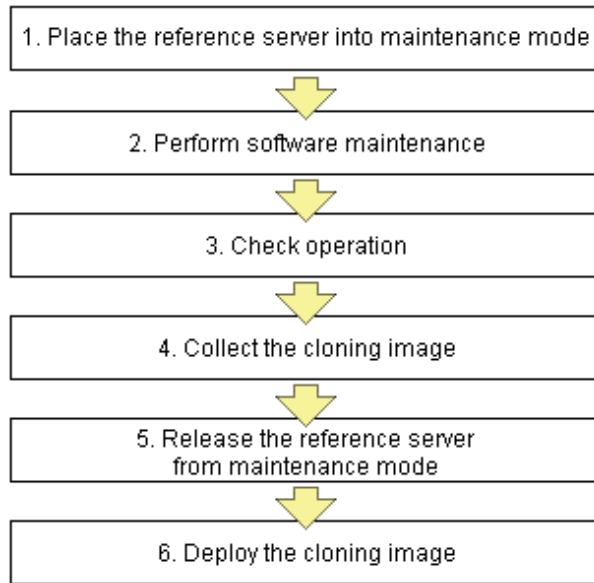
Each of these steps is explained below.

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 the admin server.

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	Not Required	-
Session encryption keys	rcxkeydefbackup	Yes	After password saving (after execution of the rcxlogin -save command)	Not Required	-
System images and cloning images	scwbackup	Yes	After addition, deletion, and modification of physical server images	Not Required	-
Configuration definition information	rcxbackup	Yes	After creation, registration, modification, unregistration, and deletion of resources	Not Required	-
Information related to image files	scwbackup	Yes	After the registration and unregistration of VM hosts	Not Required	-
Definition files	rcxkeydefbackup	Yes	Modification of definition files	Not Required	-
Image management information	rcxkeydefbackup	Yes	After rcxadm imagemgr command operations	Not Required	-

Backup operations are necessary at the timing listed in "Table 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 (*)

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

📙 Note

The configuration definition information managed by Resource Orchestrator is the target of backup and restore.

VM management software, VM hosts, VM guest boot images, and VM guest virtual disks are not the target of backup and restore. Perform backup and restore another way.

9.1.2 Backing Up the Admin Server

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. - 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 configuration definition file.

 Example
・・
Once every hour
・・

- Backup Destination

Decide the disk on which the backup data will be stored.

It is recommended to specify a different disk from the one that Resource Orchestrator is installed on.

For details on the free disk space necessary for backups, refer to the notes in "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 D 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 rcxkeydefnackup 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/FJSVrcvmr/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 "2.4.2.5 Dynamic Disk Space" in the "Design Guide VE".

. . . .

3. Back up virtual machines of VM management software

   For details on how to perform backup, refer to the manual of the VM management software.

4. Back up configuration definition information

   Execute the following commands to write configuration definition information. Specify a directory or folder to write the configuration definition information and the version XML to.

   Specify the directory or folder using -dir. If the specified directory or folder does not exist, an error occurs.

   For details 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/FJSVrcvmr/bin/rcxbackup

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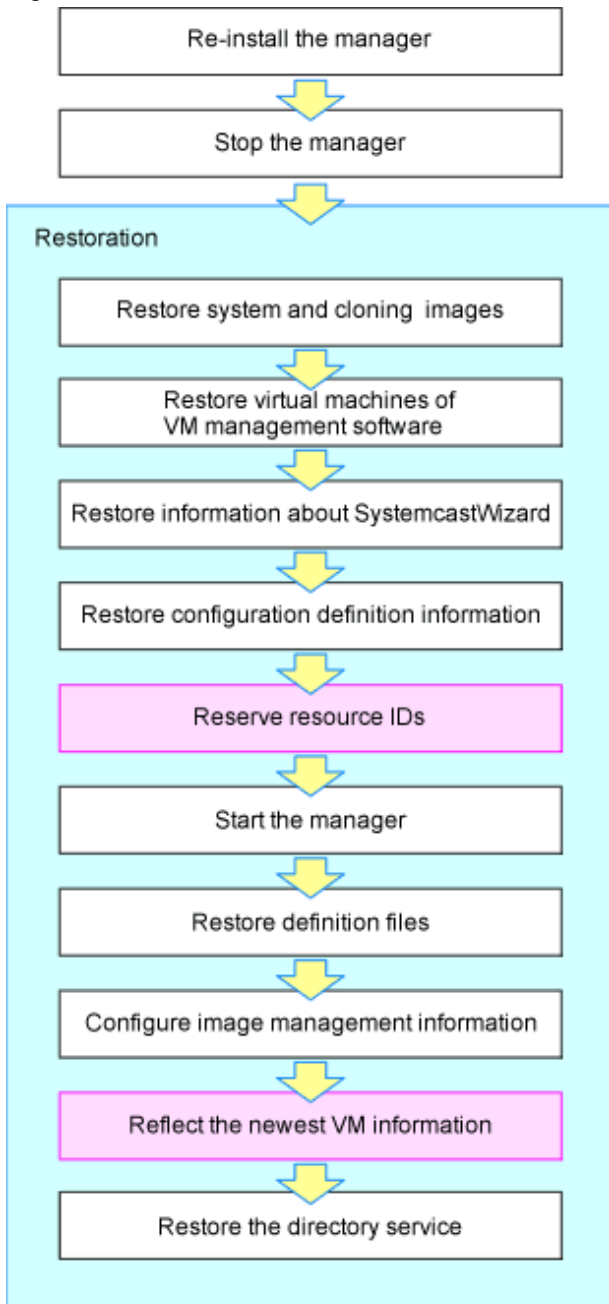
Note

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

: Activities performed when restoring the operations from after a backup

Note

In a clustered manager configuration, restore backed up contents to the cluster-shared disk.
For details on the folder names used on the shared disk, refer to "Appendix D 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.

Stop the manager after re-installation.
For details on how to stop the manager, refer to "2.1 Starting and Stopping the Manager".

b. Execute the rcxkeydefrestore command to restore certificates, session encryption keys, definition files, and image management information.
For details of the rcxkeyrestore 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 following command:

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. Start the manager

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

6. Reflect the newest information of VM on Resource Orchestrator using VM management software.

   For details of the rcxadm vmmgr refresh command, refer to "5.14 rcxadm vmmgr" in the "Reference Guide (Command) VE".

   > **rcxadm vmmgr refresh** <RETURN>

   Wait for at least 60 seconds.

   > **rcxadm vmmgr refresh** <RETURN>

Note

Be sure to wait for 60 seconds or more before executing the rcxadm vmmgr refresh command for the second time. Otherwise, the newest information of VM may not be reflected correctly.

7. Restore a directory service

   When using a directory service for user management, restore the directory service.

   For details on how to perform restoration, refer to the manual of the directory service.

Note

- In a clustered manager configuration, restore backed up contents to the cluster-shared disk.
  For details on the folder names used on the shared disk, refer to "Appendix D 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

    - Collection of snapshots

        - 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 an Agent"

- Connection information of LAN switches and network maps cannot be backed up. For details on how to register LAN switches and obtain the network information, refer to "13.2 Preparations" in the "User's Guide VE".

- VIOM coordination user names and passwords cannot be backed up. Register VIOM coordination before performing restoration. For details on operation methods, refer to "7.1 Registering VIOM 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. Files

   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. Stop the Manager

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

   ## Note

   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.

   ## Note

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

   Start the Manager

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

   ## Note

   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.

Note

- 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 BIOS Settings for 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. Stop the Manager

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

    ![Note icon] **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 icon] **Note**
    . . . .
    Copy the image files in the image file storage folders using the names of the resource folders when they were backed up.
    However, if a resource folder of the same version exists, change the version part of the resource folder to an integer in the range of "1 to the maximum version number plus 1", which does not overlap.
    . . . .

5. Start the Manager

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

    ![Note icon] **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

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, LAN 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.

📖 Note
. . . .

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 Hosts	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 Firewall Server load balancer	L2 switch Firewall Server load balancer
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
	VM guest
	LAN switch blade L2 switch
	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
None	normal	Normal	No action is necessary
⚠	warning	Warning An error has occurred but the resource can still be used.(*1)	Action must be taken
	unknown	Unknown The status of the resource cannot be obtained. (*2, *3)	Action must be taken
⏹	stop	Stop The resource has stopped and cannot be used.	No action is necessary
❌	error	Error An error whose cause is unknown has occurred and the resource cannot be used.	Action must be taken
	fatal	Fault A fault has occurred in the resource and the resource cannot be used.	Action must be taken

*1: When a LAN switch is in "warning" status, it may mean that the LAN switch has been replaced with another model.
To use the LAN switch as it is, first delete the registered LAN switch, and then register it again.
*2: When a VM guest is in "unknown" status, check the operation status of the VM host on which the VM guest is running.
*3: When a LAN switch is in "unknown" status, check the physical connection between the LAN switch and admin LAN as well as whether or not the LAN switch is responding to commands.

Note

. . . .

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

- For other servers, hardware statuses cannot be obtained from server management software (ServerView). Therefore, only "normal", "stop" or "unknown" statuses are shown, while "warning", "error", and "fatal" statuses cannot be detected.

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

. . . .

Table 11.5 Physical Server Icons

Icon	Meaning
	Spare server
	Maintenance mode server

Table 11.6 OS Icons

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

Information

. . . .

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

  - VM management software

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

  - VM host

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

  - VM guest

    Errors detected from server virtualization software are reflected in VM guest statuses.
    VM guest statuses can be one of the following: "normal", "warning", "error", "unknown", or "stop".
    For details, refer to "D.3 Functional Differences between Products" in the "Design Guide VE".

- For LAN switches, "error" and "fatal" are not displayed.
  Only "warning", "normal", or "unknown" are 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 OS's, VM hosts, or VM guests.
   If Auto-Recovery has been enabled for a physical OS or VM host, it will be automatically switched over with a spare server. If Auto-Recovery has not been enabled, server switchover can still be performed manually as long as a spare server has been designated.

   For more information regarding server switchover, refer to "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 "θ", this factor is expressed as "$\cos\theta$").
. . . .

Note
. . . .

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

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".

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.

- Note the following points regarding the occurrence of a fault in the switchover destination spare server during server switchover.

  - The server switchover state returns to pre-switchover state. Additionally, maintenance mode is set for the switchover source server, and server switchover processing ends. If the switchover source server has been stopped, the switchover source server does not start.

  - Even when more than one spare server is set for the primary server, there is no automatic switch to another spare server. Specify another spare server, then perform server switchover manually.

  - To perform operations on the switchover source server, start the server and then release maintenance mode. However, when Auto-Recovery is enabled and the switchover source server is faulty, Auto-Recovery occurs when maintenance mode is released. Restore the switchover source server to its pre-fault status and then release maintenance mode.

Redundancy Configurations for the Admin LAN

If communication issues occur on the admin LAN, or one of the network interfaces used by a managed server on the admin LAN fails, the following operations may result in errors. In such cases, restore the admin LAN network as quickly as possible.

- Backup and restore operations

- Collection and deployment of cloning images

- Server switchover and failback

HBA address rename

- With Resource Orchestrator, the factory-set WWN of a managed server's HBA is overridden when the HBA address rename function is used. The WWN is reset to its factory-set value when the server is deleted from Resource Orchestrator.
  Before using HBAs in an environment that is not managed by Resource Orchestrator, first delete the server in which it is mounted using the ROR console.
  For information on deleting servers, refer to "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 the Manager".

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:

- Configuration File

[Windows Manager]
Installation_folder\SVROR\Manager\rails\config\rcx\rcx_manager_params.rb

[Linux Manager]
/opt/FJSVrcvmr/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 the manager services
	
	  Specify "true".
	
	 - When not restarting
	
	  Specify "false".
		true

RESTART_HOUR	Specify the restart time (hour) from 0 to 23.	3
RESTART_MIN	Specify the restart time (minutes) from 0 to 59.	45
RESTART_CYCLE	Specify the restart interval (days) from 1 to 5.	1

- Parameter Change Procedure

1. Stop the manager.

2. Use an editor and change the parameters of the rcx_manager_params.rb file.

3. Start the manager.

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

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.

Changing Multiple Operations of Managers

For the manager, the number of processes executed at the same time is limited to optimize the memory usage.

Depending on the environment for use, the upper limit can be modified. To modify the configuration, edit the following definition file.

When there is no definition file, create one.

Placeholder for the Definition File

> [Linux Manager]
> /etc/opt/FJSVrcvmr/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:

> | *Key = Value* |
> | --- |

Items in the Definition File

> Specify the following items.

Table A.2 Items in the Definition File

Item	Key	Value	Remarks
Multiplicity	TASK_WORKER _COUNT	Specify the multiplicity from 5 - 30.	The initial value is "5". If there is no definition file, the default value is used.

Example of the Definition File

> The following is an example of the definition file. In this example, the multiplicity is set to "10".

> | TASK_WORKER_COUNT=10 |
> | --- |

Changing Procedures of Definition Files

- When the manager is operating in a normal environment

  1. Stop the manager.

  2. Use an editor and change the value of TASK_WORKER_COUNT in the rcx_base.rcxprop file.
     If there is no rcx_base.rcxprop file, create one.

  3. Start 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. Use an editor and change the value of "TASK_WORKER_COUNT" in the rcx_base.rcxprop file on the shared disk.
   If there is no rcx_base.rcxprop file, create one.

   Placeholder for the Definition File

   Drive_name\Fujitsu\ROR\SVROR\customize_data\rcx_base.rcxprop

4. Start the manager.

[Linux Manager]

1. Stop the manager.

2. Mount the shared disk for the admin server on the primary or secondary node.

3. Use an editor and change the value of TASK_WORKER_COUNT in the rcx_base.rcxprop file on the shared disk.
   If there is no rcx_base.rcxprop file, create one.

   Placeholder for the Definition File

   Mount_destination_of_shared_disk/Fujitsu/ROR/SVROR/etc/opt/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 the Manager".

Note

• •

Memory usage will increase according to the multiplicity.
For details on the memory usage to increase, refer to "Table A.3 Increased Memory Use with Multiple Operations".
Calculate the memory used from a value in the table and the memory size required for the manager operations described in "2.4.2.6 Memory Size" in the "Design Guide VE", and then add memory if necessary.

Table A.3 Increased Memory Use with Multiple Operations

Multiplicity	Increase in Memory Use (Unit: MB)
5	-
6 - 14	$1080 + (Multiplicity * 40)$
15 - 30	$2104 + (Multiplicity * 40)$

• •

Glossary

access path

A logical path configured to enable access to storage volumes from servers.

active mode

The state where a managed server is performing operations.
Managed servers must be in active mode in order to use Auto-Recovery.
Move managed servers to maintenance mode in order to perform backup or restoration of system images, or collection or deployment of cloning images.

active server

A physical server that is currently operating.

admin client

A terminal (PC) connected to an admin server, which is used to operate the GUI.

admin LAN

A LAN used to manage resources from admin servers.
It connects managed servers, storage, and network devices.

admin server

A server used to operate the manager software of Resource Orchestrator.

affinity group

A grouping of the storage volumes allocated to servers. A function of ETERNUS.

Equivalent to the LUN mapping of EMC.

agent

The section (program) of Resource Orchestrator that operates on managed servers.

Auto-Recovery

A function which continues operations by automatically switching over the system image of a failed server to a spare server and restarting it in the event of server failure.
This function can be used when managed servers are in a local boot configuration, SAN boot configuration, or a configuration such as iSCSI boot where booting is performed from a disk on a network.

- When using a local boot configuration

  The system is recovered by restoring a backup of the system image of the failed server onto a spare server.

- When booting from a SAN or a disk on a LAN

  The system is restored by having the spare server inherit the system image on the storage.
  Also, when a VLAN is set for the public LAN of a managed server, the VLAN settings of adjacent LAN switches are automatically switched to those of the spare server.

BACS (Broadcom Advanced Control Suite)

An integrated GUI application (comprised from applications such as BASP) that creates teams from multiple NICs, and provides functions such as load balancing.

Basic Mode

A function that can be used by configuring a Cloud Edition license after installing ROR VE.

BASP (Broadcom Advanced Server Program)

LAN redundancy software that creates teams of multiple NICs, and provides functions such as load balancing and failover.

blade server

A compact server device with a thin chassis that can contain multiple server blades, and has low power consumption.
As well as server blades, LAN switch blades, management blades, and other components used by multiple server blades can be mounted inside the chassis.

blade type

A server blade type.
Used to distinguish the number of server slots used and servers located in different positions.

BladeViewer

A GUI that displays the status of blade servers in a style similar to a physical view and enables intuitive operation.
BladeViewer can also be used for state monitoring and operation of resources.

BMC (Baseboard Management Controller)

A Remote Management Controller used for remote operation of servers.

boot agent

An OS for disk access that is distributed from the manager to managed servers in order to boot them when the network is started during image operations.

CA (Channel Adapter)

An adapter card that is used as the interface for server HBAs and fibre channel switches, and is mounted on storage devices.

chassis

A chassis used to house server blades and partitions.
Sometimes referred to as an enclosure.

cloning

Creation of a copy of a system disk.

cloning image

A backup of a system disk, which does not contain server-specific information (system node name, IP address, etc.), made during cloning.
When deploying a cloning image to the system disk of another server, Resource Orchestrator automatically changes server-specific information to that of the target server.

Cloud Edition

The edition which can be used to provide private cloud environments.

Domain

A system that is divided into individual systems using partitioning. Also used to indicate a partition.

DR Option

The option that provides the function for remote switchover of servers or storage in order to perform disaster recovery.

end host mode

This is a mode where the uplink port that can communicate with a downlink port is fixed at one, and communication between uplink ports is blocked.

environmental data

Measured data regarding the external environments of servers managed using Resource Orchestrator.
Measured data includes power data collected from power monitoring targets.

ESC (ETERNUS SF Storage Cruiser)

Software that supports stable operation of multi-vendor storage system environments involving SAN, DAS, or NAS. Provides configuration management, relation management, trouble management, and performance management functions to integrate storage related resources such as ETERNUS.

Express

The edition which provides server registration, monitoring, and visualization.

external FTP server

An FTP server used to relay network device files between the ROR manager and network devices that do not possess their own FTP server function.

FC switch (Fibre Channel Switch)

A switch that connects Fibre Channel interfaces and storage devices.

fibre channel switch blade

A fibre channel switch mounted in the chassis of a blade server.

global zone

The actual OS that is used for a Solaris container.

A Solaris environment that has been installed on a physical server.

GLS (Global Link Services)

Fujitsu network control software that enables high availability networks through the redundancy of network transmission channels.

GSPB (Giga-LAN SAS and PCI_Box Interface Board)

A board which mounts onboard I/O for two partitions and a PCIe (PCI Express) interface for a PCI box.

GUI (Graphical User Interface)

A user interface that displays pictures and icons (pictographic characters), enabling intuitive and easily understandable operation.

HA (High Availability)

The concept of using redundant resources to prevent suspension of system operations due to single problems.

hardware initiator

A controller which issues SCSI commands to request processes.
In iSCSI configurations, NICs fit into this category.

hardware maintenance mode

In the maintenance mode of PRIMEQUEST servers, a state other than Hot System Maintenance.

HBA (Host Bus Adapter)

An adapter for connecting servers and peripheral devices.
Mainly used to refer to the FC HBAs used for connecting storage devices using Fibre Channel technology.

HBA address rename setup service

The service that starts managed servers that use HBA address rename in the event of failure of the admin server.

HBAAR (HBA address rename)

I/O virtualization technology that enables changing of the actual WWN possessed by an HBA.

host affinity

A definition of the server HBA that is set for the CA port of the storage device and the accessible area of storage.
It is a function for association of the Logical Volume inside the storage which is shown to the host (HBA) that also functions as security internal to the storage device.

Hyper-V

Virtualization software from Microsoft Corporation.

Provides a virtualized infrastructure on PC servers, enabling flexible management of operations.

I/O virtualization option

An optional product that is necessary to provide I/O virtualization.
The WWNN address and MAC address provided is guaranteed by Fujitsu Limited to be unique.
Necessary when using HBA address rename.

IBP (Intelligent Blade Panel)

One of operation modes used for PRIMERGY switch blades.
This operation mode can be used for coordination with ServerView Virtual I/O Manager (VIOM), and relations between server blades and switch blades can be easily and safely configured.

ILOM (Integrated Lights Out Manager)

The name of the Remote Management Controller for SPARC Enterprise T series servers.

image file

A system image or a cloning image. Also a collective term for them both.

IPMI (Intelligent Platform Management Interface)

IPMI is a set of common interfaces for the hardware that is used to monitor the physical conditions of servers, such as temperature, power voltage, cooling fans, power supply, and chassis.
These functions provide information that enables system management, recovery, and asset management, which in turn leads to reduction of overall TCO.

IQN (iSCSI Qualified Name)

Unique names used for identifying iSCSI initiators and iSCSI targets.

iRMC (integrated Remote Management Controller)

The name of the Remote Management Controller for Fujitsu's PRIMERGY servers.

iSCSI

A standard for using the SCSI protocol over TCP/IP networks.

LAN switch blades

A LAN switch that is mounted in the chassis of a blade server.

license

The rights to use specific functions.

Users can use specific functions by purchasing a license for the function and registering it on the manager.

link aggregation

Function used to multiplex multiple ports and use them as a single virtual port.

With this function, if one of the multiplexed ports fails its load can be divided among the other ports, and the overall redundancy of ports improved.

logical volume

A logical disk that has been divided into multiple partitions.

LSB (Logical System Board)

A system board that is allocated a logical number (LSB number) so that it can be recognized from the domain, during domain configuration.

maintenance mode

The state where operations on managed servers are stopped in order to perform maintenance work.

In this state, the backup and restoration of system images and the collection and deployment of cloning images can be performed.

However, when using Auto-Recovery it is necessary to change from this mode to active mode. When in maintenance mode it is not possible to switch over to a spare server if a server fails.

managed server

A collective term referring to a server that is managed as a component of a system.

management blade

A server management unit that has a dedicated CPU and LAN interface, and manages blade servers.

Used for gathering server blade data, failure notification, power control, etc.

Management Board

The PRIMEQUEST system management unit.

Used for gathering information such as failure notification, power control, etc. from chassis.

manager

The section (program) of Resource Orchestrator that operates on admin servers.

It manages and controls resources registered with Resource Orchestrator.

virtual switch

A function provided by server virtualization software to manage networks of VM guests as virtual LAN switches.

The relationships between the virtual NICs of VM guests and the NICs of the physical servers used to operate VM hosts can be managed using operations similar to those of the wiring of normal LAN switches.

VLAN (Virtual LAN)

A splitting function, which enables the creation of virtual LANs (seen as differing logically by software) by grouping ports on a LAN switch.

Using a Virtual LAN, network configuration can be performed freely without the need for modification of the physical network configuration.

VLAN ID

A number (between 1 and 4,095) used to identify VLANs.

Null values are reserved for priority tagged frames, and 4,096 (FFF in hexadecimal) is reserved for mounting.

VM (Virtual Machine)

A virtual computer that operates on a VM host.

VM guest

A virtual server that operates on a VM host, or an OS that is operated on a virtual machine.

VM Home Position

The VM host that is home to VM guests.

VM host

A server on which server virtualization software is operated, or the server virtualization software itself.

VM maintenance mode

One of the settings of server virtualization software, that enables maintenance of VM hosts.
For example, when using high availability functions (such as VMware HA) of server virtualization software, by setting VM maintenance mode it is possible to prevent the moving of VM guests on VM hosts undergoing maintenance.
For details, refer to the manuals of the server virtualization software being used.

VM management software

Software for managing multiple VM hosts and the VM guests that operate on them.
Provides value adding functions such as movement between the servers of VM guests (migration).

VMware

Virtualization software from VMware Inc.
Provides a virtualized infrastructure on PC servers, enabling flexible management of operations.

Web browser

A software application that is used to view Web pages.

WWN (World Wide Name)

A 64-bit address allocated to an HBA.
Refers to a WWNN or a WWPN.

WWNN (World Wide Node Name)

The WWN set for a node.
The Resource Orchestrator HBA address rename sets the same WWNN for the fibre channel port of the HBA.

WWPN (World Wide Port Name)

The WWN set for a port.
The Resource Orchestrator HBA address rename sets a WWPN for each fibre channel port of the HBA.

WWPN zoning

The division of ports into zones based on their WWPN, and setting of access restrictions between different zones.

Xen

A type of server virtualization software.

XSB (eXtended System Board)

Unit for domain creation and display, composed of physical components.

XSCF (eXtended System Control Facility)

The name of the Remote Management Controller for SPARC Enterprise M series servers.

zoning

A function that provides security for Fibre Channels by grouping the Fibre Channel ports of a Fibre Channel switch into zones, and only allowing access to ports inside the same zone.