FUJITSU Software
ServerView Resource Orchestrator
Virtual Edition V3.1.2

User's Guide

Windows/Linux

Preface

Purpose of This Document

This manual provides an outline of the operation method of the ROR console provided by FUJITSU Software ServerView Resource Orchestrator Virtual Edition (hereinafter Resource Orchestrator).

Intended Readers

This manual is written for people who will install Resource Orchestrator.
When setting up systems, it is assumed that readers have the basic knowledge required to configure the servers, storage, and network devices to be installed.

Structure of This Document

This manual is composed as follows:

Chapter 1 Login and Logout

Explains how to log in and out of the ROR console.

Chapter 2 Home

Explains the ROR Console Home window display.

Chapter 3 Resource Management Overview

Provides an overview of the two views available in Resource Orchestrator.

Chapter 4 License Setup and Confirmation

Explains license setup.

Chapter 5 Managing User Accounts

Explains how to register, modify, and delete user accounts.

Chapter 6 BladeViewer

Provides an overview of BladeViewer and explains its features.

Chapter 7 Registering Resources

Explains how to register the resources used by Resource Orchestrator.

Chapter 8 Changing Admin Server Settings

Explains how to change the settings of the admin server.

Chapter 9 Changing Resources

Explains how to change settings for the admin server or resources registered on the admin server.

Chapter 10 Configuring the Operating Environments of Managed Servers

Explains how to install software to the registered managed servers and set up their operating environment.

Chapter 11 Deleting Resources

Explains how to delete resources.

Chapter 12 Pre-configuration for Resource Registration and Modification

Provides an overview of the pre-configuration function and explains how to use system configuration files.

Chapter 13 NetworkViewer

Provides an overview of the NetworkViewer and explains its features.

Web Site URLs

URLs provided as reference sources within the main text are correct as of November 2015.

Please understand that they are subject to change without notice.

Document Conventions

The notation in this manual conforms to the following conventions.

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

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

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

[Windows Manager]	Sections related to Windows manager
[Linux Manager]	Sections related to Linux manager
[Windows]	Sections related to Windows
[Linux]	Sections related to Linux
[Red Hat Enterprise Linux]	Sections related to Red Hat Enterprise Linux
[Solaris]	Sections related to Solaris
[VMware]	Sections related to VMware

[Horizon View]	Sections related to VMware Horizon View
[Hyper-V]	Sections related to Hyper-V
[Xen]	Sections related to RHEL5-Xen
[KVM]	Sections related to RHEL-KVM
[Solaris Zones]	Sections related to Solaris zones
[OVM for x86 3.2]	Sections related to Oracle VM Server for x86 3.2
[OVM for SPARC]	Sections related to Oracle VM Server for SPARC
[Physical Servers]	Sections related to physical servers

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

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

- Oracle Solaris Zones may also be indicated as Solaris Containers or Solaris Container.

- Oracle VM Server for x86 may also be indicated as Oracle VM.

- In Resource Orchestrator, the following servers are referred to as SPARC Enterprise.

    - SPARC Enterprise M3000/M4000/M5000/M8000/M9000

    - SPARC Enterprise T5120/T5140/T5220/T5240/T5440

- In Resource Orchestrator, the following servers are referred to as SPARC M10.

    - SPARC M10-1/M10-4/M10-4S

- Fujitsu M10 is the product name used for SPARC M10 when they are sold outside Japan.

- 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 "#".

- If using Windows 8 or Windows Server 2012, please note the following:
  Operations descriptions in this manual use examples assuming operating systems up to Windows 7 and Windows Server 2008 - if using this product with Windows 8 or Windows Server 2012, read instructions regarding the [Start] menu as if they were instructions for the [Apps] page.
  Display the [Apps] page by right-clicking in the [Start] screen, and then clicking on [All apps].

- When using Resource Orchestrator on Windows 8.1 and Windows Server 2012 R2, please note the following.
  When OS operations are explained in this manual, the examples assume OSs up to Windows 7 and Windows Server 2008. When using Resource Orchestrator on Windows 8.1 or Windows Server 2012 R2, take explanations regarding the [Start] menu as indicating the [Apps] screen.
  The [Apps] screen can be displayed by swiping the [Start] screen from bottom to top, or clicking the downward facing arrow on the lower-left of the [Start] screen.

Menus in the ROR console

Operations on the ROR console can be performed using either the menu bar or pop-up menus.

By convention, procedures described in this manual only refer to pop-up menus.

Regarding Installation Folder Paths

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

Replace it as shown below.

- When using Windows 64-bit (x64)

    C:\Program Files (x86)\Resource Orchestrator

- When using Windows 32-bit (x86)

    C:\Program Files\Resource Orchestrator

Command Examples

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

Abbreviations

The following abbreviations are used in this manual:

Abbreviation	Products
Windows	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 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) 2012 Standard Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2012 R2 Essentials Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Datacenter Microsoft(R) Windows(R) XP Professional operating system Windows Vista(R) Business Windows Vista(R) Enterprise Windows Vista(R) Ultimate Windows(R) 7 Professional Windows(R) 7 Ultimate Windows(R) 8 Pro Windows(R) 8 Enterprise Windows(R) 8.1 Pro Windows(R) 8.1 Enterprise
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 Server 2008	Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise

Abbreviation	Products
	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 2012	Microsoft(R) Windows Server(R) 2012 Standard Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2012 R2 Essentials Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Datacenter
Windows PE	Microsoft(R) Windows(R) Preinstallation Environment
Windows XP	Microsoft(R) Windows(R) XP Professional operating system
Windows Vista	Windows Vista(R) Business Windows Vista(R) Enterprise Windows Vista(R) Ultimate
Windows 7	Windows(R) 7 Professional Windows(R) 7 Ultimate
Windows 8	Windows(R) 8 Pro Windows(R) 8 Enterprise Windows(R) 8.1 Pro Windows(R) 8.1 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) 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)

Abbreviation	Products
	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) 5.9 (for x86)
	Red Hat(R) Enterprise Linux(R) 5.9 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 5.10 (for x86)
	Red Hat(R) Enterprise Linux(R) 5.10 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 5.11 (for x86)
	Red Hat(R) Enterprise Linux(R) 5.11 (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(R) Enterprise Linux(R) 6.3 (for x86)
	Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 6.4 (for x86)
	Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 6.5 (for x86)
	Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64)
	SUSE(R) Linux Enterprise Server 10 Service Pack 2 for x86
	SUSE(R) Linux Enterprise Server 10 Service Pack 2 for EM64T
	SUSE(R) Linux Enterprise Server 10 Service Pack 3 for x86
	SUSE(R) Linux Enterprise Server 10 Service Pack 3 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 Pack 1 for x86
	SUSE(R) Linux Enterprise Server 11 Service Pack 1 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)

Abbreviation	Products
	Red Hat(R) Enterprise Linux(R) AS (4.8 for EM64T)
	Red Hat(R) Enterprise Linux(R) ES (4.8 for EM64T)
	Red Hat(R) Enterprise Linux(R) 5 (for x86)
	Red Hat(R) Enterprise Linux(R) 5 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 5.1 (for x86)
	Red Hat(R) Enterprise Linux(R) 5.1 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 5.2 (for x86)
	Red Hat(R) Enterprise Linux(R) 5.2 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 5.3 (for x86)
	Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 5.4 (for x86)
	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) 5.9 (for x86)
	Red Hat(R) Enterprise Linux(R) 5.9 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 5.10 (for x86)
	Red Hat(R) Enterprise Linux(R) 5.10 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 5.11 (for x86)
	Red Hat(R) Enterprise Linux(R) 5.11 (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(R) Enterprise Linux(R) 6.3 (for x86)
	Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 6.4 (for x86)
	Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64)
	Red Hat(R) Enterprise Linux(R) 6.5 (for x86)
	Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64)
Red Hat 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)

Abbreviation	Products
	Red Hat(R) Enterprise Linux(R) 5.9 (for x86) Red Hat(R) Enterprise Linux(R) 5.9 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.10 (for x86) Red Hat(R) Enterprise Linux(R) 5.10 (for Intel64) Red Hat(R) Enterprise Linux(R) 5.11 (for x86) Red Hat(R) Enterprise Linux(R) 5.11 (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) Red Hat(R) Enterprise Linux(R) 6.3 (for x86) Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.4 (for x86) Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64) Red Hat(R) Enterprise Linux(R) 6.5 (for x86) Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64)
RHEL-KVM	Red Hat(R) Enterprise Linux(R) 6.1 (for x86) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.1 (for Intel64) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.2 (for x86) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.2 (for Intel64) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.3 (for x86) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.3 (for Intel64) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.4 (for x86) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.4 (for Intel64) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.5 (for x86) Virtual Machine Function Red Hat(R) Enterprise Linux(R) 6.5 (for Intel64) Virtual Machine Function
Xen	Citrix XenServer(R) 5.5 Citrix Essentials(TM) for XenServer 5.5, Enterprise Edition Citrix XenServer(R) 6.0 Citrix Essentials(TM) for XenServer 6.0, Enterprise Edition Red Hat(R) Enterprise Linux(R) 5.3 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.3 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.4 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.4 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.6 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.6 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.7 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.7 (for Intel64) Linux Virtual Machine Function 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 Red Hat(R) Enterprise Linux(R) 5.9 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.9 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.10 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.10 (for Intel64) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.11 (for x86) Linux Virtual Machine Function Red Hat(R) Enterprise Linux(R) 5.11 (for Intel64) Linux Virtual Machine Function
XenServer 6	Citrix XenServer(R) 6.0 Citrix Essentials(TM) for XenServer 6.0, Enterprise Edition
DOS	Microsoft(R) MS-DOS(R) operating system, DR DOS(R)

Abbreviation	Products
SUSE Linux Enterprise Server	SUSE(R) Linux Enterprise Server 10 Service Pack 2 for x86 SUSE(R) Linux Enterprise Server 10 Service Pack 2 for EM64T SUSE(R) Linux Enterprise Server 10 Service Pack 3 for x86 SUSE(R) Linux Enterprise Server 10 Service Pack 3 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 Pack 1 for x86 SUSE(R) Linux Enterprise Server 11 Service Pack 1 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	Oracle Solaris10 05/09 (Update7) Media Pack Oracle Solaris11 11/11 Media Pack Oracle Solaris11.1 Media Pack
OVM for x86 3.2	Oracle VM Server for x86 v3.2.1 Oracle VM Server for x86 v3.2.2 Oracle VM Server for x86 v3.2.3 Oracle VM Server for x86 v3.2.4 Oracle VM Server for x86 v3.2.6 Oracle VM Server for x86 v3.2.7
OVM for SPARC	Oracle(R) VM Server for SPARC
SCVMM	System Center Virtual Machine Manager 2008 R2 System Center 2012 Virtual Machine Manager System Center 2012 R2 Virtual Machine Manager
VMware	VMware(R) Infrastructure 3 VMware vSphere(R) 4 VMware vSphere(R) 4.1 VMware vSphere(R) 5 VMware vSphere(R) 5.1 Vmware vSphere(R) 5.5
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 ESXi 5.1	VMware(R) ESXi(TM) 5.1
VMware ESXi 5.5	VMware(R) ESXi(TM) 5.5
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 5.1	VMware vSphere(R) 5.1
VMware vSphere 5.5	VMware vSphere(R) 5.5
VMware vSphere Client	VMware vSphere(R) Client
VMware vCenter Server	VMware(R) vCenter(TM) Server
VMware vClient	VMware(R) vClient(TM)

Abbreviation	Products
VMware Horizon View	VMware Horizon View 5.2.*x* VMware Horizon View 5.3.*x* VMware Horizon 6.0 (with View)
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
Excel	Microsoft(R) Office Excel(R) 2003 Microsoft(R) Office Excel(R) 2007 Microsoft(R) Office Excel(R) 2010
Excel 2003	Microsoft(R) Office Excel(R) 2003
Excel 2007	Microsoft(R) Office Excel(R) 2007
Excel 2010	Microsoft(R) Office Excel(R) 2010
Internet Explorer	Windows(R) Internet Explorer(R) 8 Windows(R) Internet Explorer(R) 9 Windows(R) Internet Explorer(R) 10 Windows(R) Internet Explorer(R) 11
RCVE	ServerView Resource Coordinator VE
ROR	FUJITSU Software ServerView Resource Orchestrator
ROR VE	FUJITSU Software ServerView Resource Orchestrator Virtual Edition
ROR CE	FUJITSU Software ServerView Resource Orchestrator Cloud Edition
Resource Coordinator	Systemwalker Resource Coordinator
Resource Coordinator VE	ServerView Resource Coordinator VE Systemwalker Resource Coordinator Virtual server Edition
Resource Orchestrator	FUJITSU Software ServerView Resource Orchestrator

Export Controls

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

Trademark Information

- BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries.

- Citrix(R), Citrix XenServer(R), 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-DOS, Windows Server, Windows Vista, Excel, Active Directory, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

- Firefox is a registered trademark or trademark of Mozilla Foundation in the United States and/or 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

Issue Date and Version

Month/Year Issued, Edition	Manual Code
November 2011, First Edition	J2X1-7606-01ENZ0(00)
December 2011, Edition 1.1	J2X1-7606-01ENZ0(01)
December 2011, Edition 1.2	J2X1-7606-01ENZ0(02)
February 2012, Edition 1.3	J2X1-7606-01ENZ0(03)
March 2012, Edition 1.4	J2X1-7606-01ENZ0(04)
April 2012, Edition 1.5	J2X1-7606-01ENZ0(05)
July 2012, Second Edition	J2X1-7606-02ENZ0(00)
October 2012, Third Edition	J2X1-7606-03ENZ0(00)
December 2012, Fourth Edition	J2X1-7606-04ENZ0(00)
January 2013, Fifth Edition	J2X1-7606-05ENZ0(00)
January 2013, Edition 5.1	J2X1-7606-05ENZ0(01)
January 2013, Edition 5.2	J2X1-7606-05ENZ0(02)
June 2013, Edition 5.3	J2X1-7606-05ENZ0(03)
August 2013, Edition 5.4	J2X1-7606-05ENZ0(04)
December 2013, Sixth Edition	J2X1-7606-06ENZ0(00)
February 2014, Edition 6.1	J2X1-7606-06ENZ0(01)
February 2014, Edition 6.2	J2X1-7606-06ENZ0(02)
April 2014, Edition 6.3	J2X1-7606-06ENZ0(03)
April 2014, Edition 6.4	J2X1-7606-06ENZ0(04)
June 2014, Edition 6.5	J2X1-7606-06ENZ0(05)
November 2015, Edition 6.6	J2X1-7606-06ENZ0(06)

Copyright

Contents

Chapter 1 Login and Logout

This chapter describes how to open and close the ROR console.

Preparations

Before opening the ROR console, be sure to read the following instructions and restrictions.

- When accessing the ROR console, be sure to enable the Compatibility View in Internet Explorer. Select [View]-[Encoding] in Internet Explorer, and check if [Auto-Select] is checked. If [Auto-Select] is not checked, select it.

- When downloading files using the ROR console, it is necessary to disable [Do not save encrypted pages to disk] in the Advanced Settings of the browser.

- The ROR console uses the Web browser's standard fonts and is designed to be viewed in a window of 1024 by 768 pixels or larger. When using a monitor with a higher resolution than this, it is recommended to enlarge the screen size. If the Web browser is resized by a significant amount, the display quality may deteriorate.

- The ROR console uses JavaScript, Active Script, Cookies, and IFRAMEs. These must be enabled in the Web browser settings before using the ROR console. Use SSL 3.0 and TLS 1.0.

- Specify either one of the following for the Web browser pop-up blocker:

  - Disable the pop-up blocker

  - Add the URL of the ROR Console to the **Address of web site to allow** setting.
    Check with the system administrator for the URL of the ROR Console.

- Surrogate pair characters cannot be used on the ROR Console.

- When opening the ROR console right after launching a Web browser, a warning window concerning the site's security certificate will be displayed.
  The following message is displayed: "There is a problem with this web site's security certificate." This warns the user that Resource Orchestrator uses a self-signed certificate to encrypt its HTTPS (SSL) communication with the Web browser.
  Resource Orchestrator generates a unique, self-signed certificate for each admin server during manager installation.
  Within a firewall-protected intranet, a network where the risk of identity theft is low, or where all correspondents are trusted, there is no risk in using self-signature certificates for communications. Accept the warning to display the Resource Orchestrator login screen. The login screen can be displayed by selecting the following option: "Continue to this web site (not recommended)."

- The background of the address bar will become red and the words "Certificate Error" will be displayed on the right side of the address bar of the login screen, the ROR console, and BladeViewer.
  Furthermore, the Phishing Filter may show a warning on the status bar. These warnings are referring to the same self-signed certificate issue discussed in the previous bullet. It is safe to continue with the current browser settings.

- To stop displaying the security certificate warning screen and the certificate error icon, create a certificate associated with the IP address or hostname of the admin server and add it to the Web browser.
  Refer to "Appendix B HTTPS Communications" in the "Design Guide VE" for details.

- In environments where the admin server is Windows, and multiple IP addresses are used, when a login window with a different URL from the address bar's URL in which the IP address or host name (FQDN) is specified, the warning may not disappear. Also, the following may occur.

  - The login window is not displayed

  - A certificate error occurs even though the certificate is registered

  Perform the following corrective action:

  - Windows Server 2008

    Set a higher priority for binding of the network adapter used on the admin LAN than for other network adapters.

    ### 📓 Example
    ....
    When changing the order of priority of network adapter binding in Microsoft(R) Windows Server(R) 2008 R2 Enterprise

1. Click <Start>, and then click [Control Panel].

2. When [Network and Internet] is displayed, click this item.

   When [Network and Internet] is not displayed, proceed to the next step without clicking.

3. Click [Network and Sharing Center], and click [Change adapter settings] in the left side of the window.

4. Click [Advanced Settings] in the [Advanced] menu.

   When the [Advanced] menu is not displayed, push the [Alt] key.

5. From the list of [Connections] in the [Adapters and Bindings] tab, click the target network adapter, and the "Up" or "Down" buttons to change the order of priority of connections.

6. Click <OK>.

- Windows Server 2012 or later

  On the admin server, set the metric of the admin LAN interface that is smaller than other interface.
  The metric value of interfaces can be checked using the "netstat -r" command.

Example

When modify the value of Interface metric in Microsoft(R) Windows Server(R) 2012 Standard

1. Press [Windows logo + R] key.

   [Run] will be opened.

2. Type ncpa.cpl and click <OK>.

3. Right-click the LAN Icon that connects, and click [Properties].

4. Click [Internet Protocol Version4 (TCP/IPv4)] and click [Properties] button.

5. Click [Advanced] button.

6. Uncheck [Automatic metric] in the [IP Settings], and input the value in [Interface metric] field.

Opening the ROR Console

This section explains how to access the ROR console.

Add the URL of the ROR console to the "Trusted sites" of the browser.

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

When Single Sign-On has been configured, the login window for Single Sign-On will be displayed. However, when Single Sign-On authentication has already been performed, the ROR console can be started without displaying the login window.
When Single Sign-On is not configured, the login window for Resource Orchestrator will be displayed.

Refer to "Chapter 10 Installing and Defining Single Sign-On" in the "Design Guide VE" for details on Single Sign-On.

> URL: https://*Admin_server_IP_address*:23461/

On a Windows admin server, the ROR console can also be opened by selecting [start]-[All Programs]-[Fujitsu]-[Resource Orchestrator]-[ROR console].

When modifying the URL of the start menu from localhost to the FQDN of an admin server, edit the following file:

- *System drive*\ProgramData\Microsoft\Windows\Start Menu\Programs\Fujitsu\Resource Orchestrator\ROR Console

  - Before Editing

    ```
    [InternetShortcut]
    URL=https://localhost:23461/
    ```

- After Editing

```
[InternetShortcut]
URL=https://FQDN:23461/
```

Note

- If the login screen is not displayed, confirm the following.

    - URL entered in address bar of the Web browser.

    - The proxy settings of the Web browser are correct.

    - The firewall settings on the admin server are correct.

- If already logged in from another Web browser window, login may be performed automatically (without displaying the login screen).

Login

In the login screen, enter the following items, and click <Login>.
The ROR console or BladeViewer is displayed after a successful login.

- User ID

- Password

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

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

Information

- During installation, enter the following user account name and password.

    - When Single Sign-On is configured

        The name of the user account and password used for ServerView Operations Manager

    - When Single Sign-On is not configured

        The user name and password of the user account specified in "2.1 Manager Installation" in the "Setup Guide VE".

- When logging in for the first time, the ROR console is displayed.

    However, when Single Sign-On is configured, the ROR console is always displayed.

- Opening the ROR console in multiple Web browsers may not allow multi-user login.
  To log in as a different user, start up a new Web browser from the Windows start menu.

- When logging in for the first time, the [Home] tab is displayed. When logging in for the second time and successive times, the tab that was displayed at the last logout is displayed.
  It is also possible for each user to set whether the [Home] tab is to be displayed at login. To change the option, click "Options" in the upper right corner of the ROR Console.

Logout

To log out, select "Logout" in the global header, and click <OK> in the confirmation dialog.

Note

. . . .

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

- If the ROR console or BladeViewer has been opened simultaneously in several Web browser windows, those login sessions may be terminated.

. . . .

Chapter 2 Home

This chapter explains the ROR Console Home window.

When the ROR Console is started, the Home window is displayed. Refer to "Chapter 1 Login and Logout" for information on how to start the ROR Console.

The elements of the Home window are explained below.

- Functions list

  The functions list displays the items that can be operated using ROR Console tabs.

  Click the triangle icon next to the Function list to toggle Display/Hide.

- Information

  Information from the Special Administrator and Infrastructure Administrator is displayed.

2.1 Editing the Home Messages

This section explains how to edit the messages that are shown in the lower section of the home window of the ROR console.

Information can be edited from the ROR console using the following procedure:

1. Click [Edit] on the upper-right side of the table.

2. The [Edit - Information] window is displayed.

   To add information, click [Add] on the [Edit - Information] window.

   To perform other operations, select information from the list, and then click [Move up]/[Move down], [Edit], or [Delete].

   Click [Save] to save the changes after operations have been completed.

   ### Adding Information

   This section explains how to add information.

   Perform the following procedure to add information.

   a. Click [Add] on the [Edit - Information] window.

      The [Add entry] dialog is displayed.

   b. Set the following items:

      Schedule

      There is no specified format.

      When not displaying the date, leave this field blank.

      Enter up to 30 alphanumeric characters or symbols. Commas (",") cannot be used.

      Messages

      Enter up to 250 alphanumeric characters or symbols.

   c. Click [OK].

      The entered information is added.

   ### Editing Information

   This section explains how to edit information.

   Perform the following procedure to edit information:

   a. Select the information to edit from the list.

   b. Click [Edit].

      The [Edit entry] dialog is displayed.

c. Set the following items:

Schedule

There is no specified format.

When not displaying the date, leave this field blank.

Enter up to 30 alphanumeric characters or symbols. Commas (",") cannot be used.

Messages

Enter up to 250 alphanumeric characters or symbols.

d. Click [OK].

The information is updated.

Moving Information

This section explains how to move information in the list.

Perform the following procedure to move information:

a. Select the information to move from the list.

b. Click [Move up] or [Move down].

The selected information is moved up or down one line.

Deleting Information

This section explains how to delete information.

Perform the following procedure to delete information:

a. Select the information to delete from the list.

b. Click [Delete].

The [Delete entry] dialog is displayed.

c. Click [Yes].

The selected information is deleted.

3. Click [Save] to save the changes after operations have been completed.

Click [Cancel] to discard the changes and return to the [Information] window.

P Point
. . . .
These messages can be used to inform all users of contact and enquiry information.
. . . .

Chapter 3 Resource Management Overview

This chapter provides an overview of the two views available on the [Resource] tab in Resource Orchestrator.

Resource Orchestrator provides two different GUIs on the [Resource] tab: the default window and BladeViewer.
Choosing an appropriate GUI depends on the administrator's authority level, or the kind of operations to be performed.

- ROR console

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

- BladeViewer

  BladeViewer offers a simplified, lifelike representation of blade servers and their statuses. While this enables intuitive operation, it does not include the tree-based navigation or detailed menus available in the [Resource] tab of the ROR console.
  BladeViewer makes it easier to monitor blade servers, visualize their hosted applications, and perform power operations. This makes BladeViewer suitable for administrators who only need to monitor blades and perform basic operations.

To switch the view of the [Resource] tab from the default window to BladeViewer, click <BladeViewer>>>. To switch the view of the [Resource] tab from BladeViewer to the default window, click <Advanced>>>.

Information

- All descriptions about the user interface other than those in "Chapter 6 BladeViewer" apply to the default window.

- For details on the [Resource] tab of the ROR console, refer to "Appendix A User Interface".

- For details on BladeViewer, refer to "Chapter 6 BladeViewer". This explains the BladeViewer screen and the functions that it provides.

- When logging in for the first time, the ROR console is displayed.
  Otherwise, the last view used before logging out (either the ROR console or BladeViewer) is displayed.

Chapter 4 License Setup and Confirmation

This chapter explains how to configure and confirm licenses.

License Setup

When using Resource Orchestrator, it is necessary to configure the license first.

Use the following procedure to configure the license:

1. After logging in to Resource Orchestrator, select [Tools]-[Licenses] from the menu, and click <Add> in the displayed dialog.

   The [Register License] dialog is displayed.

2. In the [Register License] dialog, enter the license key to register.

3. Click <OK>.

   The license will be registered.

Confirming the License

Use the following procedure to confirm the registered license:

1. After logging in to Resource Orchestrator, select [Tools]-[Licenses] from the menu, and click the license name in the displayed dialog.

   The [Licenses] dialog is displayed.

When using a command, execute the rcxadm license command.

For details on the rcxadm license command, refer to "5.10 rcxadm license" in the "Reference Guide (Command) VE".

Note

When "-" is displayed for "NUMBER_OF_LICENSES", the same number of agents as purchased licenses can be used.

Chapter 5 Managing User Accounts

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

Add User Account

Only privileged users can perform this operation.

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

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

   The [User Accounts] dialog is displayed.

2. Click <Add>.

   The [Add User Account] dialog is displayed.

3. Set the following:

   User ID

   Enter a character string beginning with an alphanumeric character and containing up to 16 alphanumeric characters, underscores ("_"), hyphens ("-"), and periods (".").
   Please note that user names are case-sensitive.

   Password (Confirm password)

   - When using Single-Sign-On

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

   - When not using Single-Sign-On

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

   Authority level

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

4. Click <OK>.

   The user account is created.

Change User Account Settings

Both privileged users and general users can perform this operation.
Privileged users can modify any account information. General users can only modify their own password.

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

   The [User Accounts] dialog is displayed.

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

   The [Change User Account] dialog is displayed.

3. Set the following:

   Password

   No change/Change

   Select the appropriate action.
   By default, the "No change" option is selected.

   Current password

   Enter a string using up to 16 alphanumeric characters or symbols.
   This is displayed when general users modify their own passwords.

New password (Confirm password)

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

Authority Level

No change/Change

Select the appropriate action.
By default, the "No change" option is selected.

Authority level

Select either "Manage" or "Monitor".
By default, the current authority level is selected.

4. Click <OK>.

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

Delete User Account

Only privileged users can perform this operation.

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

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

The [User Accounts] dialog is displayed.

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

The [Delete User Account] dialog is displayed.

3. Click <OK>.

The selected user account is deleted.

Chapter 6 BladeViewer

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

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

For details on the ROR console, refer to "Appendix A User Interface".

6.1 Overview

This section provides a functional overview of BladeViewer.

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

Figure 6.1 BladeViewer
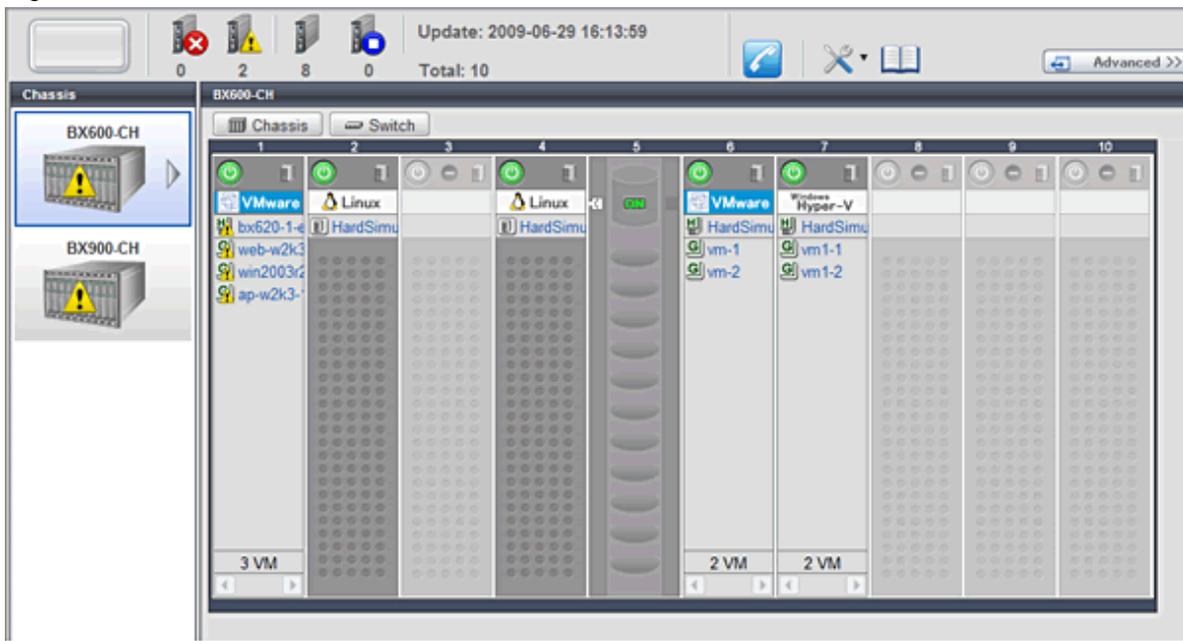
BladeViewer allows the following operations:

- Monitoring of resource statuses

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

  When using virtual servers, BladeViewer shows a list of VM guests for each VM host. This helps keeping track of relationships between VM guests and VM hosts.
  BladeViewer also makes it easy to confirm which operating systems (physical OS and guest OS) are affected by a hardware failure.

- Display and control of power status

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

- Display of custom labels and comments

  BladeViewer allows users to define custom labels and comments for each physical OS, VM host, and VM guest.
  Once defined, labels are shown on top of each displayed physical OS, VM host, and VM guest. Using labels to display application contents makes it easy to visualize what applications are running on each server blade and identify the applications affected by a server failure.
  Clicking on a label displays the comment defined for the related resource. Registering troubleshooting and recovery procedures beforehand can speed up the recovery of affected applications when a problem occurs.

- Display of contact information

BladeViewer allows users to define technical (support) contact information for their entire IT system. This contact information can be shown by clicking on the Contact icon.
Registering contact details of technical support staff beforehand can help streamline recovery procedures when problems occur.

6.2 Screen Layout

This section explains how the BladeViewer screen is organized.

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

Figure 6.2 BladeViewer: Screen Layout
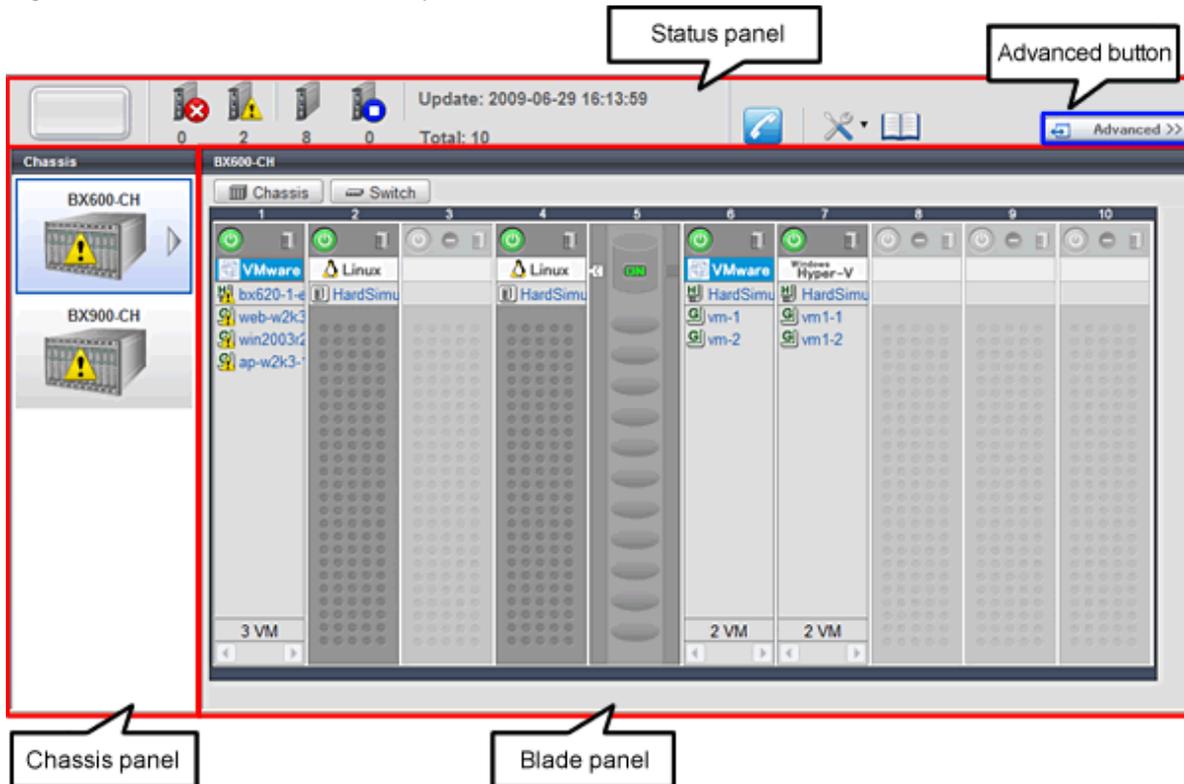
Status panel

This panel displays a summary of resources statuses.

Chassis panel

This panel displays the statuses of each registered chassis.

Blade panel

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

Information

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

6.3 Resource Status Monitoring

This section explains how to monitor resource statuses using BladeViewer.

6.3.1 Status Panel

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

When a problem occurs in the system, a red or yellow light icon starts blinking on the left side of the status panel.
Clicking the light icon changes its color back to gray.
The table below shows the status and meaning associated with each light icon.

Table 6.1 Light Icons

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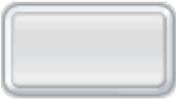
Information

. . . .

When the light icon blinks, it means that a warning or an error has been detected. Check the location of the problem from the chassis or blade panel.
If BladeViewer shows no resources with a warning or error status in either the chassis panel or blade panel, switch to the ROR console and check the event log to identify the cause of the problem.

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

. . . .

Table 6.2 Displaying the Server Icon and the Number of Units

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

* Note: N is the number of servers.

Table 6.3 Status Icons

Icon	Status	Meaning
None	Normal	The resource can be used normally.
⚠	Warning	An error occurred, however the resource can be used. Alternatively, the status of some resources cannot be obtained.
❌	Error	A fault or error occurred, therefore the resource cannot be used.
⏹	Stop	The resource is stopped, therefore it cannot be used.

6.3.2 Chassis Panel

The chassis panel displays the statuses of each registered chassis.

Table 6.4 Chassis Icon

Icon	Meaning
	Chassis

See

. . . .

For details on the different chassis statuses, refer to "Table 6.3 Status Icons" of "6.3.1 Status Panel".

If a chassis icon shows a warning or error status, it means that a problem occurred in a resource contained in the chassis.
For details on how to identify faulty resources, refer to "6.3.3 Blade Panel".

. . . .

Information

. . . .

Selecting a chassis icon from the chassis panel displays the contents of that chassis in the blade panel.
For details, refer to "6.3.3 Blade Panel".

. . . .

6.3.3 Blade Panel

The blade panel displays the statuses of all the resources inserted into the selected chassis. Those resources are shown in a format representative of their physical configuration (shape and position).
To display the contents of a specific chassis in the blade panel, click on its icon in the chassis panel.

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

Table 6.5 Chassis Icon

Icon	Meaning
	Chassis

Table 6.6 LAN Switch Icons

Icon	Meaning
	LAN switches

See

. . . .

For details on the status icons that are displayed for the chassis and its LAN switches, refer to "Table 6.3 Status Icons" of "6.3.1 Status Panel".

. . . .

6.3.3.1 Resource List

The blade panel graphically displays each slot within a chassis. Each server or storage blade is displayed according to its actual position (slot) within the chassis.
Note that an unregistered server is shown in light gray while an empty slot is shown in white.

Figure 6.3 Blade Panel: Resource List
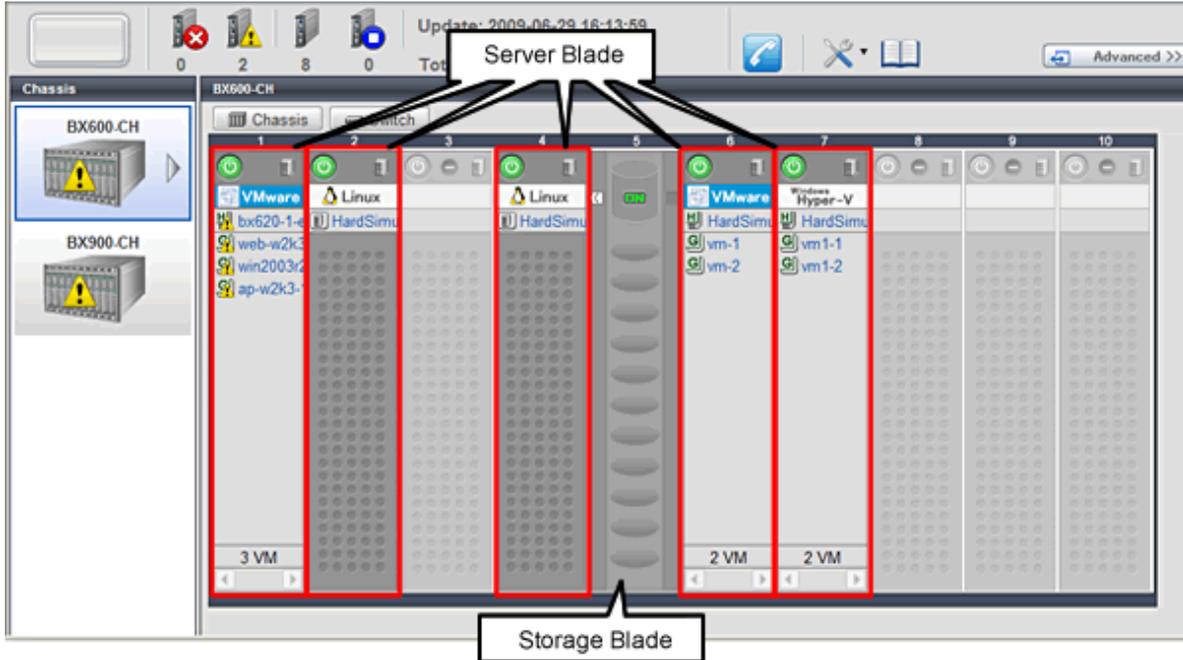
Server Blade

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

Table 6.7 Server Blade Power Buttons

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

Information
. . . .

The power status of a server blade can be easily controlled by clicking on its power button.
For details, refer to "6.4.1 Server Blade".
. . . .

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

Table 6.8 Physical Server Icons

Icon	Meaning
	Server
	Spare server
	Unregistered server
	Maintenance mode server

See

For details on the different physical server statuses, refer to "Table 6.3 Status Icons" in "6.3.1 Status Panel".

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

Table 6.9 Admin Server Icon

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

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

Table 6.10 OS Icons

Icon	Meaning
Windows	Windows OS
Linux	Linux OS
VMware	VMware host OS
Windows Hyper-V	Hyper-V host OS
XenServer™	Citrix XenServer host OS
Xen®	Linux Xen host OS
KVM	KVM host OS
OVM86	OVM for x86 host OS
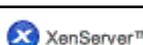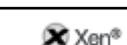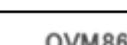
Information

Clicking on a VM host OS icon displays a detailed list of the VM guests operating on the selected VM host.
For details, refer to "6.3.3.2 VM Guest List".

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

- If no label is set

    The OS name is displayed.

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

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

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

Table 6.11 Resource Icons

Icon	Meaning
	Physical OS
	VM host
	VM guest

 See
....

For details on the resource status, refer to "Table 6.3 Status Icons" in "6.3.1 Status Panel".
....

 Information
....

If a comment has been defined for a server, clicking on its label displays the [Server Properties] dialog.
The [Server Properties] dialog displays the comment and label set for the selected server, as well as its OS name, server name (for a physical OS, the physical server name, for a VM guest, the VM guest name), and IP address.
For details on defining comments, refer to "6.5.1 Listing and Editing of Labels and Comments".
....

Storage Blade

A power lamp is displayed in the top part of each storage blade.
The table below shows the status and meaning associated with each power lamp.

Table 6.12 Storage Blade Power Lamps

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

6.3.3.2 VM Guest List

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

Figure 6.4 Blade Panel: VM Guest List
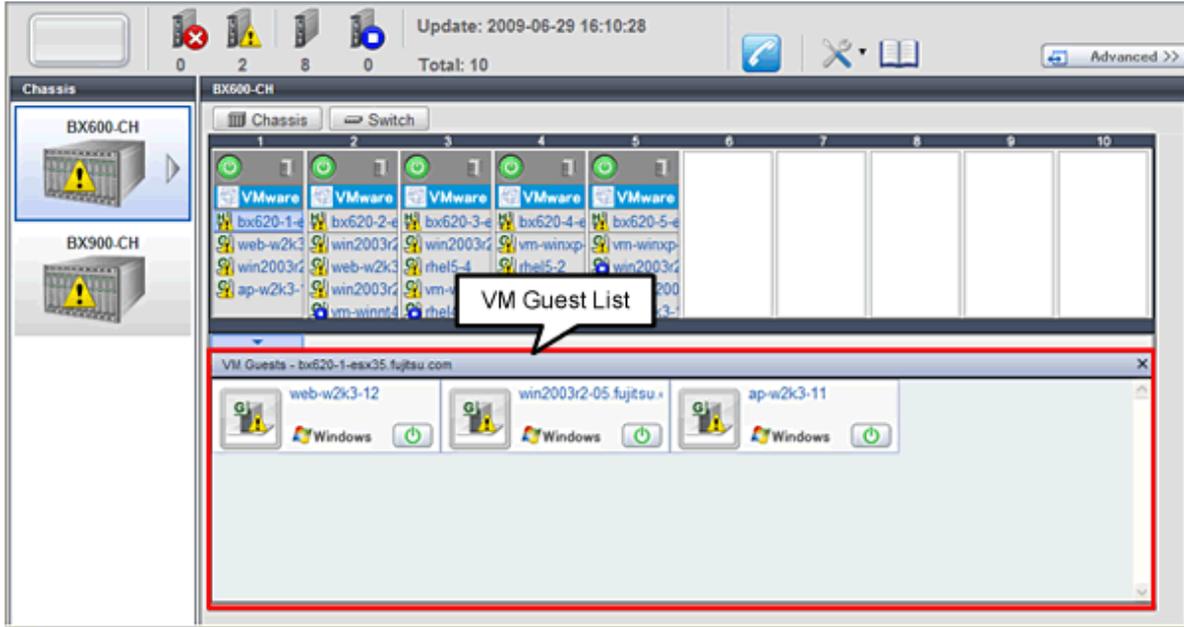
A VM guest icon is shown on the left side of each VM guest displayed in the VM guest list.

Table 6.13 VM Guest Icon

Icon	Meaning
	VM guest

See

For details on the different VM guest statuses, refer to "Table 6.3 Status Icons" in "6.3.1 Status Panel".

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

- If no label is set

  The OS name is displayed.

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

  The VM guest name is displayed.

An OS icon is displayed below the label.
For details on the different OS icons, refer to "Table 6.10 OS Icons" in "6.3.3.1 Resource List".

A power button is displayed on the lower-right side of each VM guest.
This power button represents the power status of each VM guest, as shown below.

Table 6.14 VM Guest Power Buttons

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

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

Information
. . . .

The power status of a VM guest can be easily controlled by clicking on its power button.
Refer to "6.4.2 VM Guest" for details.
. . . .

6.3.4 Resource Details

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

- Chassis

  Clicking a chassis icon (from the blade panel) opens up its management blade's Web interface in a new window.
  This Web interface provides more details on the chassis' status and contents.
  For details on the chassis icon, refer to "6.3.3 Blade Panel".

- LAN switches

  Clicking on a LAN switch icon opens up its LAN switch details screen.
  This screen provides more details on the LAN switch's status and configuration.
  For details on the LAN switch icon, refer to "6.3.3 Blade Panel".

- Physical Server

  Clicking on a physical server icon opens it up in the ServerView Operation Manager's Web interface.
  This interface provides more details on the physical server's status and its internal components.
  For details on the physical server icon, refer to "Table 6.8 Physical Server Icons" in "6.3.3.1 Resource List".

6.4 Power Control

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

6.4.1 Server Blade

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

Table 6.15 Actions of Server Blade Power Buttons

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

Power On

Clicking on a power button that shows "Power OFF" status will power on the target server blade. A confirmation dialog is displayed first.
Clicking <OK> in the confirmation dialog powers on the server and starts its OS.
At this time, the power button changes to an intermediate "Power ON in progress" state (green - blinking). The power button finally displays a "Power ON" state after confirming that the OS has started up correctly on the target server.

Power Off and Reboot

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

Figure 6.5 Power Operation Dialog
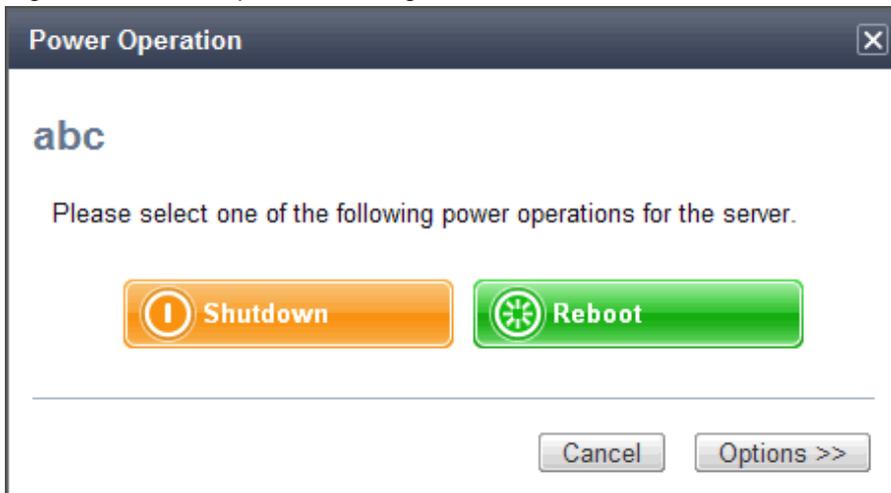
- "Shutdown"

Selecting "Shutdown" will shut down the target server blade. A confirmation dialog is displayed first.
Clicking <OK> in the confirmation dialog shuts down the OS and powers off the managed server.
At this time, the power button changes to an intermediate "Power OFF in progress" state (orange - blinking). The power button finally displays "Power OFF" status after confirming that the target server has been shut down correctly.

- "Reboot"

Selecting "Reboot" will reboot the target server blade. A confirmation dialog is displayed first.
Clicking <OK> in the confirmation dialog shuts down the OS and reboots the managed server.
At this time, the power button changes to an intermediate "Power ON in progress" state (green - blinking). The power button finally displays "Power ON" status after confirming that the OS has started up correctly on the target server.

Forced Power Off and Reboot

Clicking on a power button that shows "Power ON" status, and selecting <Options >>> in the displayed [Power Operation] dialog enables selection of the "Force Shutdown" and "Force Reboot" actions.
A forced shutdown (or reboot) will forcibly power off (or reboot) the managed server blade without waiting for its OS to shut down cleanly.

Figure 6.6 Power Operation Dialog (with Additional Options)

- "Force Shutdown"

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

- "Force Reboot"

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

![Note]

[VMware] [Hyper-V] [Xen] [Citrix Xen] [KVM] [Solaris Zones] [OVM for x86 3.2] [OVM for SPARC]
Take caution regarding the following points when powering-off or rebooting a VM host.

- When using a server virtualization software's high-availability feature, confirm that the server is set to VM maintenance mode within that virtualization software. This can be confirmed from the virtualization software client.

- Perform power operations only after setting VM maintenance mode (either from the VM management software client or using the resource control command).
  Refer to the server virtualization software manual, or to "3.2 rcxadm server" in the "Reference Guide (Command) VE" for details.
  Depending on the server virtualization software used, some restrictions may apply to the use of VM maintenance mode settings. For details about such restrictions, refer to "D.3 Functional Differences between Products" in the "Design Guide VE".

6.4.2 VM Guest

The power status of a VM guest can be controlled by clicking the OS icon of its VM host and then clicking its power button in the list of VM guests that is displayed.
Clicking on the power button provides power controls similar to those provided for server blades.

Table 6.16 Actions of VM Guest Power Buttons

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

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

![Note icon] **Note**

· ·

- VM guests need to be properly configured in order to use the shut down or reboot buttons.
  Attempting to shut down or reboot a VM guest that is not properly configured will result in an error.
  For details, refer to "D.2 Configuration Requirements" in the "Design Guide VE".

- Depending on the server virtualization environment, a VM guest may automatically migrate to another VM host when a power control operation is performed. This may cause power control operations to fail and return an error when used on VM guests.
  For details, refer to "D.3 Functional Differences between Products" in the "Design Guide VE".

- A VM guest can be configured to automatically start or stop whenever its VM host starts up or shuts down. This can be achieved by configuring the VM guest's startup and shutdown options in the server virtualization software used.
  For details, refer to the server virtualization software manual.

[Windows]

- Take caution regarding the following points when shutting down or rebooting a managed server running a Windows operating system.

  - If Windows is not configured to shut down when the computer's power button is pressed, the power operations in Resource Orchestrator may not function properly.
    To check this option, access the Control Panel, open the [Power Options], and check the settings of the [Advanced] tab in the [Power Options Properties] window.

  - If a file is being edited by a logged-in user, a dialog prompting the user to save the file is displayed, and the system may not shut down immediately.
    In such cases, shutdown does not take place until the user takes the appropriate action or a specified time (approximately five minutes) has elapsed.

· ·

6.5 Status Panel Operations

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

Figure 6.7 BladeViewer: Tool Icons
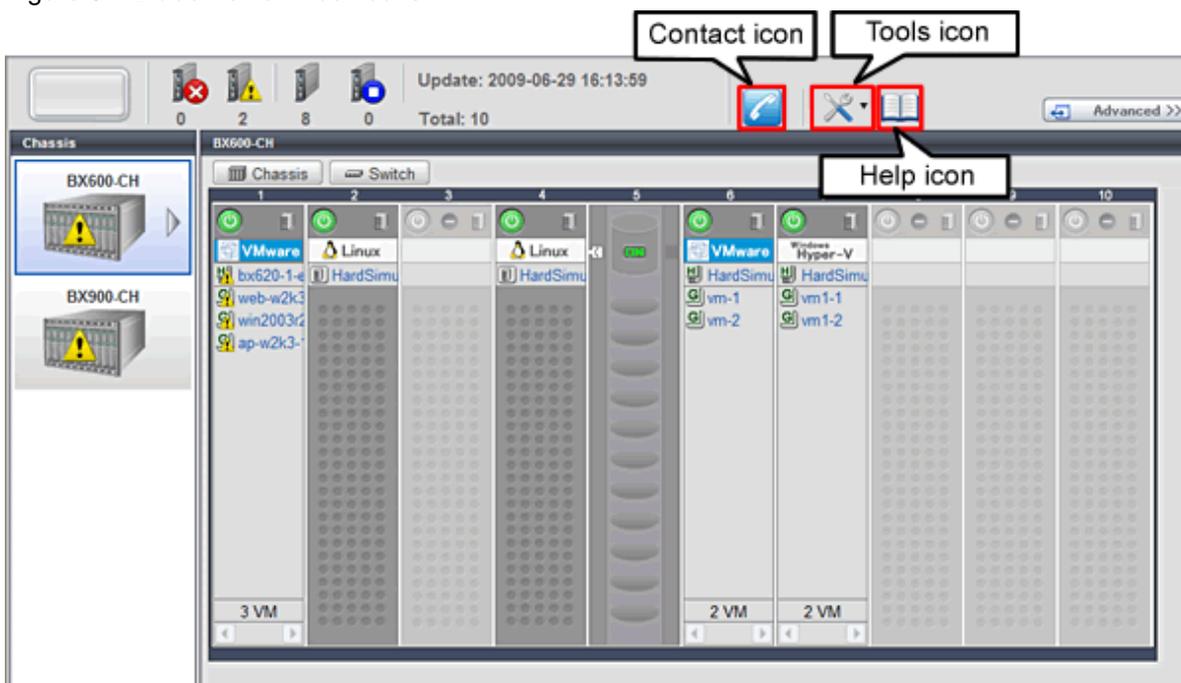
Contact icon

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

Tools icon

Enables selection of the following menu options:

Display Label List

Displays the [Label List] dialog.
Displays a list of labels. This list also allows modification of labels and comments.
For details on editing labels and comments, refer to "6.5.1 Listing and Editing of Labels and Comments".

Set Contact Information

Displays the [Set Contact Information] dialog.
For details on modifying contact information, refer to "6.5.2 Editing Contacts".

Change Password

Displays the [Change Password] dialog.
For details on changing passwords, refer to "6.5.3 Changing Passwords".

Help icon

The Help is displayed.

6.5.1 Listing and Editing of Labels and Comments

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

Figure 6.8 Label List
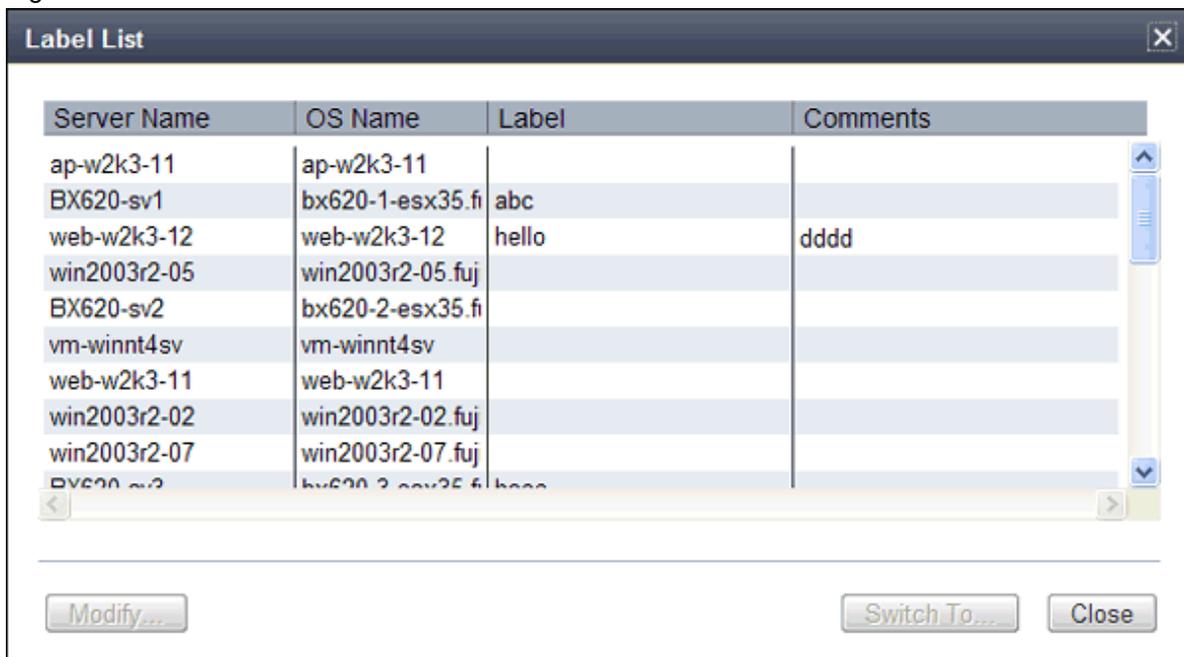
Contents of the Label List

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

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

Editing Labels and Comments

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

- Privileged user

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

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

  Label

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

  Comment

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

  Note

  ⁃⁃⁃

  New lines are counted as two characters.

  ⁃⁃⁃

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

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

- General user

  If logged in as a general user, <Show> is displayed in place of <Modify> in the [Label List] dialog.
  Clicking <Show> displays the [Server Properties] dialog, but does not allow editing of labels or comments.

6.5.2 Editing Contacts

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

Enter the following item.

Contact

The currently defined contact information is displayed.
Enter a maximum of 256 characters.

Note

⁃⁃⁃

New lines are counted as two characters.

⁃⁃⁃

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

6.5.3 Changing Passwords

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

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

- Privileged user

  New password (Confirm password)

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

- General user

  Current password

    Enter the password that is currently set.
    Enter a string using up to 16 alphanumeric characters or symbols.

  New password (Confirm password)

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

Chapter 7 Registering Resources

This chapter explains how to register, change, and delete resources used by Resource Orchestrator.
The Resource Orchestrator manager must be completely installed beforehand.

In addition to the usual method of registering each resource individually, it is also possible to register or change registered settings of multiple resources in batches using the pre-configuration function.

- Registering or modifying resources individually

    This method is used when the number of servers to be installed is small (from one to four), or when adding a similar number of servers to an existing environment.

- Registering or modifying multiple resources collectively

    This method is used when there are many (five or more) servers to be installed.

For information on how to register and modify multiple resources together, refer to "Chapter 12 Pre-configuration for Resource Registration and Modification".

Information

- **User Accounts**

    When creating new user accounts, changing passwords, or modifying permission levels during setup, refer to "Chapter 5 Managing User Accounts".

- **Backing up the Admin Server**

    The admin server should be backed up after the entire system has been completely set up, or after registering, changing, or deleting resources.
    For information about backing up the admin server, refer to "Chapter 9 Backup and Restoration of Admin Servers" in the "Operation Guide VE".

7.1 Registering VIOM Coordination

Use the following procedure to configure management software settings:

1. From the ROR console menu, select [Settings]-[Register]-[Management Software (VIOM)].

    The [Register Management Software(VIOM)] dialog is displayed.

2. Perform the following settings:

    User ID

        Enter the ID of a VIOM user account.

    Password

        Enter the password of the above VIOM user account.

3. Click <OK>.

7.1.1 Registering VIOM Server Profiles

Use the following procedure to configure VIOM server profiles:

1. Select Management Software (VIOM) from the ROR console, and then select the [Resource Details] tab.

2. In General of the [Resource Details] tab, click the link for the Management software.
    The Web interface of ServerView Virtual-IO Manager starts up.

3. Refer to the ServerView Virtual-IO Manager manual to configure server profiles.

Note

....

HBA address rename and VIOM cannot be used together within the same chassis.

....

When using backup and restore or cloning, prioritize the following two boot operations:

1. Boot from the first admin LAN network interface (NIC1 (Index1))

2. Boot from the network interface used by the admin LAN (NIC2 (Index2))

When not using the onboard LAN of rack mount and tower servers as the admin LAN, refer to "".

7.1.2 When Using Rack Mount and Tower Servers

When managing rack mount and tower servers, the position of admin LAN is specified with "cardinfo" in the following definition file. By default, the onboard LAN is the admin LAN.

Storage Location of the Definition File

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

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

Definition File Name

server_spec.rcxprop

Character Code

[Windows Manager] [Linux Manager]
UTF-8

Line Break Code

[Windows Manager]
CR/LF

[Linux Manager]
LF

Definition File Format

- The following line must be entered in the first line of definition files.

    ```
    ServerSpec,V1.1
    ```

- In the definition file, enter the configuration information (CPU core count, CPU clock speed, memory capacity, card information, etc.), separated by commas (",").

- When defining two or more servers, use line breaks.

    Enter each line in the following format.

    ```
    model_name, cpu_core_count, cpu_clock, memory_size, cpu_type, cardinfo
    or
    physical_server, cpu_core_count, cpu_clock, memory_size, cpu_type, cardinfo
    ```

- Blank spaces between data and commas (",") are ignored.

- If there is duplicated configuration information (CPU core count, CPU clock speed, memory capacity, etc.) for the same physical server, the values that appear first will be used.

- When adding comments, start the line with a number sign ("#").

Definition File Items

model_name

Enter the model name of the managed server.
Enter "[" for the first character, and "]" for the last character.
The model name displayed in the General information of the Resource Details window.

physical_server

Enter the same physical server name as the one entered when registering a managed server.
Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

cpu_core_count

The total number of physical CPU cores.
Enter "0", because this is not used when changing the specified admin LAN.

cpu_clock

The CPU clock speed.
Enter "0", because this is not used when changing the specified admin LAN.

memory_size

The total memory size.
Enter "0", because this is not used when changing the specified admin LAN.

cpu_type

The CPU type.
Do not enter the value, because this is not used when changing the specified admin LAN.

cardinfo

Enter the information for cards mounted on servers.
Specify the NIC used for the admin LAN.
Enter the information for each card in the following format. Use colons (":") to separate each piece of card information.

- Card type

  Enter one of the following card types:

  - "LAN"

  - "FC"

  - "CNA"

  If something other than the above is entered, the card information will be invalid.

- Slot type

  Enter the slot type.
  Enter an integer between 0 and 9 for the slot type, based on the following.

  - "0": Onboard

  - "1" to "9": PCI slot numbers

- Port number

  Enter the port numbers. Enter an integer between 1 and 9 for the port number, preceded by a hyphen ("-").

- Flag to confirm if the LAN card is used for an admin LAN

  When using a LAN card for an admin LAN, enter "**" or "*" to indicate that the LAN card is used for an admin LAN.
  When using the card for a LAN other than an admin LAN, do not enter anything.

  This item is enabled when the card type is set to "LAN" or "CNA".

  - The card for the primary admin LAN: Enter "*".

- The card for the secondary admin LAN: Enter "**".

- A card not for an admin LAN: Leave blank.

📝 Example

. . . .

In the following an example, admin LAN is ports 1 and 2 of the PCI slot1.

```
ServerSpec,V1.1
[PRIMERGY RX300 S7],0,0,0,,LAN0-1:LAN0-2:LAN1-1*:LAN1-2**
server00,0,0,0,,LAN0-1:LAN0-2:LAN1-1*:LAN1-2**
```

. . . .

7.2 Registering VM Management Software

This section explains how to register VM management software.

Registration of VM management software (such as VMware vCenter Server) is necessary to enable VM guest migrations.
For details on the required VM management software settings, refer to "D.2 Configuration Requirements" in the "Design Guide VE".

Use the following procedure to register VM management software:

1. From the ROR console menu, select [Settings]-[Register], and then select the type of the VM management software to use.

   The [Register Management Software(*name*)] dialog is displayed.
   In *name*, the type of the VM management software is displayed.

2. Perform the following settings:

   Management software name

   Enter the name of the target VM management software.
   Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens
   ("-").

   Location

   Select the location where the VM management software to register is operating.

   - If VM management software is installed on the admin server

     Select [Admin Server].

   - In other cases

     Select [Other Server].
     Selecting this option activates the IP address field. Enter the IP address of the server on which VM management software
     is installed.
     By default, [Admin Server] is selected.

   IP address

   Enter the IP address of VM management software. When specifying [Admin Server] for the location, entry is not possible, as
   the IP address of admin server remains displayed.
   Enter the IP address using periods ".".

   📙 Note

   . . . .

   When receiving SNMP traps from VM management software (VMware vCenter Server), the configured IP address and the
   SNMP trap source IP address of the VM management software (VMware vCenter Server) should be the same. The SNMP trap
   source IP address is the IP address of the protocol with the highest priority of protocol binding. When changing the SNMP trap
   source IP address, change the order of protocol binding.

   . . . .

User ID

Enter the user ID to use to control VM management software.
Enter up to 84 characters, including alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e).

Password

Enter the password for VM management software.
Enter up to 128 characters, including alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e).

3. Click <OK>.

VM management software is registered with the entered information.

Information

Registration and management of multiple VM management software packages (VMware vCenter Server, etc) are possible.
It is also possible to register a single VM management product multiple times and use it for management.

The following VM management software can be registered in Resource Orchestrator.

- VMware vCenter Server

- System Center Virtual Machine Manager

7.3 When Using Blade Servers

This section explains how to register resources when using blade servers.

When using blade servers, use the following procedure to register resources:

- Register Chassis

- Register blade servers

- Register LAN switch blades

- Configure VLANs on LAN switch blades

7.3.1 Registering Chassis

This section explains how to register a chassis.

Registering chassis makes it possible to use the optional power monitoring settings.
When collecting power data, perform the power data collection settings according to "9.6.1 Changing Environmental Data Settings".
For details on devices supporting power monitoring, refer to "2.5 Hardware Environment" in the "Design Guide VE".

By registering a chassis, every server blade mounted in the chassis will be automatically detected and displayed as an unregistered server in the server resource tree. Register these managed servers individually.

For details on registering servers to manage, refer to "7.3.2 Registering Blade Servers".

Use the following procedure to register a chassis:

1. In the ROR console server resource tree, right-click "Server Resources", and select [Register]-[Chassis] from the popup menu.

   The [Register Chassis] dialog is displayed.

2. Perform the following settings:

   Admin LAN (IP address)

   Enter the IP address that was set on the chassis management blade.
   Enter the IP address using periods ".".

Chassis name

Enter a name to assign to this chassis.

Enter a character string beginning with an alphabetical character and containing up to 10 alphanumeric characters and hyphens ("-").

SNMP Community

Enter the SNMP community that was set on the chassis management blade.

Either select "public" or enter an arbitrary string.

Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

3. Click <OK>.

The mounted chassis will be displayed under the server resource tree.

Any server blade mounted within this chassis will be detected automatically and shown as: [*chassis_name-Slot_number*[Unregistered]].

The only operation available for those unregistered server blades is server registration, while the ROR console can only display their hardware statuses and properties.

If the manager is installed on one of those server blades, this blade will be shown as: [*chassis_name-Slot_number*[Admin Server]]. In that case, server registration will not be available for the admin server, but its hardware status and properties will be displayed in the ROR console.

7.3.2 Registering Blade Servers

To register a blade server (PRIMERGY BX series), its enclosing chassis must be registered first.

When using VIOM for I/O virtualization, VIOM server profiles should be registered in advance according to the procedure described in "7.1.1 Registering VIOM Server Profiles".

To register blade servers other than PRIMERGY BX servers, refer to "7.4 When Using Rack Mount and Tower Servers".

Figure 7.1 Status Transition Diagram for Managed Servers
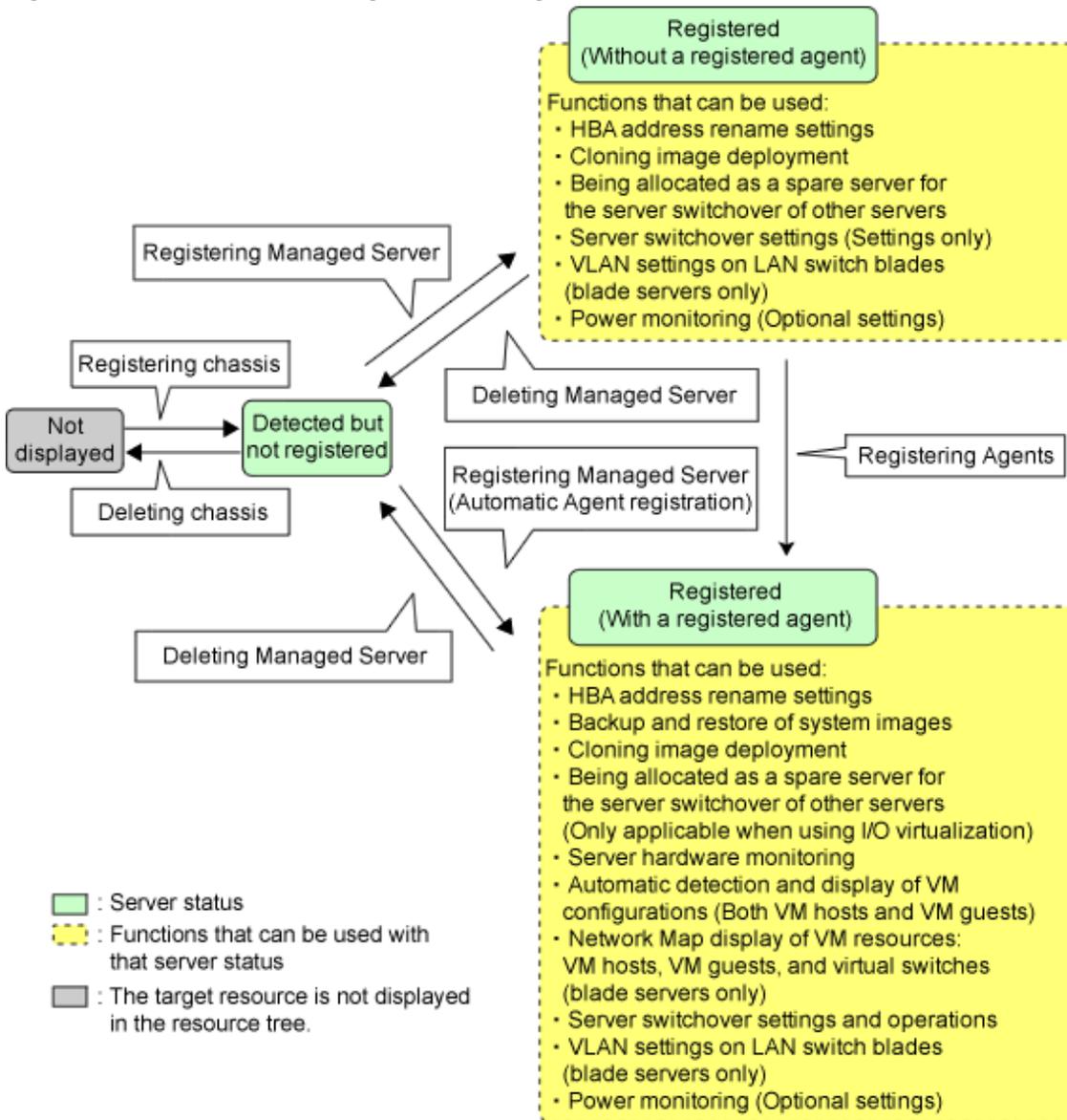
Use the following procedure to register blade servers.

1. In the ROR console server resource tree, right-click an unregistered server blade or partition in the target chassis, and select [Register]-[Server] from the popup menu.

   The [Register Server] dialog is displayed.

2. Perform the following settings:

   Physical Server Name

   > Enter a name to assign to this physical server.
   > Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

   Admin LAN (IP address)

   > Enter the IP address used by this server on the admin LAN.

   > **When IP address is displayed**
   > Entering an admin LAN (IP address) is not required.
   > Agents are automatically registered.

Note

- If ServerView Agents (mandatory software) is not running, message number 67231 will be displayed. In this case, server registration succeeds, but the agent is not registered.

  For details on the appropriate corrective action, refer to "Message number 67231" in "Messages".

- If the admin LAN (IP address) of servers not running a physical OS or a VM host are displayed, old information may have been being displayed. After canceling registration of the server, right-click the chassis on the server resource tree and select [Update] from the popup menu to request an update of hardware properties. The IP address is updated to the correct value (it takes several seconds to obtain the information and to update).

When IP address is not displayed
Enter the IP address of this server's admin LAN network interface.
The Agent will not be registered automatically, but can be manually registered after server registration if necessary. After registering servers, register agents as required.
For details on registering agents, refer to "Chapter 7 Installing Software and Registering Agents on Managed Servers" in the "Setup Guide VE".

Information

When a physical OS and VM host are running on this server, the admin LAN (IP address) may be obtained automatically.
After canceling registration of the server, right-click the chassis on the server resource tree and select [Update] from the popup menu to request an update of hardware properties.
If the IP address is not shown after going through the above procedure, set it by manually entering the IP address and registering the server.

Server OS category

This option is displayed if the target server runs a physical OS or VM host.
Select the appropriate server OS category (Physical OS or VM host).
Selecting [VM Host] activates the user ID and password input fields. Those refer to the user name and password entered during installation of this VM host.
Select the server OS category depending on whether the relevant server is used on a physical OS or a VM host.

- For a Physical OS

  Select [Windows/Linux] or [Solaris].

- For a VM Host

  Select [VM Host], and enter the VM host login account information.
  This login account information will be used by Resource Orchestrator to control and communicate with the registered VM host.

User ID

Enter the user ID to log in to the VM host. Specify a user ID that has VM host administrator authority.

Password

Enter the password of the user to log in to the VM host.

[Apply Admin LAN NIC settings] checkbox

The checkbox is displayed only for blade servers (PRIMERGY BX servers).

- When not changing the Admin LAN NIC settings

  NIC1 (Index1) and NIC2 (Index2) are used, without changing the NICs used for the admin LAN, the HBA address rename setup service, or for redundancy of the admin LAN.

- When changing the Admin LAN NIC settings

NIC1 (Index1) and NIC2 (Index2) are used as the NICs for the admin LAN, the HBA address rename setup service, and redundancy of the admin LAN.
Select the NICs to use from Admin LAN (MAC address1) and Admin LAN (MAC address2).

Admin LAN (MAC address 1)

Displayed when the [Apply Admin LAN NIC settings] checkbox is selected.
Select the NIC to use for the admin LAN. The IP address allocated to the selected NIC is displayed in [Admin LAN (IP address)].
When an IP address is not allocated, specify the admin LAN (IP address) of the server to register.

Admin LAN (MAC address 2)

Displayed when the [Apply Admin LAN NIC settings] checkbox is selected.
Select the NICs used for the HBA address rename setup service or for admin LAN redundancy.
For the following cases, select the [Disable MAC address 2].

- When not using the HBA address rename setup service

- When not performing admin LAN redundancy

Note

- For details about the network interfaces used on the admin LAN, refer to "7.1 Network Configuration" in the "Design Guide VE".
  If an incorrect network interface is used, Resource Orchestrator will use a wrong MAC address for the admin LAN.
  An admin LAN IP address is required even when registering a spare server.
  Enter an IP address that does not conflict with the IP address of any other managed server on the admin LAN.

- When using backup and restore, cloning, or HBA address rename, the NIC (or LAN expansion board) must support PXE boot.

- When registering a newly-mounted PRIMERGY BX900 server, as recognition of this server blade's admin LAN MAC address will take time, error message number 61142 may be displayed.
  In this case, after registration has been canceled, right-click the chassis on the server resource tree and select [Update] from the popup menu to request an update of hardware properties. This will update the MAC address to the correct value. This may also take a few minutes to obtain hardware information and update internal properties.
  Confirm that the correct MAC address is displayed correctly before registering the server again.

  For details on the appropriate corrective action, refer to "Message number 61142" in "Messages".

- A server running a VM host can still be registered as a physical OS if its [Server OS category] is set to [Windows/Linux]. (For Windows Server 2008, etc.)
  A VM host server that was mistakenly registered as a physical OS should be deleted and re-registered as a VM host.

- The same NIC cannot be selected for [Admin LAN (MAC address 1)] and [Admin LAN (MAC address 2)].

- For the following cases, after selecting [Disable MAC address 2] for [Admin LAN (MAC address 2)], the lowest numbered NIC which is not used for [Admin LAN (MAC address 1)] is used for Admin LAN2.

  - When using the HBA address rename setup service

  - When performing admin LAN redundancy

3. Click <OK>.

   The registered server will be displayed in the server resource tree.

Note

- When an agent is registered on a VM host, all VM guests running on that VM host are also registered automatically. Whenever a VM guest is created, modified, deleted, or moved on a registered VM host, the changes are automatically updated in the server resource tree.

- The VM guest name displayed in the ROR console is either the VM name defined in its server virtualization software or the host name defined in the guest OS.

The timing at which the host name of a guest OS is detected and displayed varies according its server virtualization software. For details, refer to "D.3 Functional Differences between Products" in the "Design Guide VE".

- It is recommended not to use duplicate names for physical OSs, VM hosts, and VM guests. If duplicated names are used, those resources cannot be managed from the command-line.

- When registering a server on which the agent was installed, it is necessary to either reboot the server or restart its related services (explained in the "2.2 Starting and Stopping Agents" in the "Operation Guide VE") after server registration. This step has to be done before running any image operation (system image backup or cloning image collection).
  For details on how to restart the agent, refer to "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

7.3.3 Registering LAN Switch Blades

To register a LAN switch blade, its enclosing chassis must be registered first.

Use the following procedure to register a LAN switch blade.

1. In the ROR console server resource tree, right-click an unregistered LAN switch blade from the target chassis, and select [Register]-[LAN Switch] from the popup menu.

   The [Register LAN Switch] dialog is displayed.

2. Perform the following settings: For a LAN switch blade PY CB 10Gb FEX Nexus B22, only the LAN switch name can be configured.

   LAN switch name

      Enter the name to assign to this LAN switch blade.
      Enter up to 15 characters, including alphanumeric characters (upper or lower case), underscores ("_"), or hyphens ("-").

   Admin port

      When using LAN switch blade PY CB Eth Switch 10/40Gb 18/8+2, it is a set item.

      Select either [oob] or [cfab]. The default setting is [oob]

   Admin LAN (IP address)

      Enter the admin LAN IP address that was set on this LAN switch blade.
      Enter the IP address using periods ".".

      When using LAN switch blade PY CB Eth Switch 10/40Gb 18/8+2, Enter the IP address corresponding to the admin port.

         - When the admin port is cfab

            Enter the virtual IP address of Converged Fabric

         - When the admin port is oob

            Enter the IP address of oob

   User ID

      Enter the name of a telnet or SSH user account that can log in to this LAN switch blade.
      For a LAN switch blade PY CB DCB SW 10Gb 18/6/6, enter the name of the administrator account for the LAN switch blade.

   Password

      Enter the password of the above telnet or SSH user account.

   Connection method

      Select either [Telnet] or [SSH]. The default setting is as follows:

         - LAN switch blade PY CB DCB SW 10Gb 18/6/6 or PY CB Eth Switch 10/40Gb 18/8+2

            [SSH]

         - In other cases

            [Telnet]

Administrative password

Enter the password of this LAN switch blade's telnet or SSH administrator account.

If the user ID and the password of the administrator account for the LAN switch blade were set in [User ID] and [Password], simply re-enter the same password in this field. In this case, Resource Orchestrator does not check whether the password entered here matches the password set on the LAN switch blade.

SNMP Community

Enter the SNMP community that was set on this LAN switch blade.

Either select [public] or enter an arbitrary string.

Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

For LAN switch blades operating in Converged Fabric mode, select [public]. In this case, Resource Orchestrator does not communicate with LAN switch blades using SNMP, so it does not check whether the SNMP community entered here matches the SNMP community set on the LAN switch blade.

3. Click <OK>.

The registered LAN switch blade will be displayed in the server resource tree.

Information

For the following LAN switch blades, check the setting after the LAN switch blade has been registered.

- For a PY CB DCB SW 10Gb 18/6/6

  Check that the following settings are displayed correctly in the resource details of the LAN switch blade.

  - Operation mode (VCS mode and other modes)

  - VCS ID and RBridge ID

- For a PY CB Eth Switch 10/40Gb 18/8+2 operating in Converged Fabric mode

  Check that the following settings are displayed correctly in the resource details of the LAN switch blade.

  - Fabric ID, Domain ID, and Switch ID

If a displayed value is incorrect, log in to the LAN switch blade and check that the settings of operating mode and these IDs are correct. For the confirmation method, refer to the manual for the LAN switch.

If the settings are correct, delete the LAN switch blade and register it again.

Note

- A telnet or SSH connection is made when registering a LAN switch blade.
  When telnet or SSH (SSH version 2) connection is disabled, enable it.
  Refer to the manual of the relevant product.
  Some models may have restrictions regarding the number of simultaneous connections. In this case, log out from other connections.

  If the connection is unavailable, the following features are also unavailable.

  - Registration of LAN switch blades

  - Changing of LAN switch blade settings

  - Changing and setting the VLAN for LAN switch blades (internal and external connection ports)

  - Restoration of LAN switch blades

  - Server switchover (changing network settings while a server is switched over)

- SSH connection (SSH version 2) can be selected for the following LAN switch blades.

  - LAN switch blade PY CB Eth Switch/IBP 10Gb 18/8 (1.00 or later version)

  - LAN switch blade PY CB Eth Switch 10/40Gb 18/8+2 (1.00 or later version)

- LAN switch blade PY CB Eth Switch/IBP 1Gb 36/8+2 (4.16 or later version)

- LAN switch blade PY CB Eth Switch/IBP 1Gb 36/12 (3.12 or later version)

- LAN switch blade PY CB Eth Switch/IBP 1Gb 18/6 (3.12 or later version)

- LAN switch blade PY CB DCB SW 10Gb 18/6/6 (2.1.1_fuj or later version)

- Virtual domain representative IP addresses cannot be registered with LAN switch blade CB Eth Switch 10/40Gb 18/8+2.

7.3.4 Configuring VLANs on LAN Switch Blades

On managed LAN switch blades, VLANs should be set on both internal ports (those connected to network interfaces on managed servers) and external ports (those connected to external, adjacent LAN switches).

📑 Note

- VLANs cannot be configured on PRIMERGY BX 900 and BX 400 LAN switch blades operating in IBP mode or Converged Fabric mode.

- For a LAN switch blade PY CB 10Gb FEX Nexus B22, this cannot be configured.

7.3.4.1 Configuring VLANs on External Ports

Use the following procedure to configure VLANs on a LAN switch blade's external ports.

1. In the ROR console server resource tree, right-click the target LAN switch blade and select [Modify]-[Network Settings] from the popup menu.

   The [VLAN Settings] dialog is displayed.

2. Perform the following settings:

   VLAN

   > Specify the VLAN ID to assign to a LAN switch blade port.

   > **Adding a new VLAN ID**

   >> a. Under VLAN, select [Create new].

   >> b. Enter a VLAN ID number.
   >> For details on VLAN IDs, refer to the manual of the LAN switch blade to be used.

   > **Modifying an existing VLAN ID**

   >> a. Under VLAN, select [Change].

   >> b. Select a VLAN ID.

   Physical Port, Link Aggregation

   > Select port numbers to configure or VLAN types of link aggregation group names ([Untagged] or [Tagged]).

3. Click <OK>.

   Check that the VLAN has been set.

4. Select the LAN switch blade in the server resource tree of the ROR console and display the [Resource Details] tab.
   Confirm that the VLAN information is displayed in [VLAN Area] on [Resource Details].

📑 Note

For a LAN switch blade PY CB DCB SW 10Gb 18/6/6, the VLAN settings of external ports cannot be configured.

7.3.4.2 Configuring VLANs on Internal Ports

Use the following procedure to configure VLANs on a LAN switch blade's internal ports.

1. In the ROR console server resource tree, right-click the target server (or the physical OS or VM host on the server), and select [Modify]-[Network Settings] from the popup menu.

   The [Network Settings] dialog is displayed.

2. Select the index of the network interface for which to assign a VLAN ID, and click <Setting>.

   The [VLAN Configuration] dialog is displayed.

3. Perform the following settings:

   Port VLAN

   VLAN ID

   Enter the VLAN ID to assign to the LAN switch blade port that is connected to the network interface selected in step 2.

   Tagged VLAN

   VLAN ID

   Enter the tagged VLAN ID(s) to assign to the LAN switch blade port that is connected to the network interface selected in step 2.
   Multiple VLAN IDs can be entered by separating them with commas (",").

4. Click <OK>

   Note that the VLAN settings are not applied onto the LAN switch blade at this stage. To configure VLANs for multiple network interfaces, repeat steps 2 to 4.

5. Confirm the configuration set in the [Network Settings] dialog.

6. Click <OK>.

   VLAN settings are applied to the related LAN switch blade.

📌 Note

- When the VLAN configuration of a registered LAN switch blade is changed from the Web-based or command-based interface of the LAN switch, it may take a while for that configuration to be reflected on Resource Orchestrator through periodic queries.

   When performing server switchover before new VLAN information is reflected, the VLAN information previously set is configured in LAN switch blades. Set the VLAN configuration from the ROR console instead of the LAN switch's own Web-based and command-based interfaces.

- If the Port VLAN ID field is left blank and a value is entered for Tagged VLAN ID in the [VLAN Configuration] dialog, the tagged LAN only will be enabled.

   To enable a port VLAN, enter a value for Port VLAN ID.
   When only a tagged VLAN is configured, the value for the port VLAN is not displayed on the ROR console even if it has been configured on the switch. For the devices for which port VLANs cannot be deleted, it is necessary to limit the frames that let ports pass through to the tagged frames only.
   If the port VLAN ID is unspecified or 1, a tagged VLAN ID cannot be set to 1.

- VLAN settings cannot be configured for ports with Automatic Migration of Port Profile (AMPP) configured.

7.3.5 HBA address rename Settings

For details, refer to "7.4.2 HBA address rename Settings".

7.4 When Using Rack Mount and Tower Servers

This section explains how to register resources when using rack mount or tower servers.

When using rack mount or tower servers, use the following procedure to register resources:

- Register Rack Mount or Tower Servers

- Register LAN Switches

7.4.1 Registering Rack Mount or Tower Servers

This section explains how to register a rack mount or tower server.

When using VIOM for I/O virtualization, VIOM server profiles should be registered in advance according to the procedure described in "7.1.1 Registering VIOM Server Profiles".

Figure 7.2 Status Transition Diagram for Managed Servers
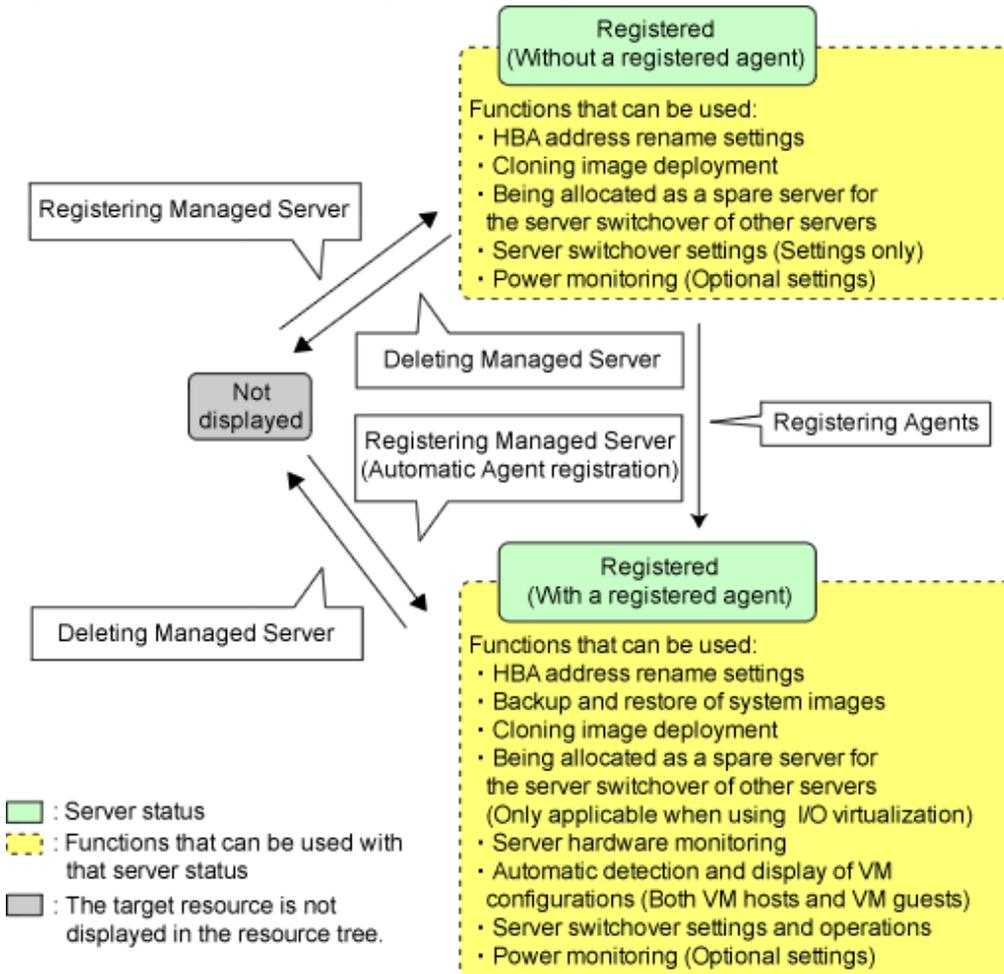
Use the following procedure to register rack mount or tower servers.

1. In the ROR console server resource tree, right-click [Server Resources], and select [Register]-[Server] from the popup menu.

   The [Register Server] dialog is displayed.

2. Perform the following settings:

   Enter items differ depending on whether the [Register agent] checkbox is selected, as described below.
   If this checkbox is checked, agents will be registered after server registration.
   If this checkbox is not checked, registration of agents will not be performed, so register agents after server registration when necessary.
   For details on registering agents, refer to "Chapter 7 Installing Software and Registering Agents on Managed Servers" in the "Setup Guide VE".

   Without Agent Registration

- Physical server name

- Remote management controller

  - IP address

  - User ID

  - Password

- Association with server management software (ServerView)

  - Enable/Disable

  - SNMP Community

- Admin LAN

  - IP address

  - MAC address (NIC1)

- SAN Boot/Admin LAN Redundancy

  - MAC address (NIC2)

Automatic registration of agents is not performed after server registration. After registering servers, register agents as required.

If registering agents, register agents after checking the product name is displayed in the General Area of [Resource Details] tab.

Executing [Update] acquires the latest information.

With Agent Registration

- Physical server name

- Remote management controller

  - IP address

  - User ID

  - Password

- Association with server management software (ServerView)

  - Enable/Disable

  - SNMP Community

- Admin LAN

  - IP address

- Admin LAN Redundancy

  - MAC address (NIC2)

- OS

  - Type

Agents are automatically registered after server registration is completed.

Physical Server Name

  Enter a name to assign to this physical server.
  Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

Remote management controller

  IP address

    Enter the IP address of this server's remote management controller.

User ID

Enter the ID of a remote management controller user account with administrative authority over this server.
Enter up to 16 characters, including alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e).

Password

Enter the password of the above remote management controller user account.
Enter up to 16 characters, including alphanumeric characters and symbols (ASCII characters 0x20 to 0x7e).
This field can be omitted if no password has been set for this user account.

Association with server management software (ServerView)

Enable/Disable

For PRIMERGY BX servers
Select [Enable] and enter an [SNMP Community].

For servers other than PRIMERGY servers
Select [Disable].

By default, [Enable] is selected.

SNMP Community

Enter the SNMP community that was set on this server.
Either select "public" or enter an arbitrary string.
Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

Admin LAN

IP address

Enter the IP address used by this server on the admin LAN.

MAC address (NIC1)

Enter the MAC address of this server's admin LAN network interface.
Enter a physical MAC address in either one of the following formats: hyphen-delimited ("xx-xx-xx-xx-xx-xx"), or colon-delimited ("xx:xx:xx:xx:xx:xx").
MAC addresses will be automatically detected when the [Register agent] checkbox is selected.

SAN Boot/Admin LAN Redundancy

MAC address (NIC2)

Enter the MAC address of the second admin LAN network interface. This network interface is to be used by the HBA address rename setup service, or to enable admin LAN redundancy on the registered server.
Enter a physical MAC address in either one of the following formats: hyphen-delimited ("xx-xx-xx-xx-xx-xx"), or colon-delimited ("xx:xx:xx:xx:xx:xx").
This field can be omitted in the following cases.

- When not using the HBA address rename setup service

- When not using GLS for admin LAN redundancy on the managed server

- For a spare server whose primary servers are not using admin LAN redundancy

OS

Type

This option is displayed if the target server runs a physical OS or VM host.
Select the appropriate server OS category (Physical OS or VM host).
Selecting [VM Host] activates the user ID and password input fields. Those refer to the user name and password entered during installation of this VM host.
Select the server OS category depending on whether the relevant server is used on a physical OS or a VM host.

For a Physical OS
Select [Windows/Linux].

For a VM Host

Select [VM Host], and enter the VM host login account information.

This login account information will be used by Resource Orchestrator to control and communicate with the registered VM host.

User ID

Enter the user ID to log in to the VM host. Specify a user ID that has VM host administrator authority.

Password

Enter the password of the user to log in to the VM host.

Note

- For details about the network interfaces used on the admin LAN, refer to "7.1 Network Configuration" in the "Design Guide VE".
  If an incorrect network interface is used, Resource Orchestrator will use a wrong MAC address for the admin LAN.
  An admin LAN IP address is required even when registering a spare server.
  Enter an IP address that does not conflict with the IP address of any other managed server on the admin LAN.

- When using backup and restore, cloning, or HBA address rename, the NIC (or LAN expansion board) must support PXE boot.

- A server running a VM host can still be registered as a physical OS if its [Category] of [Server OS] is set to [Windows/Linux]. (For Windows Server 2008, etc.)
  A VM host server that was mistakenly registered as a physical OS should be deleted and re-registered as a VM host.

- When registering rack mount servers on which VMware ESXi is operating, select [Disable] for [Association with server management software (ServerView)] even when using PRIMERGY servers.
  After registering the server, clear the [Register agent] checkbox and register the agent after registration of the server is complete.

3. Click <OK>.

   The registered server will be displayed in the server resource tree.

Note

- After registering the server, please verify that the information registered for the remote management controller is correct. This can be verified by trying out power operations (from Resource Orchestrator) against that server. Refer to "Chapter 14 Power Control" for power operations.

- When using HBA address rename setup service, please confirm that the registered server can boot properly using the HBA address rename setup service.
  If the server cannot be booted properly, ensure that the specified MAC address (NIC2) is correct.

- When an agent is registered on a VM host, all VM guests running on that VM host are also registered automatically. Whenever a VM guest is created, modified, deleted, or moved on a registered VM host, the changes are automatically updated in the server resource tree.

- The VM guest name displayed in the ROR console is either the VM name defined in its server virtualization software or the host name defined in the guest OS.
  The timing at which the hostname of a guest OS is detected and displayed varies according its server virtualization software. For details, refer to "D.3 Functional Differences between Products" in the "Design Guide VE".

- It is recommended not to use duplicate names for physical OSs, VM hosts, and VM guests. If duplicated names are used, those resources cannot be managed from the command-line.

- When registering a server on which the agent was installed, it is necessary to either reboot the server or restart its related services (explained in the "2.2 Starting and Stopping Agents" in the "Operation Guide VE") after server registration. This step has to be done before running any image operation (system image backup or cloning image collection).
  For details on how to restart the agent, refer to "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

7.4.2 HBA address rename Settings

Use the following procedure to configure HBA address rename settings.

The HBA address rename function allows the admin server to control the WWNs set on a managed server's HBAs. Since the admin server carried over these settings when performing maintenance on or switching managed servers, it is not necessary to set the storage side configuration again.
Use of the HBA address rename function requires registering specific settings for each managed server in advance.

🛈 Note

. . . .

- The HBA address rename function is not available if ServerView Deployment Manager is used on the admin LAN. For details, refer to "Appendix B Co-Existence with ServerView Deployment Manager" in the "Setup Guide VE".

- For servers which already have server switchover configured, when configuring or changing HBA address rename, the following conditions must be met:

    - Primary servers with HBA address rename configured

    - Spare servers with the server switchover method HBA address rename configured

    For any servers that do not meet these conditions, cancel any existing recovery settings before enabling the HBA address rename function on a server.

- HBA address rename and VIOM cannot be used together within the same chassis.

. . . .

1. Storage Settings

Refer to "8.2 Configuring the Storage Environment" in the "Design Guide VE" to configure the storage.
When altering the configuration of a storage device already used by active servers, ensure those servers are powered off before performing any configuration changes.

2. Settings for the HBA address rename Function

1. On the ROR console server resource tree, right-click the target server (or the physical OS or VM host on the server), and select [Modify]-[HBA Address Rename Settings] from the popup menu.

    The [HBA Address Rename Settings] dialog is displayed.

2. Define the following settings:

    WWNN

       Specify the WWNN value provided by the "I/O virtualization Option".
       The admin server generates WWPNs automatically from the values that are input into the WWNN and the number of HBA ports.

    HBA ports

       Specify the following values according to the system configuration.

          - To create a single-path configuration, specify "1".

             For details, refer to "Figure 7.3 Procedures for Single-path Configurations".

          - To create a multi-path configuration, specify "2".

             However, it is necessary to specify "1" during installation of the operating system. Specify "2" and reconfigure HBA address rename settings after setting up the multi-path driver.
             For details, refer to "Figure 7.4 Procedures for Multi-path Configurations".

Figure 7.3 Procedures for Single-path Configurations
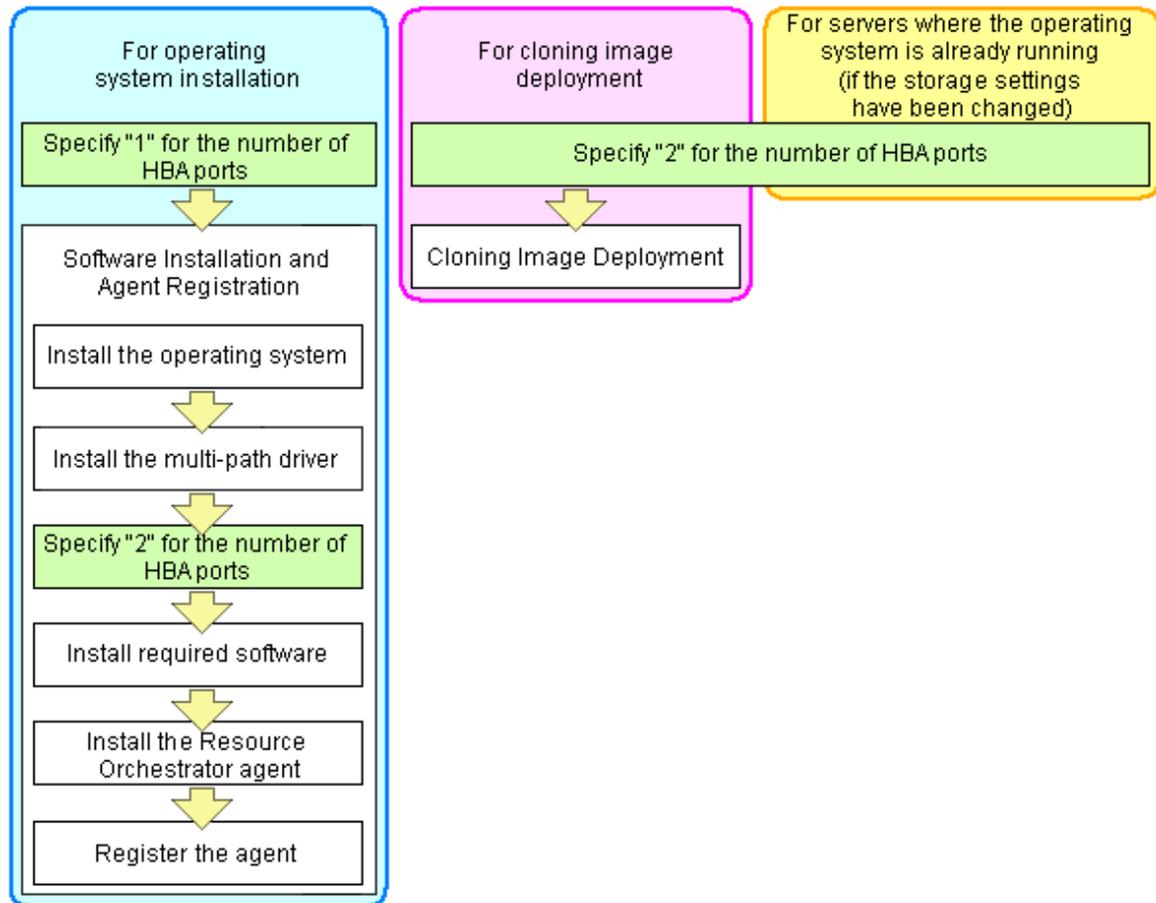
Figure 7.4 Procedures for Multi-path Configurations
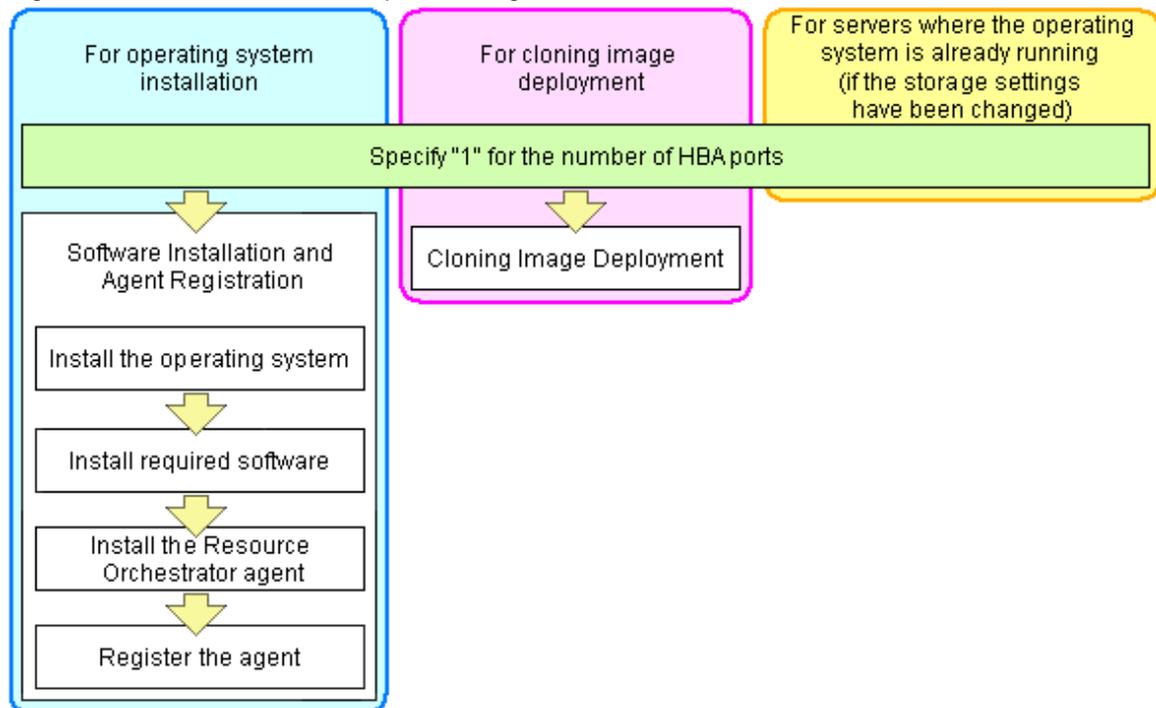
Example

For a server with two ports, WWNs could be configured as follows.

WWNN value provided by "I/O Virtualization Option": 20:00:00:17:42:51:00:00

Values to set in the [HBA address rename settings] dialog

"WWNN" value 20:00:00:17:42:51:00:00
"HBA port number" on board: 2

Values actually set by the admin server on the HBA (WWPNs are generated automatically)

```
WWNN value for ports 1 and 2 of the HBA     : 20:00:00:17:42:51:00:00
WWPN value for HBA port 1                    : 21:00:00:17:42:51:00:00
WWPN value for HBA port 2                    : 22:00:00:17:42:51:00:00
```

Information

WWN settings are applied to managed servers during server startup.

Note

With HBA address rename, as WWNs are allocated to the I/O addresses of HBAs in descending order, the order may not match the port order listed in the HBA.
For details, refer to "C.2 WWN Allocation Order during HBA address rename Configuration" in the "Design Guide VE".

3. Check the [Restart the server] checkbox if the server is to be restarted.

Information

Select server restart in the following cases.

  - When installing an operating system immediately after performing the above settings

    Insert the operating system installation CD in the target server and select server restart. Once the server has been restarted, its WWN settings are applied and the operating system installation starts.

  - When an operating system is already running (if changing storage settings)

    Click <OK> to restart the target server and apply its WWN settings.

The server restart is not required in other cases. The WWN that has been set is enabled at the next restart.

4. Click <OK>.

Information

When using a server without an OS, the resource name displayed on the server resource tree is the same as that of the physical server.

5. Restart the HBA address rename setup service.

The HBA address rename setup service must be running to use the HBA address rename function.
For details on how to configure these settings, refer to "Chapter 6 Settings for the HBA address rename Setup Service" in the "Setup Guide VE".

7.5 When Using PRIMEQUEST Servers

This section explains how to register resources when using PRIMEQUEST servers.

- Registering Chassis (For PRIMEQUEST Servers)

- Registering PRIMEQUEST Servers

7.5.1 Registering Chassis (For PRIMEQUEST Servers)

By registering a chassis, every partition mounted in the chassis will be automatically detected and displayed as an unregistered server in the server resource tree. Register these managed servers individually.

For details on registering servers, refer to "7.5.2 Registering PRIMEQUEST Servers".

Use the following procedure to register a chassis:

1. In the ROR console server resource tree, right-click [Server Resources], and select [Register]-[PRIMEQUEST] from the popup menu.

    The [Register Chassis] dialog is displayed.

2. Perform the following settings:

    Admin LAN (IP address)

    > Enter the virtual IP address that was set on the chassis management board.
    > Enter the IP address using periods ".".

    Chassis name

    > Enter a name to assign to this chassis.
    > Enter a character string beginning with an alphabetical character and containing up to 10 alphanumeric characters and hyphens ("-").

    SNMP Community

    > Enter the SNMP community that was set on the chassis management board.
    > Either select [public] or enter an arbitrary string.
    > Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

    Remote server management

    > User ID

    >> Enter the ID of a remote server management user account with administrative authority over this managed server.
    >> This user ID must be between 8 and 16 alphanumeric characters long.
    >> A user ID with at least administrator privileges within the remote server management must be specified.

    > Password

    >> Enter the password of the above remote server management user account.
    >> This password must be between 8 and 16 alphanumeric characters long.

    ### 📒 Note
    ....
    The [User ID] and [Password] of [Remote server management] are different from the user name and password used to log in on the Web-UI for management board.
    ....

3. Click <OK>.

    The mounted chassis will be displayed under the server resource tree.
    Any partition mounted within this chassis will be detected automatically and shown as: [*chassis_name-partition_number*[Unregistered]].
    The only operation available for those unregistered partitions is server registration, while the ROR console can only display their hardware statuses and properties.
    If the manager is installed on one of those partitions, this partition will be shown as: [*chassis_name-partition_number*[Admin

Server]].

In that case, server registration will not be available for the admin server, but its hardware status and properties will be displayed in the ROR console.

![Information] Information

For the PRIMEQUEST 2000 series, when the chassis is registered, PPAR and Extended Partition partitions are detected automatically and they are displayed as unregistered servers in the server resource tree. However, PPAR with Extended Partition Mode set to "Enable" are not displayed.

When [Extended Partition Mode] of PPAR#3 is set to "Enable" and Extended Partition#4 and Extended Partition#5 are configured from PPAR#3 as shown in the figure below, PPAR#3 is not displayed in the server resource tree after the chassis is registered. Extended Partition#4 and Extended Partition#5 configured from PPAR#3 are displayed in the server resource tree.

Figure 7.5 About Auto-detection of Partitions on the PRIMEQUEST 2000 Series

7.5.2 Registering PRIMEQUEST Servers

This section explains how to register servers when using PRIMEQUEST servers.

For the PRIMEQUEST 2000 series, the following partitions can be registered as managed servers.

- PPAR partitions with Extended Partitioning Mode set to "Disable"

- Extended Partitioning partitions configured on the PPAR partition with Extended Partitioning Mode set to "Enable"

Do not change Extended Partitioning Mode after registering the server. If Extended Partitioning Mode of a PPAR is changed to "Enable" after server registration, [Extended Partitioning Mode] is displayed for that PPAR. PPAR with [Extended Partitioning Mode] displayed cannot be used. If you want to change the Extended Partitioning Mode of a PPAR after server registration, delete it from managed servers first, change the Extended Partitioning Mode, and then register the PPAR again.

Register the server using the following procedure:

1. In the ROR console server resource tree, right-click an unregistered server blade or partition in the target chassis, and select [Register]-[Server] from the popup menu.

   The [Register Server] dialog is displayed.

2. Perform the following settings:

   Physical Server Name

   Enter a name to assign to this physical server.

   Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

   Admin LAN (IP address)

   Enter the IP address used by this server on the admin LAN.

   Enter the IP address of this server's admin LAN network interface.

   The Agent will not be registered automatically, but can be manually registered after server registration if necessary. After registering servers, register agents as required.

   Boot option

   Specify the boot option configured from BIOS when installing the OS.

   - For UEFI

     Select [UEFI].

   - For Legacy Boot

     Select [Legacy boot].

   By default, [UEFI] is selected.

   These settings can be changed after server registration.
   For details on how to modify these settings, refer to "9.1.10 Changing Boot Options".

3. Click <OK>.

   The registered server will be displayed in the server resource tree.

📌 Note

For PRIMEQUEST, after IOU replacement or immediately after powering on, the MAC Address for each partition that is obtained from the MMB becomes FF:FF:FF:FF:FF:FF. As correct LAN MAC addresses are obtained from the MMB after each partition is powered on, perform server registration after that.

7.6 When Using Fujitsu M10/SPARC Enterprise

This section explains how to register resources when using Fujitsu M10/SPARC Enterprise.

- Registering Chassis (SPARC Enterprise M4000/M5000/M8000/M9000) or FUJITSU M10-4S

- Registering SPARC Enterprise (M3000/T Series) servers or SPARC M10-1/M10-4

7.6.1 Registering Chassis (SPARC Enterprise M4000/M5000/M8000/M9000) or FUJITSU M10-4S

By registering a chassis, every partition mounted in the chassis will be automatically detected and displayed as an unregistered server in the server resource tree. Register these managed servers individually.

For details on registering managed servers, refer to "7.6.2 Registering SPARC Enterprise (M3000/T Series) and FUJITSU M10-1/ M10-4".

Use the following procedure to register a chassis:

1. In the ROR console server resource tree, right-click [Server Resources], and select as below.

    - For SPARC Enterprise M4000/M5000/M8000/M9000 servers

      Select [Register]-[SPARC Enterprise (Partition Model)] from the popup menu.

    - For SPARC M10-4S

      Select [Register]-[SPARC M10-4S] from the popup menu.

    The [Register Chassis] dialog is displayed.

2. Perform the following settings:

    Admin LAN (IP address)

      Enter the IP address of the XSCF of the target chassis.
      Enter the IP address using periods ".".

    Chassis name

      Enter a name to assign to this chassis.
      Enter a character string beginning with an alphabetical character and containing up to 10 alphanumeric characters and hyphens
      ("-").

    SNMP Community

      Enter the SNMP community of the XSCF used to manage the target chassis.
      Either select [public] or enter an arbitrary string.
      Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

    Remote management controller (XSCF)

      User ID

        Enter the ID of an XSCF user account with administrative authority over the target chassis.
        Enter a string of up to 31 alphanumeric characters, hyphens ("-"), and underscores ("_"). This name must start with an alphabet
        character.
        This user should have "platadm" privileges for XSCF.

        The user ID reserved for the system cannot be used. Create another user ID.
        For details, refer to the XSCF manuals.

      Password

        Enter the password of an XSCF user account with administrative authority over the target chassis.
        Enter up to 32 characters, including alphanumeric characters, blank spaces (" "), and any of the following symbols.
        "!", "@", "#", "$", "%", "^", "&", "*", "[", "]", "{", "}", "(", ")", "-", "+", "=", "~", ",", ">", "<", "/", "", "?", ";", ":"

3. Click <OK>.

    The mounted chassis will be displayed under the server resource tree.
    Any partition mounted within this chassis will be detected automatically and shown as: [*chassis_name-partition_number*[Unregistered]].
    The only operation available for those unregistered partitions is server registration, while the ROR console can only display their
    hardware statuses and properties.

7.6.2 Registering SPARC Enterprise (M3000/T Series) and FUJITSU M10-1/ M10-4

This section explains the methods for registering SPARC Enterprise (M3000/T series) and SPARC M10-1/M10-4.
This section also describes how to register servers in SPARC Enterprise M4000/M5000/M8000/M9000 and SPARC M10-4S chassis.

[Solaris Zones] [OVM for SPARC]
When the Logical Domains Manager daemon is enabled, VM hosts can be registered as Solaris Zones by configuring the definition files.
For details, refer to "D.4 Definition Files of Each Product" in the "Design Guide VE".

Use the following procedure to register servers:

1. The dialog is displayed.

   - For SPARC Enterprise (M3000/T series)

     In the ROR console server resource tree, right-click [Server Resources], and select as below.

     Select [Register]-[SPARC Enterprise (M3000/T Series)] from the popup menu.

     The [Register SPARC Enterprise] dialog is displayed.

   - For SPARC M10-1/M10-4

     In the ROR console server resource tree, right-click [Server Resources], and select as below.

     Select [Register]-[SPARC (M10-1/M10-4)] from the popup menu.

     The [Register SPARC (M10-1/M10-4)] dialog is displayed.

   - For SPARC Enterprise M4000/M5000/M8000/M9000 or SPARC M10-4S

     Right-click the server in the chassis, and select as follows:

     Select [Register]-[Server] from the popup menu.

     The [Register Server] dialog is displayed.

2. Perform the following settings:

   When using SPARC Enterprise M4000/M5000/M8000/M9000 or FUJITSU M10-1/M10-4/M10-4S, the items related to Remote Management Controller are not displayed.

   - Physical Server Name

   - [Register agent] checkbox

   - Remote management controller (ILOM/XSCF)

       - Controller type

       - IP address

       - User ID

       - Password

       - SNMP Community

   - Admin LAN

       - IP address

   With Agent Registration

   - OS

       - Type

       - User ID

       - Password

   Physical Server Name

       Enter a name to assign to this physical server.
       Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

   [Register agent] checkbox

       - Without Agent Registration

         Automatic registration of agents is not performed after server registration.
         After registering servers, register agents as required.

         If registering agents, register agents after checking the product name is displayed in the General Area of [Resource Details] tab.

Executing [Update] acquires the latest information.

- With Agent Registration

Agents are automatically registered after server registration is completed.

Remote management controller (ILOM/XSCF)

For SPARC Enterprise M3000 servers

Controller type

Select [XSCF].

IP address

Enter the IP address of this server's remote management controller (XSCF).

User ID

Enter the ID of a XSCF user account with administrative authority over this server.
Enter up to 31 characters, including alphanumeric characters, underscores ("_"), or hyphens ("-"). This name should start with an alphabet character.
This user should have "platadm" privileges for XSCF.

The user ID reserved for the system cannot be used. Create another user ID.
For details, refer to the XSCF manuals.

Password

Enter the password of the above XSCF user account.
Enter up to 32 characters, including alphanumeric characters, blank spaces (" "), and any of the following symbols.
"!", "@", "#", "$", "%", "^", "&", "*", "[", "]", "{", "}", "(", ")", "-", "+", "=", "~", ",", ">", "<", "/", "''", "?", ";", ":"

SNMP Community

Enter the SNMP community that was set on this server's remote management controller (XSCF).
Either select [public] or enter an arbitrary string.
Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

For SPARC Enterprise T series

Controller type

Select [ILOM].

IP address

Enter the IP address of this server's remote management controller (ILOM).

User ID

Enter the ID of an ILOM user account with administrative authority over this server.
Enter between 4 and 16 characters, including alphanumeric characters, underscores ("_"), or hyphens ("-"). This name should start with an alphabet character.
This user ID should have "Admin" privileges for ILOM.

Password

Enter the password of the above ILOM user account.
Enter between 8 and 16 characters, including alphanumeric characters, blank spaces (" "), and any of the following symbols.
"!", "@", "#", "$", "%", "^", "&", "*", "[", "]", "{", "}", "(", ")", "-", "+", "=", "~", ",", ">", "<", "/", "''", "?", ";", ":"

SNMP Community

Enter the SNMP community name of this server's remote management controller (ILOM).
Either select [public] or enter an arbitrary string.
Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

Admin LAN

IP address

Enter the IP address used by this server on the admin LAN.

Server OS

Category

Select the appropriate server OS category (Physical OS or VM host).
Selecting [Solaris Zone] activates the user name and password input fields.
Those refer to the user name and password entered during installation of this VM host.

For a Physical OS
Select [Solaris].

For a VM Host
Select [VM Host], and enter the VM host login account information.
This login account information will be used by Resource Orchestrator to control and communicate with the registered VM host.

Note

Server switchover is possible only while registering as [VM host] in the case of OVM for SPARC.

User ID

Enter the user ID to log in to the VM host.
Specify the user ID "root" which has VM host administrator authority.

Note

When using Solaris 11, if user accounts are created during installation, root will be registered for the role. Therefore, the root account cannot be used for login. Log in using the user account, and use the su command to become a root user.

When using Solaris 10 or earlier versions, execute the following as root in order to change to enable direct login using the root account. In this case, the root role is recognized as a root user.

```
rolemod -K type=normal root <RETURN>
```

Use SSH connection with the root account, and check if communication with the VM host is possible.
If communication fails, modify the configuration. For details, refer to the manual of the basic software.

Password

Enter the password of the user to log in to the VM host.
Enter up to 256 characters, including alphanumeric characters, blank spaces (" "), and symbols.

3. Click <OK>.

The registered server will be displayed in the server resource tree.

Note

After registering the server, please verify that the information registered for the remote management controller is correct. This can be verified by trying out power operations (from Resource Orchestrator) against that server. Refer to "Chapter 14 Power Control" for power operations.

7.6.3 Registering Guest Domains on Oracle VM for SPARC

This section explains the methods for registering guest domains on Oracle VM for SPARC.

When a guest domain is registered as a VM host, information for zones created on the guest domain is also displayed.

Use the following procedure to register VM hosts. Perform it with the VM guest started.

When using a virtual L-Server for the target guest domain, if the IP address specified when performing this operation is used for the admin LAN of the virtual L-Server, perform this operation after deleting the NIC.

1. In the ROR console server resource tree, right-click the VM guest in [Server Resources], and select [Register]-[Agent] from the popup menu.

   The [Register VM Host] dialog is displayed.

2. To use this feature, the following settings must be defined:

   Admin LAN IP Address

      Enter the IP address of the XSCF of the target chassis.
      Enter the IP address using periods ".".

   📕 Note
   ···
   - After registering the guest domain, confirm that the VM guest is displayed under the VM host in the guest domain of Oracle VM for SPARC, and that the same VM guest is in the Solaris Zone operating on the actual server.
     When different VM guests are displayed, check the registered IP address and then change it to the correct one.

   - L-Servers in L-Platforms cannot be registered.
   ···

   User ID

      Enter the user ID to log in to the guest domain.
      Specify the user ID "root" which has guest domain administrator authority.

   Password

      Enter the password of the user to log in to the VM host.
      Enter up to 256 characters, including alphanumeric characters, blank spaces (" "), and symbols.

3. Click <OK>.

   The registered VM Host will be displayed in the server resource tree.

7.7 Registering Power Monitoring Devices

This section explains how to register power monitoring devices.

Registering power monitoring devices (PDU or UPS) enables monitoring of power consumption.

Use the following procedure to register power monitoring devices.

1. In the ROR console power monitoring device tree, right-click [Power Monitoring Devices] and select [Register]-[Power Monitoring Device] from the popup menu.

   The [Register Power Monitoring Device] dialog is displayed.

2. Perform the following settings:

   Device name

      Enter a name to assign to this power monitoring device. When exporting power consumption data, use this name to select power monitoring devices for which to export data.
      Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

   Admin LAN (IP address)

      Enter the IP address that was set on this power monitoring device. This IP address will be used to collect power consumption data from this power monitoring device.

SNMP Community

Enter the SNMP community that was set on this power monitoring device.

Either select [public] or enter an arbitrary string.

Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

This SNMP community will be used to collect power consumption data from this power monitoring device (via SNMP protocol).

Voltage

Enter the voltage (V) supplied to this power monitoring device. Enter a number between 10 and 999. Power consumption data is calculated using the electrical current value obtained from this power monitoring device and its specified voltage.

Comment

Enter a comment that describes this power monitoring device.

Enter up to 128 alphanumeric characters or symbols (ASCII characters 0x20 to 0x7e).

Note

A line break is counted as one character.

3. Click <OK>.

The registered power monitoring device will be displayed under the power monitoring devices tree.

If collection of power data is disabled in the option settings, data will not be collected even if power monitoring devices are registered. Change power data collection settings according to "9.6.1 Changing Environmental Data Settings".

Note

Resource Orchestrator is not aware of the relationship between power monitoring devices and actual server resources. Make sure to register the power monitoring devices that are connected to the server resources for which you want to monitor power consumption.

7.8 Registering Admin LAN Subnets

This section explains how to perform admin LAN subnet registration.

Registering admin LAN subnets enables management of managed servers belonging to subnets other than that of the admin LAN.

Use the following procedure to register an admin LAN subnet.

1. From the ROR console menu, select [Settings]-[Admin LAN Subnet].

   The [Admin LAN Subnet] dialog is displayed.

2. Click <Add>.

   The [Add Admin LAN Subnet] dialog is displayed.

3. Perform the following settings:

Subnet name

Set the subnet name for registration.

Enter a character string beginning with an alphabetic character and containing up to 16 alphanumeric characters, underscores ("_"), hyphens ("-"), and periods (".").

Network address

Configure the network address of the subnet used as the admin LAN.

Enter valid values for the network address.

Subnet mask

Enter valid values for the subnet mask.

Gateway

Enter the settings for the gateway used for communication with the admin server on the admin LAN.

4. Click <OK>.

Information
. . . .
When registering an admin LAN subnet for the first time, change the simplified DHCP service for Resource Orchestrator to the OS standard DHCP Service.
Resource Orchestrator takes exclusive possession of the OS standard DHCP Service.
. . . .

Note
. . . .

- It is necessary to perform network settings for each admin LAN subnet so that managed servers belonging to subnets other than the admin LAN can communicate with the admin server.

  For details on how to configure the network settings, refer to "7.6 Configuring the Network Environment" in the "Design Guide VE".

- In a clustered manager configuration, when registering an admin LAN subnet for the first time, perform "Settings for Clustered Manager Configurations".

- When managing a managed server in a separate subnet from the admin server, an OS standard DHCP server is necessary.

  For details, refer to "2.1.1.2 Software Preparation and Checks" or "2.1.2.2 Software Preparation and Checks" in the "Setup Guide VE".
. . . .

Settings for Clustered Manager Configurations

The following configuration is necessary only when registering an admin LAN subnet for the first time.

[Windows Manager]

Information
. . . .
When configuring a cluster system in an environment that already has an admin LAN registered, perform steps 5 to 10, and 13.
. . . .

1. Allocate the shared disk to the primary node.

   Right-click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree, and select [Move this service or application to another node]-[1 - Move to node *node_name*] from the displayed menu.
   The name of the primary node is displayed for *node_name*.

2. Delete the registry replication settings from the following "Services and Applications" of the manager.

   Based on the following table, delete registry replication for the resources.

   - x64

Resources for Deletion	Registry Key
Deployment Service	[HKEY_LOCAL_MACHINE\]SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\ResourceDepot
	[HKEY_LOCAL_MACHINE\]SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\DatabaseBroker\Default

Resources for Deletion	Registry Key
PXE Services	[HKEY_LOCAL_MACHINE\]SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\DHCP
	[HKEY_LOCAL_MACHINE\]SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\PXE\ClientBoot\

- x86

Resources for Deletion	Registry Key
Deployment Service	[HKEY_LOCAL_MACHINE\]SOFTWARE\Fujitsu\SystemcastWizard\ResourceDepot
	[HKEY_LOCAL_MACHINE\]SOFTWARE\Fujitsu\SystemcastWizard\DatabaseBroker\Default
PXE Services	[HKEY_LOCAL_MACHINE\]SOFTWARE\Fujitsu\SystemcastWizard\DHCP
	[HKEY_LOCAL_MACHINE\]SOFTWARE\Fujitsu\SystemcastWizard\PXE\ClientBoot\

Perform the following procedure for each of the above resources:

    a. Right-click the target resource on [Other Resources] on the [Summary of RC-manager] displayed in the middle of the [Failover Cluster Management] window, and select [Properties] from the displayed menu.
The [*target_resource* Properties] window will be displayed.

    b. From the [Root Registry Key] displayed on the [Registry Replication] tab, select the above registry keys and click <Remove>.

    The selected key is removed from [Root Registry Key].
When deleting the second registry key, repeat step b.

    c. Click <Apply>.

    The settings are applied.

    d. Click <OK> to close the dialog.

3. Take the following services of the "Services and Applications" for the manager offline.

  - Deployment Service

  - TFTP Service

  - PXE Services

4. Register the admin LAN subnet.

5. On the primary node, bring the shared disk of the manager online, and take all other cluster resources offline.

6. Open [Services] from [Administrative Tools] on the Windows Control Panel, and then configure the startup type of DHCP Server service as "Manual" on the [Services] window.

7. From the [Services] window, stop the DHCP Server service.

8. Using Explorer, copy the following folder from the local disk of the primary node to the folder on the shared disk.

Local Disk (Source)	Shared Disk (Target)
%SystemRoot%\System32\dhcp	*Drive_name*:\Fujitsu\ROR\SVROR\dhcp

💡 Example
・・・

When the OS has been installed on the C drive, it is %SystemRoot%C:\Windows.

・・・

9. Configure access rights for the folder for the DHCP Server that was copied to the shared disk. Execute the following command using the command prompt of the primary node:

> >**cacls** *Drive_name***:\Fujitsu\ROR\SVROR\dhcp /T /P "NT AUTHORITY\SYSTEM:F" "BUILTIN**
> **\Administrators:F" "NT SERVICE\DHCPServer:F"** <RETURN>

10. Add the DHCP Server to "Services and Applications" for the manager.

   a. Right-click [Services and Applications]-[RC-manager], and select [Add a resource]-[Other Resources]-[1 - Add a DHCP Service] from the displayed menu.

   A [New DHCP Service] will be created in the [DHCP Service] in [Summary of RC-manager].

   b. Right-click the [New DHCP Service], and select [Properties] from the popup menu.

   The [New DHCP Service Properties] window will be displayed.

   c. Change the [Resource Name] on the [General] tab, and set the paths given in the following table.

Item	Value to Specify
Database path	*Drive_name*:\Fujitsu\ROR\SVROR\dhcp\
Monitoring file path	*Drive_name*:\Fujitsu\ROR\SVROR\dhcp\
Backup path	*Drive_name*:\Fujitsu\ROR\SVROR\dhcp\backup\

   After making the settings, click <Apply>.

   From here, the explanation is made assuming that [Resource Name] was set as [DHCP Server].

   d. On the "Resource" of the [Dependencies] tab, select the following name, and select AND from "AND/OR".

      - Shared Disks

      - Network Name

      - Admin LAN IP Address

   e. Click <Apply>.

   f. Click <OK>.

11. Configure the registry replication settings from the following "Services and Applications" of the manager.

   Following the table in step 2, set replication of the registry of the resource.

   Perform the following procedure for each resource.

   a. Right-click the target resource on [Other Resources] on the [Summary of RC-manager] displayed in the middle of the [Failover Cluster Management] window, and select [Properties] from the displayed menu.

   The [*target_resource* Properties] window will be displayed.

   b. Click <Add> on the [Registry Replication] tab.

   The [Registry Key] window will be displayed.

   c. Configure the above registry key in [Root registry key].

   d. Click <OK>.

   When configuring the second registry key as well, repeat steps b. to d.

   e. After configuration of the registry keys is complete, click <Apply>.

   f. Click <OK> to close the dialog.

12. Configure the dependencies of the resources of the manager "service or application".

   Configure the dependencies of resources based on the following table.

   If some resources have been configured, select AND from [AND/OR] and add the dependent resource.

Resource for Configuration	Dependent Resource
PXE Services	DHCP Server

13. Restart the manager.

   Right-click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree, and select [Bring this service or application online] from the displayed menu.

[Linux Manager]

ℹ️ **Information**
....
When configuring a cluster system in an environment that already has an admin LAN registered, in addition to the installation procedure for the cluster system, perform steps 1 to 2 and 4 to 11.
In that case, set the manager that is operating now as the primary node of the cluster system.
....

1. Stop cluster applications.

   Use the cluster system's operation management view (Cluster Admin) and stop the manager cluster service (cluster application).

2. Mount the shared disk (Primary node)

   Mount the shared disk for managers on the primary node.

3. Stop automatic startup of the dhcpd service (Primary node and Secondary node)

   Disable automatic startup of the dhcpd service by executing the following command.

   > # **chkconfig dhcpd off** <RETURN>

4. Copy dynamic disk files (Primary node)

   a. Copy the files and directory on the local disk of the primary node to the shared disk for managers.

      Execute the following command:

      > # **tar cf -** *copy_target* **| tar xf - -C** *Shared_disk_mount_point***/Fujitsu/ROR/SVROR** <RETURN>

      - Files and Directory to Copy

        - /etc/dhcpd.conf (*1)

        - /etc/dhcp/dhcpd.conf (*2)

        - /var/lib/dhcpd

        *1: When using Red Hat Enterprise Linux 5
        *2: When using Red Hat Enterprise Linux 6

   b. After copying the files, change source_file_name by executing the following command.

      Make sure a name like "*source_file_name*_old" is specified for the *target_file_name*.

      > # **mv -i** *source_file_name target_file_name* <RETURN>

5. Configure symbolic links for the shared disk (Primary node)

   Configure symbolic links from the files and directory on the local disk of the primary node for the files on the shared disk.

   Execute the following command:

   > # **ln -s** *shared_disk local_disk* <RETURN>

Table 7.1 Files to Link

Shared Disk	Local Disk
Mount_destination_of_shared_disk/Fujitsu/ROR/SVROR/etc/dhcpd.conf (*1)	/etc/dhcpd.conf
Mount_destination_of_shared_disk/Fujitsu/ROR/SVROR/etc/dhcp/dhcpd.conf (*2)	/etc/dhcp/dhcpd.conf
Mount_destination_of_shared_disk/Fujitsu/ROR/SVROR/var/lib/dhcpd	/var/lib/dhcpd

*1: When using Red Hat Enterprise Linux 5
*2: When using Red Hat Enterprise Linux 6

6. Change the settings of the DHCP service (Primary node)

   Change the following files when registering the admin LAN subnet, and set the takeover logical IP address after the change to the DHCP server.

   File name

   - Red Hat Enterprise Linux 5

     /etc/dhcpd.conf

   - Red Hat Enterprise Linux 6

     /etc/dhcp/dhcpd.conf

   Add the following lines, and set the takeover logical IP address.

   ```
   option dhcp-server-identifier takeover logical IP address;
   ```

   ## 📝 Example
   ・・・

   When the takeover logical IP address is 192.168.4.100

   ```
   #
   # DHCP Server Configuration file.
   # see /usr/share/doc/dhcp*/dhcpd.conf.sample
   #
   ddns-update-style none;
   option vendor-class-identifier "PXEClient";
   option dhcp-server-identifier 192.168.4.100; # This line is added.
   subnet 192.168.4.0 netmask 255.255.255.0 {
   ```

   ・・・

7. Unmount the shared disk. (Primary node)

   Unmount the shared disk for managers from the primary node.

8. Mount the shared disk (Secondary node)

   Mount the shared disk for managers on the secondary node.

9. Back up files and configure symbolic links for the shared disk (Secondary node)

   a. Perform step b. of step 4 and back up the files on the local disk.

   b. Perform step 5 and configure symbolic links for the shared disk.

10. Unmount the shared disk. (Secondary node)

    Unmount the shared disk for managers from the secondary node.

11. Start cluster applications.

    Use the cluster system's operation management view (Cluster Admin) and start the manager cluster service (cluster application).

12. Register the admin LAN subnet.

7.9 Registering ETERNUS SF Storage Cruiser

This section explains how to register ETERNUS SF Storage Cruiser.

Registering ETERNUS SF Storage Cruiser enables server switchover integrated with Fibre Channel switch zoning using ESC and host affinity reconfiguration on storage devices.
This operation is necessary when using server switchover (storage affinity switchover method) functions on managed servers (for Solaris) in SAN boot environments.

ETERNUS SF Storage Cruiser can be registered using the rcxadm storagemgr register command.
For details on the rcxadm storagemgr register command, refer to "5.13 rcxadm storagemgr" in the "Reference Guide (Command) VE".

7.10 Registering LAN Switches

Use the following procedure to register LAN switches:

1. Discover LAN switches. For instructions, refer to "Discovery".

2. Register LAN switches displayed in the network device tree. For instructions, refer to "Register".

Discovery

1. From the ROR console menu, select [Tools]-[Topology]-[Discover LAN switches].

   The [Discover LAN Switches] dialog is displayed.

2. Perform the following settings:

   Start address

   Enter the start IP address of the network in which to discover LAN switches.
   Enter the IP address using periods ".".

   Subnet mask

   Enter the subnet mask of the network where to discover LAN switches.
   Enter the IP address using periods ".".

   Addresses in range

   Enter the number of addresses to scan for LAN switches.
   Enter a number greater than 1.
   The maximum number of addresses is determined by the number of hosts allowed by the subnet mask.

   ### Example
   ....
   If subnet mask is "255.255.255.0", the number of addresses in the specified range could be any value between 1 and 256.
   ....

   SNMP Community

   Enter the SNMP community that was set on this LAN switch.
   Either select [public] or enter an arbitrary string.
   Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

3. Click <OK>.

   Resource Orchestrator starts scanning for LAN switches within the specified network range.
   Discovered LAN switches will be displayed under the network device tree with the status [[Unregistered]].

Register

1. In the ROR console network device tree, right-click a discovered LAN switch, and select [Register]-[LAN Switch] from the popup menu.

   The [Register LAN Switch] dialog is displayed.

2. Perform the following settings:

   LAN switch name

   Enter the name to assign to this LAN switch.
   Enter up to 32 characters, including alphanumeric characters (upper or lower case), underscores ("_"), hyphens ("-"), or periods (".").
   By default, the name of a discovered LAN switch will be set to its system name or to its IP address if the system name could not be detected.

   SNMP Community

   Enter the SNMP community that was set on this LAN switch.
   Either select [public] or enter an arbitrary string.
   Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

3. Click <OK>.

   The registered LAN switch will be displayed in the network device tree.

Note

It is possible to set an automatically detected IP address to another unregistered LAN switch. However, this will result in the Resource Orchestrator configuration being inconsistent with the actual network configuration.
If a LAN switch was registered with the IP address of another network device, delete the registered LAN switch following the instructions given in "11.4.2 Deleting LAN Switches ", then perform Discover and Register again.

7.11 Registering Converged Fabric Management Software

This section explains how to register the management software necessary for managing Converged Fabric when using ServerView Fabric Manager.

When registering the ServerView Fabric Manager as Converged Fabric management software, use the Windows manager. Other managers cannot be registered.

Use the following procedure to configure management software (Converged Fabric) settings:

1. From the ROR console menu, select [Settings]-[Register]-[Management Software(SVFAB)].

   The [Register Management Software(SVFAB)] dialog is displayed.

2. Define the following settings:

   Management software name

   Enter the name of the target Converged Fabric management software.
   Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

3. Click <OK>.

   The registered Converged Fabric management software will be displayed in the management software tree.

Note

In order to start the ServerView Fabric Manager window from the [Management Software] tab in the ROR console, it is necessary to configure ServerView Operations Manager Single Sign-On.
Allocate appropriate roles to users in advance.

For details, refer to "10.2.2 Single Sign-On When Using the ServerView Operations Manager Console" in the "Design Guide VE".

Chapter 8 Changing Admin Server Settings

This chapter explains how to change the settings for the admin server.

8.1 Changing Admin IP Addresses

Use the following procedure to change the IP address used on the admin LAN by the admin server.

1. Log on to the admin server with OS administrative privileges.

2. Stop the manager.

   Stop the manager, referring to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

3. Change the SNMP trap destination set for the management blade and LAN switch blades.

   Set the SNMP trap destination to the new IP address of the admin server.

   ### 🗊 Note
   ⋅⋅

   Depending on the LAN switch blade used, setting an SNMP trap destination may restrict SNMP access to the LAN switch.
   When PY CB Eth Switch 10/40Gb 18/8+2 and virtual IP address of Converged Fabric are specified and LAN switch blade is registered, the SNMP trap cannot be received.
   When making LAN switch blades in a clustered manager configuration the target of management, set the physical IP addresses of both the primary and secondary nodes as SNMP trap destinations.
   If the LAN switch blade is set to only grant access from known IP addresses, be sure to give permissions to the physical IP addresses of both the primary and secondary cluster nodes, as is done with trap destination settings.
   For details, refer to the manual of the LAN switch blade to be used.
   ⋅⋅

4. Change the IP address set within the operating system.

   Change the IP address following the instructions given in the operating system's manual.
   If the admin LAN has been made redundant, change the admin IP address set in the following tools or products.

   - PRIMECLUSTER GLS

   - BACS

   - Intel PROSet

   Refer to the manual of each product for usage details.

   In a clustered manager configuration, change the cluster IP address according to the instructions given in "Changing the IP Address of a Clustered Manager".

5. Change the IP address registered as the manager's admin IP address.

   Use the rcxadm mgrctl modify command to set a new IP address.

   [Windows Manager]

   ```
   >"Installation_folder\SVROR\Manager\bin\rcxadm" mgrctl modify -ip IP_address <RETURN>
   ```

   [Linux Manager]

   ```
   # /opt/FJSVrcvmr/bin/rcxadm mgrctl modify -ip IP_address <RETURN>
   ```

   In a clustered manager configuration, for details on how to change the admin IP address registered for the manager, refer to "Settings for Clustered Manager Configurations".

6. Log in to the managed server with an OS administrator account.

7. Change ServerView Agents settings on the managed server.

   Change the SNMP trap destination of the ServerView Agents. Refer to the ServerView Agent manual for details on changing SNMP trap settings.

8. Stop the agents on managed servers. [Windows] [Hyper-V] [Linux] [Xen] [KVM]

   Stop the agent referring to "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

9. Change Agent settings. [Windows] [Hyper-V] [Linux] [Xen] [KVM]

   Use the rcxadm agtctl modify command to set the new manager IP address.

   [Windows] [Hyper-V]

   > **"***Installation_folder***\Agent\bin\rcxadm" agtctl modify -manager** *IP_address* <RETURN>

   [Linux] [Xen] [KVM]

   # /opt/FJSVrcxat/bin/rcxadm agtctl modify -manager *IP_address* <RETURN>

10. Restart the agents on managed servers. [Windows] [Hyper-V] [Linux] [Xen] [KVM]

    Start the agent referring to "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

11. Restart the manager.

    Start the manager referring to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

    Repeat steps 6 to 11 for each managed server on which an agent is running.

12. Reconfigure the HBA address rename setup service.

    When using the HBA address rename function, change the IP address of the admin server that is set for the HBA address rename setup service according to "Chapter 6 Settings for the HBA address rename Setup Service" in the "Setup Guide VE".

13. Back up managed servers.

    If system image backups have already been collected from managed servers, it is recommended to update those images in order to reflect the changes made above. For details on system image backups, refer to "9.2 Backup" in the "Operation Guide VE".

    System images backed up before changing the admin IP address of the admin server cannot be restored anymore after the change. It is recommended to delete all system images collected before change, unless those images are specifically needed.

14. Collect a cloning image. [Physical Servers]

    If cloning images have already been collected from managed servers, it is recommended to update those images to reflect the change made above. For details on cloning image collection, refer to "17.2 Collecting".

    Cloning images collected before changing the admin IP address of the admin server cannot be deployed anymore after the change. It is recommended to delete all cloning images collected before change, unless those images are specifically needed.

Note

- IP addresses belonging to registered admin LAN subnets cannot be changed.

- When a managed server belongs to the same subnet as the admin server, either delete the managed server or manually change the admin IP address of the managed server. Without changing the IP address of the managed server, it is not possible to register the information of the subnet the managed server belongs to, or change the information of the subnet.

Changing the IP Address of a Clustered Manager

In a clustered manager configuration, use the following procedure to change the IP address set within the operating system.

[Windows Manager]
Change the IP address using the [Failover Cluster Management] window.

[Linux Manager]

1. Stop the manager's cluster service.

   Stop the manager's cluster service from the cluster administration view (Cluster Admin).

2. Log in to the admin server's primary node.

   Log in to the operating system of the admin server's primary node with administration privileges.

3. Mount the shared disk on the primary node.

   Mount the admin server's shared disk on the primary node.

4. Change takeover the logical IP address.

   Release PRIMECLUSTER GLS virtual interface settings from the PRIMECLUSTER resource, then change the PRIMECLUSTER GLS configuration.

   For details, refer to the PRIMECLUSTER Global Link Services manual.

5. Activate the takeover logical IP address.

   Use the PRIMECLUSTER GLS command-line to activate the takeover logical IP address.

   For details, refer to the PRIMECLUSTER Global Link Services manual.

Settings for Clustered Manager Configurations

In a clustered manager configuration, use the following procedure to register an IP address as the manager's admin LAN IP address.

[Windows Manager]

1. Cancel registry replication settings.

   On the primary node, bring online the shared disk and IP address, and take all other resources offline.
   Next, remove the following registry key from the registry replication settings set for the [PXE Services] cluster resource.

   - x64

     SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\DHCP

   - x86

     SOFTWARE\Fujitsu\SystemcastWizard\DHCP

   Use the following procedure to remove the registry key.

   a. In the [Failover Cluster Management] window, right-click the "PXE Services" resource in [Summary of RC-manager]-[Other Resources], and select [Properties] from the popup menu.

      The [PXE Services Properties] window will be displayed.

   b. In the [Registry Replication] tab, select the above registry key.

   c. Click <Remove>.

      The selected key is removed from the [Root registry key] list.

   d. After removing the registry key, click <Apply>.

   e. Click <OK> to close the dialog.

2. Change the manager IP address on the primary node.

   On the primary node, use the rcxadm mgrctl modify command to set the new IP address.

   > ```
   >"Installation_folder\SVROR\Manager\bin\rcxadm" mgrctl modify -ip IP_address <RETURN>
   ```

3. Restore registry replication settings.

   Restore the registry key deleted in step 1 to the registry replication settings of the [PXE Services] resource.
   Use the following procedure to restore the registry key.

   a. In the [Failover Cluster Management] window, right-click the "PXE Services" resource in [Summary of RC-manager]-[Other Resources], and select [Properties] from the popup menu.

      The [PXE Services Properties] window will be displayed.

   b. Click <Add> on the [Registry Replication] tab.

      The [Registry Key] window will be displayed.

   c. Configure the above registry key in [Root registry key].

   d. Click <OK>.

   e. After configuration of the registry keys is complete, click <Apply>.

   f. Click <OK> to close the dialog.

4. Assign the manager's shared disk and IP address to the secondary node.

   Right-click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree, and select [Move this service or application to another node]-[1 - Move to node *node_name*] from the displayed menu.
   The name of the secondary node is displayed for *node_name*.

5. Change the manager IP address on the secondary node.

   On the secondary node, use the rcxadm mgrctl modify command to set the new IP address.
   Use the same IP address as the one set in step 2.

6. Assign the manager's shared disk and IP address to the primary node.

   Right-click [Services and Applications]-[RC-manager] on the Failover Cluster Management tree, and select [Move this service or application to another node]-[1 - Move to node *node_name*] from the displayed menu.
   The name of the primary node is displayed for *node_name*.

7. On the primary node, take the manager's shared disk and IP address offline.

[Linux Manager]

1. Change the IP address set for the admin LAN.

   Set a new IP address on the primary node using the following command.

   > # **/opt/FJSVrcvmr/bin/rcxadm mgrctl modify -ip** *IP_address* <RETURN>

2. De-activate the admin server's takeover logical IP address.

   Use the PRIMECLUSTER GLS command-line interface to de-activate the takeover logical IP address.

   For details, refer to the PRIMECLUSTER Global Link Services manual.

3. Register the takeover logical IP address as a PRIMECLUSTER resource.

   Use the PRIMECLUSTER GLS command-line interface to register the virtual interface as a PRIMECLUSTER resource.

   For details, refer to the PRIMECLUSTER Global Link Services manual.

4. Mount the shared disk

   Mount the shared disk for managers on the primary node.

5. Change the settings of the DHCP service (When registering the admin LAN subnet)

   When registering an admin LAN subnet, change the file below and set the DHCP server for the takeover logical IP address.

   - File name

      - Red Hat Enterprise Linux 5

        /etc/dhcpd.conf

- Red Hat Enterprise Linux 6

    /etc/dhcp/dhcpd.conf

Change the takeover logical IP address in the following line to the new takeover logical IP address.

option dhcp-server-identifier *takeover logical IP address*;

📋 **Example**
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

When the takeover logical IP address is 192.168.4.100 before being changed

```
#
# DHCP Server Configuration file.
# see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style none;
option vendor-class-identifier "PXEClient";
option dhcp-server-identifier 192.168.4.100; (*)
subnet 192.168.4.0 netmask 255.255.255.0 {
```

* Note: Change the IP address in this line to the new takeover logical IP address.
. . . .

6. Unmount the shared disk.

    Un-mount the shared disk from the primary node.

7. Log in to the admin server's secondary node.

    Log in to the operating system of the admin server's secondary node with administration privileges.

8. Change takeover the logical IP address.

    Use the PRIMECLUSTER GLS command-line interface to remove virtual interface settings from the PRIMECLUSTER resource, register the resource, and change the PRIMECLUSTER GLS configuration.

    For details, refer to the PRIMECLUSTER Global Link Services manual.

9. Change the cluster configuration.

    Use the cluster RMS Wizard to change the GLS resource set in the cluster service of either one of the cluster nodes.

    After completing the configuration, save it and execute the following operations.

    - Configuration-Generate

    - Configuration-Activate

10. Start the Manager's cluster service.

    Use the cluster administration view (Cluster Admin) to start the Manager's cluster service.

8.2 Changing Port Numbers

This section explains how to change the ports used by the Manager services and related services of Resource Orchestrator.

Resource Orchestrator requires the following services to be running. When starting these services, ensure that the ports they are using do not conflict with the ports used by other applications or services. If necessary, change the ports used by Resource Orchestrator services.

[Windows Manager]

- Manager Services

    - Resource Coordinator Manager

    - Resource Coordinator Task Manager

    - Resource Coordinator Web Server(Apache)

- Resource Coordinator Sub Web Server(Mongrel)

- Resource Coordinator Sub Web Server(Mongrel2)

- Resource Coordinator DB Server (PostgreSQL)

- Related Services

- Deployment Service

- TFTP Service

- PXE Services

- DHCP Server (*)

[Linux Manager]

- Manager Services

- rcxmanager

- rcxtaskmgr

- rcxmongrel1

- rcxmongrel2

- rcxhttpd

- rcxdb

- Related Services

- scwdepsvd

- scwpxesvd

- scwtftpd

- dhcpd (*)

* Note: Necessary when managing a managed server in a separate subnet to the admin server.
Change the ports used by the above services if there is a possibility that they will conflict with other applications or services.

For Windows operating systems, an ephemeral port may conflict with a Resource Orchestrator service if the range allowed for ephemeral ports is changed. In this case, change the port number to a value not included in the range for ephemeral ports.

For details, refer to "2.1.1.4 Checking Used Port Numbers" in the "Setup Guide VE".

For information on how to change the ports used by ServerView Operations Manager, refer to the ServerView Operations Manager manual. The ports used for SNMP communication and server power control are defined by standard protocols and fixed at the hardware level, and thus cannot be changed.

For the port numbers used by Resource Orchestrator, refer to "Appendix A Port List" in the "Design Guide VE".
When using a firewall on the network, firewall settings should be updated to match the new port definitions and allow communications for any modified port.

Manager Services

Use the following procedure to change the admin server ports used by manager services:

1. Stop the manager.

   Stop the manager, referring to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

2. Change the port numbers.

   Use the rcxadm mgrctl modify command to set a new port number for a given service name.

   [Windows Manager]

```
>"Installation_folder\SVROR\Manager\bin\rcxadm" mgrctl modify -port name=number
<RETURN>
```

[Linux Manager]

```
# /opt/FJSVrcvmr/bin/rcxadm mgrctl modify -port name=number <RETURN>
```

In a clustered manager configuration, bring offline all cluster resources except for the manager's shared disk and IP address, move all cluster resources from the primary node to the secondary node, then execute the rcxadm mgrctl modify command on all the nodes that are hosting cluster resources.

3. Restart manager services.

   Start the manager referring to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

Note

- When changing the "rcxweb" port, the following ports should be set to the same value.

  - Admin client

    Enter the "rcxweb" port in the Web browser URL used to log into Resource Orchestrator.
    If this URL is bookmarked in the Web browser "Favorites", change the port set in the bookmark's URL.

  - HBA address rename setup service

    If the HBA address rename setup service is running, change the port number used to communicate with the admin server to the "rcxweb" port according to "9.2.2 Changing the Port Number Used to Communicate with the Admin Server".

  [Windows Manager]

  - Change the ROR console shortcut on the manager

    1. Open the following folder on the admin server.

       Installation_folder\SVROR\Manager

    2. Right-click the "ROR Console" icon, and select [Properties] from the popup menu.

    3. In the [Web Document] tab, change the port number set in the "URL" field (as shown below).

       ```
       URL: https://localhost:23461/
       ```

    4. Click <OK>.

- When changing the "nfagent" port, the following ports on managed servers should be set to the same value.

  Set the "nfagent" port set on each managed server to the same value, according to the instructions given in "9.1.6 Changing Port Numbers".
  The system image and cloning images collected before the change can no longer be used, and should be deleted.
  If necessary, re-collect system images and cloning images.

Related Services

Use the following procedure to change the port numbers used for the related services: However, the port numbers of the DHCP server and the dhcpd service cannot be changed.

[Windows Manager]

1. Change the port numbers.

    a. Open the Windows Registry Editor, and search for the following subkey:

        - When using a 32-bit version of Windows:

            Key name: HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\SystemcastWizard\CLONE

        - When using a 64-bit version of Windows:

            Key name: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\CLONE

    b. Select "PortBase" from the registry entries under this subkey.

    c. From the menu, select [Edit]-[Modify].

        The [Edit DWORD Value] dialog is displayed.

    d. Select [Decimal] and click <OK>.

        This port value will define the first port of the range used by deployment services.

        However, because the related services can use up to 16 port numbers, ensure that all ports included between "PortBase" (defined here) and "PortBase+15" do not conflict with any other applications or services. Moreover, be sure to set a value lower than 65519 for "PortBase" so that the highest port number ("PortBase+15") does not exceed the largest valid port number (65534).
        In a clustered manager configuration, change port numbers on both the primary and secondary node.

2. Restart the server on which the port number has been changed.

[Linux Manager]

1. Change the port numbers.

    Edit the following file: /etc/opt/FJSVscw-common/scwconf.reg.

    In PortBase (under HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\SystemcastWizard\CLONE), set the first value of the port number to be used by deployment services. This value should be entered in hexadecimal format. To avoid conflicts with ephemeral ports, use a value not included in the ephemeral port range defined by "net.ipv4_local_port_range".

    However, as a maximum of 16 port numbers are used for image file creation and deployment, ensure that the port numbers for PortBase to PortBase +15 do not conflict with ephemeral or well-known ports.

    This ensures that deployment services will use ports outside of the range defined by net.ipv4.ip_local_port_range for image operations.

    Moreover, be sure to set a value lower than 65519 for "PortBase" so that the highest port number ("PortBase+15") does not exceed the largest valid port number (65534).
    In a clustered manager configuration, change port numbers on both the primary and secondary node.

2. Restart the server on which the port number has been changed.

📖 Information
....

The related services allow managed servers to boot from the network using a dedicated module stored on the admin server during backup, restore or cloning.
Note that changing port numbers on the admin server alone is enough to support communication during the above image operations. Therefore, no additional configuration is required on the managed servers.
....

8.3 Changing the Maximum Number of System Image Versions

Use the following procedure to change the maximum number of system image versions.

1. Change the maximum number of system image versions.

2. Confirm the maximum number of system image versions.

For details of the methods for changing and checking the generations of system images, refer to "5.8 rcxadm imagemgr" in the "Reference Guide (Command) VE".

![Note icon] **Note**

. . . .

If the specified limit is smaller than the number of existing system image versions, older versions will not be deleted automatically. In this case, backing up a new system image, will only delete the oldest version.

Delete unused versions of system images manually if they are no longer necessary. For details, refer to "16.5 Deleting".

If the ROR console has been already opened, refresh the Web browser after changing the maximum number of system image versions.

. . . .

8.4 Changing the Maximum Number of Cloning Image Versions

Use the following procedure to change the maximum number of cloning image versions.

1. Change the maximum number of cloning image versions.

2. Check the maximum number of cloning image versions.

For details of the methods for changing and checking the generations of cloning images, refer to "5.8 rcxadm imagemgr" in the "Reference Guide (Command) VE".

![Note icon] **Note**

. . . .

If the specified limit is smaller than the number of existing cloning image versions, older versions will not be deleted automatically. In this case, collecting a new cloning image version will require selecting a previous image version for deletion.

Delete unused image versions manually if they are no longer necessary. For details, refer to "17.5 Deleting".

If the ROR console has been already opened, refresh the Web browser after changing the maximum number of system image versions.

. . . .

8.5 Changing the Image Folder Location

Use the following procedure to change the location (path) of the image files folder.

1. Select the [Image List] tab in the ROR console and confirm the current image list.

2. Log on to the admin server with OS administrative privileges.

3. Stop the manager.

   Stop the manager, referring to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

4. Change the location of the image file storage folder.

   Change the location of the image file storage folder according to the instructions given in "5.8 rcxadm imagemgr" in the "Reference Guide (Command) VE".
   Because image files are actually copied over to the new location, this step may take some time to complete.

   In a clustered manager configuration, for details on how to change the image file storage folder location, refer to "Settings for Clustered Manager Configurations".

5. Restart the manager.

   Start the manager referring to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

6. Select the [Image List] tab in the ROR console and confirm the image list is same as before.

Settings for Clustered Manager Configurations

Settings differ depending on the operating system used for the manager.

[Windows Manager]

1. Cancel registry replication settings.

   Bring the manager's shared disk online, and take all other resources offline.
   Next, remove the following registry key from the registry replication settings set for the [Deployment Service] cluster resource.

   - x64

     SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard\ResourceDepot

   - x86

     SOFTWARE\Fujitsu\SystemcastWizard\ResourceDepot

   Use the following procedure to remove the registry key.

   a. In the [Failover Cluster Management] window, right-click the [Deployment Service] resource in [Summary of RC-manager]-[Other Resources], and select [Properties] from the popup menu.

      The [Deployment Service Properties] window is displayed.

   b. In the [Registry Replication] tab, select the above registry key.

   c. Click <Remove>.

      The selected key is removed from the "Root registry key" list.

   d. After removing the registry key, click <Apply>.

   e. Click <OK> to close the dialog.

2. Change the location of the image file storage folder.

   Change the location of the image file storage folder according to the instructions given in "5.8 rcxadm imagemgr" in the "Reference Guide (Command) VE".
   Because image files are actually copied over to the new location, this step may take some time to complete.

   Run the rcxadm imagemgr command from either node of the cluster resource.
   The new location should be a folder on the shared disk.

3. Restore registry replication settings.

   Restore the registry key deleted in step 1 to the registry replication settings of the [Deployment Service] resource.
   Use the following procedure to restore the registry key.

   a. In the [Failover Cluster Management] window, right-click the [Deployment Service] resource in [Summary of RC-manager]-[Other Resources], and select [Properties] from the popup menu.

      The [Deployment Service Properties] window is displayed.

   b. Click <Add> on the [Registry Replication] tab.

      The [Registry Key] window will be displayed.

   c. Configure the above registry key in [Root registry key].

   d. Click <OK>.

   e. After configuration of the registry keys is complete, click <Apply>.

   f. Click <OK> to close the dialog.

[Linux Manager]

1. Mount the shared disk on the primary node.

   Log in to the primary node with OS administrator privileges and mount the admin server's shared disk.

2. Change the location of the image file storage directory.

   Change the location of the image file storage directory according to the instructions given in "5.8 rcxadm imagemgr" in the "Reference Guide (Command) VE".

   Because image files are actually copied over to the new location, this step may take some time to complete.

Run the rcxadm imagemgr command on the primary node.

Also, specify a directory on the shared disk for the new image file storage directory.

3. Un-mount the shared disk from the primary node.

Un-mount the shared disk (for which settings were performed in step 1) from the primary node.

8.6 Changing the Password for the Resource Orchestrator Database

Use the following procedure to change the password for the Resource Orchestrator database:

1. Log on to the admin server with OS administrative privileges.

2. Stop the manager.

Stop the manager, referring to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

3. Change the password for the Resource Orchestrator database.

Execute the rcxadm dbctl modify command.
Enter the new password interactively.

[Windows Manager]

>**"**_Installation_folder_**\SVROR\Manager\bin\rcxadm" dbctl modify -passwd** <RETURN>

[Linux Manager]

/opt/FJSVrcvmr/bin/rcxadm dbctl modify -passwd <RETURN>

In a clustered manager configuration, bring offline all manager resources except for the shared disk, move all cluster resources from the primary node to the secondary node, then execute the rcxadm dbctl modify command on all the nodes that are hosting cluster resources.

4. Restart the manager.

Start the manager referring to "2.1 Starting and Stopping Managers" in the "Operation Guide VE".

Chapter 9 Changing Resources

This chapter explains how to change settings for the admin server or resources registered on the admin server.

9.1 Changing Chassis and Managed Server Settings

This section explains how to change the settings for chassis and managed servers.
If collecting the system images and cloning images of managed servers, collect them after completing changes to managed server settings.

For details on backing up system images, refer to "16.2 Backup".

For details on how to collect cloning images, refer to "17.2 Collecting".

Note

. . . .

- To change VM guest settings, use the management console of the server virtualization software used.

- A managed server that has already been registered cannot be moved to a different slot.
  To move a managed server to a different slot, first delete the managed server, then move it to the new slot and register it again.

. . . .

9.1.1 Changing Chassis Names

This section explains how to change chassis names.
Use the following procedure to change the name of a registered chassis.

1. In the ROR console server resource tree, right-click the target chassis and select [Modify]-[Registration Settings] from the popup menu.

   The [Modify Chassis Settings] dialog is displayed.

2. Modify the values for the following items:

   Chassis name

      Enter a character string beginning with an alphabetical character and containing up to 10 alphanumeric characters and hyphens ("-").

3. Click <OK>.

   The chassis name is changed.

9.1.2 Changing Server Names

This section explains how to change physical server names.
Names of physical OSs, VM hosts, and VM guests can be changed by a user with administrative authority. Once changed, new names are automatically reflected in the ROR console.

Use the following procedure to change the name of a physical server.

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

   The [Modify Server Settings] dialog is displayed.

2. Modify the values for the following items:

   Physical Server Name

      Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

3. Click <OK>.

   The server name is changed.

4. If the network parameter auto-configuration function is used in the deployment of the cloning images, the "Physical Server Name" set in the definition file must also be changed.

   For details on the network parameter auto-configuration function, refer to "17.6 Network Parameter Auto-Configuration for Cloning Images".

9.1.3 Changing Admin IP Addresses

This section explains how to change admin IP addresses.

To change the IP addresses of remote management controllers, refer to "9.1.5 Changing Server Management Unit Configuration Settings".

Chassis

Use the following procedure to change the IP address of a chassis.

1. Change the IP address of the management blade.

2. In the ROR console server resource tree, right-click the target chassis and select [Modify]-[Registration Settings] from the popup menu.

   The [Modify Chassis Settings] dialog is displayed.

3. Change "Admin LAN (IP address)".

4. Click <OK>.

   The chassis admin IP address is changed.

Managed Servers

Use the following procedure to change the IP address of a managed server.
However, it is still required when using the same address for both the admin and public IP address. This procedure is not required when changing only the public IP address of a server.

1. Log in to the managed server with an OS administrator account.

2. Change the IP address set within the operating system.

   Change the IP address according to the OS manual.
   If the admin LAN has been made redundant, change the admin IP address set in the following tools or products.

   Refer to the manual of each product for usage details.

   [Windows]
   PRIMECLUSTER GLS
   BACS
   Intel PROSet

   [Linux] [Solaris]
   PRIMECLUSTER GLS: "NIC switching mode (Physical IP address takeover function)"

Note

When BladeLogic is being used for server management software, remove the managed servers that have been added to BladeLogic, and add them again. When adding managed servers, specify their admin IP address.

3. Restart the managed server.

4. In the ROR console server resource tree, right-click the target server, and select [Modify]-[Registration Settings] from the popup menu.

   The [Modify Server Settings] dialog is displayed.

5. Change [Admin LAN (IP address)].

6. Click <OK>.

   The admin IP address of the managed server is changed.

Note

- -

- It is not possible to change IP address settings of a managed server (primary server) with a spare server configured to a different subnet from the spare server.

- Please reregister of ESXi Server after changing IP address.

- -

Guest Domain of Oracle VM for SPARC

When an Oracle VM for SPARC guest domain is registered as a VM host, use the following procedure to change its admin IP address. However, it is still required when using the same address for both the admin and public IP address.
This procedure is not required when changing only the public IP address of a server.

1. Log in to the guest domain using an OS administrator account.

2. Change the IP address set within the operating system.

   Change the IP address according to the OS manual.

   If the admin LAN has been made redundant, change the admin IP address set in the "NIC switching mode (Physical IP address takeover function)" of PRIMECLUSTER GLS.

Note

- -

When BladeLogic is being used for server management software, remove the managed servers that have been added to BladeLogic, and add them again.
When adding managed servers, specify their admin IP address.

- -

3. Restart the guest domain.

4. In the ROR console server resource tree, right-click the target server, and select [Modify]-[Registration Settings] from the popup menu.

   The [Modify IP Address Settings] dialog is displayed.

5. Change [Admin LAN IP Address].

6. Click <OK>.

   The admin IP address of the guest domain is changed.

9.1.4 Changing SNMP Communities

This section explains how to change SNMP community settings.

- For blade servers, PRIMEQUEST servers, or SPARC Enterprise M4000/M5000/M8000/M9000 servers, or servers in SPARC M10-4S

  Use the following procedure to change SNMP community used by chassis and managed servers.

  1. Change the SNMP community set on the management blade, management board, or XSCF.

     The new SNMP community should have Read-Write permission.
     For details on changing SNMP communities, refer to the manual of the management blade, management board, or XSCF.

  2. Change the SNMP community set on the managed server.

     Use the same name for the SNMP community of the managed server on the management blade, the management board, and the XSCF.

Follow the instructions in the ServerView Agents manual to change the SNMP community used by a managed server.
The new SNMP community should have Read-Write permission.

3. In the ROR console server resource tree, right-click the target chassis and select [Modify]-[Registration Settings] from the popup menu.

   The [Modify Chassis Settings] dialog is displayed.

4. Change [SNMP Community].

5. Click <OK>.

   The SNMP community is changed.

- For Rack Mount and Tower Servers

Use the following procedure to change the SNMP community used by PRIMERGY servers.
For servers other than PRIMERGY servers, changing SNMP communities does not require any configuration change in Resource Orchestrator.

1. Change the SNMP community set on the managed server.

   Follow the instructions in the ServerView Agents manual to change the SNMP community used by a managed server.

2. In the ROR console server resource tree, right-click the target server, and select [Modify]-[Registration Settings] from the popup menu.

   The [Modify Server Settings] dialog is displayed.

3. Change [SNMP Community].

4. Click <OK>.

   The SNMP community is changed.

- For SPARC Enterprise M3000 or SPARC M10-1/M10-4

Use the following procedure to change the SNMP community used by the Remote Management Controller.

1. Change the SNMP community set on the remote management controller (XSCF).

   For details on changing SNMP communities, refer to the XSCF manuals.

2. In the ROR console server resource tree, right-click the target chassis and select [Modify]-[Registration Settings] from the popup menu.

   The [Modify Chassis Settings] dialog is displayed.

3. Change [SNMP Community].

4. Click <OK>.

   The SNMP community is changed.

9.1.5 Changing Server Management Unit Configuration Settings

This section explains how to modify server management unit settings.

- For rack mount or tower servers

Use the following procedure to change remote management controller settings.

1. Change settings on the remote management controller.
   If the user account is changed, it should still have administrator authority.

2. In the ROR console server resource tree, right-click the target server, and select [Modify]-[Registration Settings] from the popup menu.

   The [Modify Server Settings] dialog is displayed.

3. Change the [Remote Management Controller IP address]. To modify user account information, select the [Modify remote management controller login account] checkbox, and change the [User ID] and [Password] of the [Remote management controller].

- For SPARC Enterprise M3000 or SPARC M10-1/M10-4

   Use the following procedure to change remote management controller (XSCF) settings.

   1. Change settings on the remote management controller (XSCF).
      If the user account is changed, it should still have administrator authority ("platadm" privileges).

   2. In the ROR console server resource tree, right-click the target server, and select [Modify]-[Registration Settings] from the popup menu.

      The [Modify Server Settings] dialog is displayed.

   3. Change the [Remote Management Controller IP address (ILOM/XSCF)].
      To modify user account settings, select the [Modify remote management controller login account] checkbox, and change the [User ID] and [Password] fields under [Remote management controller (ILOM/XSCF)].

      The user ID reserved for the system cannot be used. Create another user ID.
      For details, refer to the XSCF manuals.

- For SPARC Enterprise T series

   Use the following procedure to change remote management controller settings (ILOM).

   1. Change settings on the remote management controller (ILOM).
      If the user account is changed, it should still have administrator authority ("Admin" privileges).

   2. In the ROR console server resource tree, right-click the target server, and select [Modify]-[Registration Settings] from the popup menu.
      The [Modify Server Settings] dialog is displayed.

   3. Change the [Remote Management Controller IP address (ILOM/XSCF)].
      To modify user account settings, select the [Modify remote management controller login account] checkbox, and change the [User ID] and [Password] fields under [Remote management controller (ILOM/XSCF)].

- For PRIMEQUEST servers

   Use the following procedure to change remote server management settings.

   1. Change the remote server management settings.
      If the user account is changed, it should still have administrator authority.

   2. In the ROR console server resource tree, right-click the target chassis and select [Modify]-[Registration Settings] from the popup menu.

      The [Modify Chassis Settings] dialog is displayed.

   3. Select the [Modify remote server management login account] checkbox. Then, change the [User ID] and [Password] of [Remote Server Management].

- For SPARC Enterprise M4000/M5000/M8000/M9000 or SPARC M10-4S

   Use the following procedure to change remote management controller (XSCF) settings.

   1. Change settings on the remote management controller (XSCF).

      If the user account is changed, it should still have administrator authority ("platadm" privileges).

   2. In the ROR console server resource tree, right-click the target chassis and select [Modify]-[Registration Settings] from the popup menu.

      The [Modify Chassis Settings] dialog is displayed.

   3. Select the [Modify remote server management login account] checkbox. Then, change the [User ID] and [Password] of [Remote Server Management (XSCF)].

      The user ID reserved for the system cannot be used. Create another user ID.
      For details, refer to the XSCF manuals.

9.1.6 Changing Port Numbers

This section explains how to change port numbers.

When changing port numbers of the agent, the "nfagent" port of the manager must also be changed. Change this according to information in "8.2 Changing Port Numbers".
For details on port numbers, refer to "Appendix A Port List" in the "Design Guide VE".

Use the following procedure to change the port numbers for managed servers:

1. Change the port numbers.

   [Windows] [Hyper-V]
   Use a text editor (such as Notepad) to change the following line in the *Windows_system_folder*\system32\drivers\etc\services file.

   ```
   # service name port number/protocol name
   nfagent      23458/tcp
   ```

   [Linux] [VMware] [Xen] [Citrix Xen] [KVM]
   Use a command such as vi to change the following line in the /etc/services file.

   ```
   # service name port number/protocol name
   nfagent      23458/tcp
   ```

   [Solaris]
   Use a command such as vi to change the following line in the /etc/services file.

   ```
   # service name port number/protocol name
   rcvat        23458/tcp
   ```

2. Restart the server on which the port number has been changed.

9.1.7 Changing VM Host Login Account Information

This section explains how to change VM host login account information.

If the login account information (user ID and password) of the VM host entered when the VM host was registered is changed, change the login account information of the VM host that was registered in Resource Orchestrator.

The method for changing the VM host login account is shown below.

1. In the ROR console server resource tree, right-click the target VM host, and select [Modify]-[VM Host Login Account] from the popup menu.

   The [Change Login Information] dialog is displayed.

2. Enter the new login account information that was changed on the VM host.

   User ID

   > Enter the user ID to log in to the VM host. Specify a user ID that has VM host administrator authority.

   Password

   > Enter the password of the user to log in to the VM host.

3. Click <OK>.

   VM host login information is changed.

9.1.8 Changing the VLAN Settings of LAN Switch Blades

This section explains how to change VLAN settings of LAN switch blades.
The VLAN settings of the LAN switch blade ports connected to the physical servers can be reconfigured normally within Resource Orchestrator.

Refer to "7.3.4.2 Configuring VLANs on Internal Ports" for details on how to configure these settings.

9.1.9 Changing HBA address rename Settings

This section explains how to change the HBA address rename settings.

The WWNs and HBA ports that are set by HBA address rename can be reconfigured normally within Resource Orchestrator.
Refer to "7.4.2 HBA address rename Settings" for details on how to configure these settings.

9.1.10 Changing Boot Options

This section explains how to change boot option settings.

The boot options configured for PRIMEQUEST servers can be changed by reconfiguring them.

Use the following procedure to configure the boot option settings.

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

   The [Modify Server Settings] dialog is displayed.

2. Perform the following settings:

   Boot option

   - For UEFI

     Select [UEFI].

   - For Legacy Boot

     Select [Legacy boot].

Note

. . . .

Changing the boot option changes the information registered with Resource Orchestrator.
As the actual boot option will not be changed, it is necessary to change the BIOS settings when performing the change.

. . . .

9.1.11 Changing Admin LAN Subnets

Use the following procedure to change an admin LAN subnet.

1. From the ROR console menu, select [Settings]-[Admin LAN Subnet].

   The [Admin LAN Subnet] dialog is displayed.

2. Select the subnet to change.

   The [Change Admin LAN Subnet] dialog is displayed.

3. In the [Change Admin LAN Subnet] dialog, set the following items.

   Subnet name

   Enter a character string beginning with an alphabetic character and containing up to 16 alphanumeric characters, underscores ("_"), hyphens ("-"), and periods (".").

   Network address

   Enter valid values for the network address.

   Subnet mask

   Enter valid values for the subnet mask.

   Gateway

   Enter the settings for the gateway used for communication with the admin server on the admin LAN.

4. Click <Change>.

5. Click <OK>.

📗 Note
....
When changing the information for a subnet other than the one the admin server belongs to, if there is even 1 managed server belonging to the target subnet, the "Network address" and "Subnet mask" cannot be changed.
When changing the "Network address" or "Subnet mask", refer to the "Modification Procedure when there Are Managed Servers Belonging to Different Subnets".
....

Modification Procedure when there Are Managed Servers Belonging to Different Subnets

When there are managed servers in the target subnet, change the network address or the subnet mask using the following procedure.

1. Register the subnet information using the new network address or subnet mask.

2. Use the following procedure to change the admin LAN IP addresses of all managed servers belonging to the subnet before modification.
   For details on how to configure these settings, refer to "9.1.3 Changing Admin IP Addresses".

3. Delete the subnet used before modification.

9.1.12 Changing WWN Settings for ETERNUS SF Storage Cruiser Integration

This section explains how to change WWN settings for integration with ETERNUS SF Storage Cruiser.

The WWN settings for ETERNUS SF Storage Cruiser integration can be changed by reconfiguring them.
Refer to "10.1 Configuring WWN Settings for ETERNUS SF Storage Cruiser Integration" for details on how to configure these settings.

9.1.13 Changing Target Disks of Image Operations

This section explains how to modify the target disks of image operations.

When there is a server using local boot with a SAN data configuration, use the following procedure to change the target disk for image operations.

1. When the managed server is registered as an agent, place the server into maintenance mode.

   For details on the maintenance mode, refer to "Appendix C Maintenance Mode".

2. Power off the managed server.

3. Execute the following command to update the disk information.

   Acquire the information of disks for which image operations can be performed. At this time, the managed server can be automatically started and then automatically stopped after the disk information is acquired.

   [Windows Manager]

   > *Installation_folder***SVROR\Manager\bin\rcxadm server collect -name** *physical server* **-disk** <RETURN>

   [Linux Manager]

   #/opt/FJSVrcvmr/bin/rcxadm server collect -name *physical server* **-disk** <RETURN>

4. Execute the following command to display the information of disks for which image operations can be performed.

   [Windows Manager]

   > *Installation_folder***SVROR\Manager\bin\rcxadm server show -name** *physical server* **-disk** <RETURN>

   [Linux Manager]

> **#/opt/FJSVrcvmr/bin/rcxadm server show -name** *physical server* **-disk** <RETURN>

Identify the boot disk from the information regarding size or partitions in the displayed disk information.

5. Execute the following command to configure the target disks of image operations.

    Specify the *integer* displayed as "Disk Number: *integer*" in the boot disk information for the option of the command.

    [Windows Manager]

> **>***Installation_folder***\SVROR\Manager\bin\rcxadm server set -name** *physical server* **-attr target_disk=***target_disk*
> <RETURN>

    [Linux Manager]

> **#/opt/FJSVrcvmr/bin/rcxadm server set -name** *physical server* **-attr target_disk=***target_disk* <RETURN>

6. Execute the following command to check the configured target disks of image operations.

    [Windows Manager]

> **>***Installation_folder***\SVROR\Manager\bin\rcxadm server list -target_disk** <RETURN>

    [Linux Manager]

> **#/opt/FJSVrcvmr/bin/rcxadm server list -target_disk** <RETURN>

Information

If the following commands are executed, the configurations of the target disks of image operations can be released.

[Windows Manager]

> **>***Installation_folder***\SVROR\Manager\bin\rcxadm server unset -name** *physical server* **-target_disk** <RETURN>

[Linux Manager]

> **#/opt/FJSVrcvmr/bin/rcxadm server unset -name** *physical server* **-target_disk** <RETURN>

For details on the command, refer to "3.2 rcxadm server" in the "Reference Guide (Command) VE".

Note

- Configurations of target disks of image operations are not updated unless commands are executed. Therefore, when a backup of an admin server is restored, configurations of target disks of image operations are returned to the state when the backup was taken.

- It is recommended to collect backups of admin servers after configuring the target disks of image operations for all physical servers which require the configuration.

- In the following cases, update the disk information, and configure the target disks of image operations again.

    - When restoring a backup of an admin server that was acquired before configuration of target disks of image operations

    - When modifying target disks of image operations after a backup of the admin server has been collected

    - When replacing disks configured as the target disks of image operations

9.2 Changing Settings for the HBA address rename Setup Service

This section explains how to change settings for the HBA address rename setup service. Such settings include the admin server IP address, the port used to communicate with the admin server, and the IP address of the HBA address rename server.

9.2.1 Changing the IP Address of the Admin Server

This section explains how to change the IP address of the admin server.

When this setting is changed, the HBA address rename setup service automatically checks whether it can communicate with the new admin server IP address.
Changing this setting also requires changing the port on the admin server side beforehand.

Change the IP address of the admin server according to "9.1.3 Changing Admin IP Addresses", and change the admin IP address for the HBA address rename setup service according to step 12.

9.2.2 Changing the Port Number Used to Communicate with the Admin Server

This section explains how to change the port used between the HBA address rename setup service and the admin server.

The HBA address rename setup service uses the "rcxweb" port to communicate with the admin server.

When this setting is changed, the HBA address rename setup service automatically checks whether it can communicate with the new admin server IP address.

Changing this setting also requires changing the port on the admin server side beforehand.

Use the following procedure to change the port numbers used to communicate with the admin server:

1. Change the port number of the manager.

   Change the "rcxweb" port number according to the instructions given in "8.2 Changing Port Numbers".

2. Change the port number of the HBA address rename setup service.

   Refer to "Chapter 6 Settings for the HBA address rename Setup Service" in the "Setup Guide VE", and change the port to the same port number.

9.2.3 Changing the IP Address of the HBA address rename Server

This section explains how to change the IP address of the HBA address rename server.

Use the following procedure to change the IP address of the HBA address rename server.

1. Log in to the HBA address rename server with administrator authority.

2. Stop the HBA address rename setup service.

   Stop the HBA address rename setup service according to "Chapter 6 Settings for the HBA address rename Setup Service" in the "Setup Guide VE".

3. Change the IP address set within the operating system.

   Change the IP address according to the OS manual.

4. Restart the HBA address rename setup service.

   Start the HBA address rename setup service according to "Chapter 6 Settings for the HBA address rename Setup Service" in the "Setup Guide VE".

9.3 Changing VIOM Registration Settings

Use the following procedure to perform setting changes for management software (VIOM).

1. In the ROR console management software tree, right-click the management software (VIOM), and select [Modify]-[Registration Settings] from the popup menu.
The [Modify Management Software(VIOM) Settings] dialog is displayed.

2. Perform the following settings:

   User ID

   Enter the ID of a VIOM user account.

   Password

   Enter the password of the above VIOM user account.

3. Click <OK>.
To change registered VIOM server profiles, follow the procedure described in "7.1.1 Registering VIOM Server Profiles" to open the Web interface of ServerView Virtual-IO Manager and change the settings. Changes made inside Virtual-IO Manager are automatically reflected in Resource Orchestrator.

9.4 Changing LAN Switch Settings

This section explains how to change LAN switch settings.

9.4.1 Changing LAN Switch Basic Settings

This section explains how to change LAN switch blade or LAN switch basic settings.

The following settings can be changed.

- LAN switch name (node name for management purposes)

- Admin port (LAN switch blade PY CB Eth Switch 10/40Gb 18/8+2 only)

- Admin LAN (IP address)

- User ID (LAN switch blade only)

- Password (LAN switch blade only)

- Privileged password (LAN switch blade only)

- Connection method (LAN switch blade only)

- SNMP community name

Note

When changing LAN switch settings as follows due to a configuration change, delete the registered LAN switch blade and register it again.

- For a LAN switch blade PY CB DCB SW 10Gb 18/6+6

  - When changing from VCS to another mode, or vice versa

  - Changing VCS ID or RBridge ID

- For a LAN switch blade PY CB Eth Switch 10/40Gb 18/8+2

  - Changing Fabric ID, Domain ID or Switch ID

For a LAN switch blade PY CB 10Gb FEX Nexus B22, only the LAN switch name can be configured.

Complete the changes to the settings on the target LAN switch blade or LAN switch before performing this procedure.

Use the following procedure to change LAN switch blade or LAN switch settings:

1. In the ROR console server resource tree or network resource device tree, right-click the target LAN switch name and select [Modify]-[Registration Settings] from the popup menu.

   The [Modify LAN Switch] dialog is displayed.

2. Make changes to the values as needed.

3. Click <OK>.

   The settings for the LAN switch are changed with the entered information.

📝 Note
. . . .

- It is possible to set the IP address of the target LAN switch to another unregistered LAN switch. However, this will result in the Resource Orchestrator configuration being inconsistent with the actual network configuration.
  If the IP address of the target LAN switch is unintentionally set to the same address as that of another device, change back the IP address of the target LAN switch to its original value according to the instructions given in this section.
  If there are more than one LAN switch with inconsistent IP address configurations, delete all registered LAN switches according to "11.4.2 Deleting LAN Switches " first, then perform discovery and registration again according to "7.10 Registering LAN Switches".

- SSH connection (SSH version 2) can be selected for the following LAN switch blades.

    - LAN switch blade PY CB Eth Switch/IBP 10Gb 18/8 (1.00 or later version)

    - LAN switch blade PY CB Eth Switch 10/40Gb 18/8+2 (1.00 or later version)

    - LAN switch blade PY CB Eth Switch/IBP 1Gb 36/8+2 (4.16 or later version)

    - LAN switch blade PY CB Eth Switch/IBP 1Gb 36/12 (3.12 or later version)

    - LAN switch blade PY CB Eth Switch/IBP 1Gb 18/6 (3.12 or later version)

    - LAN switch blade PY CB DCB SW 10Gb 18/6/6 (2.1.1_fuj or later version)

. . . .

9.4.2 Changing VLANs Set for External Ports of LAN Switch Blades

VLAN IDs and types (Port/Tagged VLAN) set on the external ports of a managed LAN switch blade can be changed.

📝 Note
. . . .

- VLANs cannot be changed on PRIMERGY BX900/BX400 LAN switch blades operating in IBP mode or Converged Fabric mode.

- VLANs cannot be configured on PY CB 10Gb FEX Nexus B22 LAN switch blades.

- If the port VLAN ID is unspecified or 1, a tagged VLAN ID cannot be set to 1.

- When using end host mode for the following LAN switch blades, it is not possible to modify the port VLAN ID, or remove a tag vlan for the external ports which meet the following conditions.

  When performing the operation, inactivate the target external port, or change the VLAN ID for internal ports which have the same VLAN ID as the target external port.

  LAN switch blade

    - PY CB Eth Switch/IBP 1Gb 36/8+2

    - PY CB Eth Switch/IBP 1Gb 36/12

    - PY CB Eth Switch/IBP 1Gb 18/6

  Conditions

    - The port is selected as Selected Port

    - The port is activated

- More than one internal port has the same VLAN.

....

Changing VLAN IDs

This section explains how to change VLAN IDs set on the external ports of a LAN switch.

- With Port VLANs

  Use the following procedure to change VLAN IDs:

  1. In the ROR console server resource tree, right-click the target LAN switch blade and select [Modify]-[Network Settings] from the popup menu.

     The [VLAN Settings] dialog is displayed.

  2. Perform the following settings:

     VLAN

       Select "Change" and select the VLAN ID that has been changed.

     Physical Port, Link Aggregation

       Select [Untagged] from the VLAN type of the port number to configure or link aggregation group name.

  3. Click <OK>.

     The VLAN ID is changed.

- With Tagged VLANs

  First delete the VLAN ID was set on the desired LAN switch blade port before setting the new VLAN ID.

  Use the following procedure to change VLAN IDs:

  1. In the ROR console server resource tree, right-click the target LAN switch blade and select [Modify]-[Network Settings] from the popup menu.

     The [VLAN Settings] dialog is displayed.

  2. Perform the following settings:

     VLAN

       Select "Change" and select the VLAN ID that has been changed.

     Physical Port, Link Aggregation

       Select [None] from the VLAN type of the port number to configure or link aggregation group name.

  3. Click <OK>.

     The VLAN ID set for the selected LAN switch blade port is released.

  4. Repeat step 1 and set the new VLAN ID in the [VLAN Settings] dialog.

     VLAN

       Select "Create new" or "Change" in the VLAN information and select the VLAN ID to be changed.

     Physical Port, Link Aggregation

       Select [Tagged] from the VLAN type of the port number to configure or link aggregation group name.

  5. Click <OK>.

     The VLAN ID is changed.

Changing VLAN Types

This section explains how to change the types of VLAN (port or tagged VLAN) set on the external ports of a LAN switch.

Use the following procedure to change VLAN types:

1. In the ROR console server resource tree, right-click the target LAN switch blade and select [Modify]-[Network Settings] from the popup menu.

   The [VLAN Settings] dialog is displayed.

2. Perform the following settings:

   VLAN

   Select "Change" and select the VLAN ID that has been changed.

   Physical Port, Link Aggregation

   Change the VLAN type (Untagged] or [Tagged]) of the port number to configure or link aggregation group name.

3. Click <OK>.

   The VLAN type is changed.

Deleting VLAN IDs

This section explains how to delete VLAN IDs.

- Deleting VLAN IDs from LAN switch blades

  Use the following procedure to delete VLAN IDs:

  1. In the ROR console server resource tree, right-click the target LAN switch blade and select [Modify]-[Network Settings] from the popup menu.

     The [VLAN Settings] dialog is displayed.

  2. Perform the following settings:

     VLAN

     Select "Change" and select the VLAN ID that has been changed.

  3. Click <Delete>.

     The VLAN ID is deleted.

- Deleting VLAN IDs from LAN switch ports

  Use the following procedure to delete VLAN IDs:

  1. In the ROR console server resource tree, right-click the target LAN switch blade and select [Modify]-[Network Settings] from the popup menu.

     The [VLAN Settings] dialog is displayed.

  2. Perform the following settings:

     VLAN

     Select "Change" and select the VLAN ID that has been changed.

     Physical Port, Link Aggregation

     Select [None] from the VLAN type of the port number to delete VLANs or link aggregation group name.

  3. Click <OK>.

     The VLAN ID is deleted.

9.4.3 Re-discovering LAN Switches

Newly added LAN switches can be discovered by re-executing LAN switch discovery.
For details on LAN switch discovery, refer to "Discovery" in "7.10 Registering LAN Switches".

9.5 Changing VM Management Software Settings

This section explains how to change VM management software settings.

The following settings can be changed.

- Location

- IP address

- User ID

- Password

Here the method for changing settings registered with Resource Orchestrator is explained.

Complete reconfiguration within the VM management software admin console before performing this procedure.

Use the following procedure to change VM management software settings:

1. In the ROR console management software tree, right-click the target management software, and select [Modify]-[Registration Settings] from the popup menu.

   The [Modify Management Software(*name*) Settings] dialog is displayed.
   The name of the selected VM management software is displayed in *name*.

2. Enter the following items:

   Location

   Select the location of the VM management software registration to change.

   - If VM management software is installed on the admin server

     Select [Admin Server].

   - In other cases

     Select [Other Server].

   IP address

   If [Other Server] was selected, enter the IP address of the server on which VM management software is installed.

   User ID

   Enter the user ID to use to control VM management software.

   Password

   Enter the password for VM management software.

3. Click <OK>.

   VM management software settings are changed.

9.6 Changing Power Monitoring Environment Settings

This section explains how to change power monitoring environment settings.

Power environment settings include environmental data settings, collection cancel settings, and power monitoring device settings.

9.6.1 Changing Environmental Data Settings

Use the following procedure to change environmental data settings:

1. Select [Tools]-[Options] from the ROR console menu.

   The [Options] dialog is displayed.

2. Click the [Environmental Data] category title, and input the following items in the displayed area.

Data to collect

Select the [Power] checkbox to start collecting power consumption data.

Polling interval (in minutes)

Enter the time interval of the data collection (1-6 or 10).
The number of devices that can be monitored simultaneously depends on the value of this polling interval and the load put on the admin server. The following values are guidelines.

Table 9.1 Polling Interval

Polling Interval	Number of Devices that can be Monitored Simultaneously
5 minutes	Up to 40 devices
10 minutes	Up to 60 devices

Use a polling interval of 5 minutes or longer when monitoring chassis and servers. Use a polling interval of 10 minutes if monitoring more than 40 devices.

Data storage period

Enter storage periods for each collection rate. Data older than the configured storage period will be deleted every day.
Enlarging data storage periods reduces the number of devices that can be monitored simultaneously.
Use the default storage period values when monitoring chassis and servers.

3. Click <Apply>.

The new settings are applied.

🈁 **Note**

. . . .

If the [Power] checkbox under [Data to collect] is cleared, the collection of power consumption data (including the calculation of hourly, daily, and other summarized data) will not be performed anymore.

. . . .

9.6.2 Canceling Collection Settings for Power Monitoring Environments

This section explains how to cancel the collection of power consumption data.

Use the following procedure to cancel the collection of power consumption data.

1. Select [Tools]-[Options] from the ROR console menu.

The [Options] dialog is displayed.

2. Click the [Environmental Data] category title, and modify the values for the following items in the displayed area.

Data to collect

Clear the [Power] checkbox.

3. Click <Apply>.

Collection of environmental data is canceled.

9.6.3 Changing Power Monitoring Devices

This section explains how to change power monitoring device settings.

The following settings can be changed.

- Device name

- Admin LAN (IP address)

- SNMP community name

- Voltage

- Comment

Complete setting modifications on the actual power monitoring device before performing this procedure.

Use the following procedure to change power monitoring device settings:

1. From the ROR console, right-click the power monitoring device tree, then select [Modify]-[Registration Settings] from the popup menu.

   The [Modify Power Monitoring Device] dialog is displayed.

2. Make changes to the values as needed.

3. Click <OK>.

   The power monitoring device settings will be changed with the entered information.

9.7 Changing Monitoring Information Settings

This section explains how to change and cancel monitoring information settings.

9.7.1 Changing Monitoring Information Settings

This section explains how to change monitoring information settings.

The following settings can be changed.

- Enabling or disabling of ping monitoring

- Time-out

- Recovery method

- Number of reboots

Use the following procedure to change settings:

1. In the ROR console server resource tree, right-click the target physical OS and the VM hosts, and select [Modify]-[Monitoring Settings] from the popup menu.

   The [Configuring monitoring settings] dialog is displayed.

2. Make changes to the values as needed.

3. Click <OK>.

   The settings for the monitoring information are changed to the entered settings.

9.7.2 Canceling Monitoring Information Settings

This section explains how to cancel monitoring information settings.

Use the following procedure to cancel the monitoring information settings:

1. In the ROR console server resource tree, right-click the target physical OS and the VM hosts, and select [Modify]-[Monitoring Settings] from the popup menu.
   The [Configuring monitoring settings] dialog is displayed.

2. Uncheck the [Enable ping monitoring] checkbox.

3. Click <OK>.
   The settings for the monitoring information are canceled.

9.8 Changing Storage

This section explains how to change storage settings.

9.8.1 Changing Storage Management Software Basic Information

This section explains how to change the basic settings of storage management software.

The following settings can be changed.

- Label

- Comment

Use the following procedure to change the basic settings of storage management software:

1. In the ROR console storage tree, right-click the target storage management software, and select [Modify]-[Registration Settings] from the displayed menu.

   The [Resource Change Setting] dialog is displayed.

2. Modify the values for the following items:

   Label

       Enter up to 32 alphanumeric characters or symbols.

   Comment

       Enter up to 256 alphanumeric characters or symbols.

3. Click <OK>.

   Basic information for the storage management software is modified.

9.8.2 Changing Storage Unit Basic Information

This section explains how to change the basic information of storage units.

The following settings can be changed.

- Label

- Comment

Use the following procedure to change the basic information of storage units:

1. In the ROR console storage tree, right-click the target storage unit, and select [Modify]-[Registration Settings] from the displayed menu.

   The [Resource Change Setting] dialog is displayed.

2. Modify the values for the following items:

   Label

       Enter up to 32 alphanumeric characters or symbols.

   Comment

       Enter up to 256 alphanumeric characters or symbols.

3. Click <OK>.

   Basic information for the storage unit is modified.

9.8.3 Changing Virtual Storage Resource Basic Information

This section explains how to change the basic settings of virtual storage resources.

The following settings can be changed.

- Label

- Comment

Use the following procedure to modify the basic information for virtual storage resources:

1. In the ROR console storage tree, right-click the target virtual storage resource, and select [Modify]-[Registration Settings] from the popup menu.

   The [Resource Change Setting] dialog is displayed.

2. Modify the values for the following items:

   Label

   > Enter up to 32 alphanumeric characters or symbols.

   Comment

   > Enter up to 256 alphanumeric characters or symbols.

3. Click <OK>.

   The basic information of the virtual storage resource is modified.

9.8.4 Changing Disk Resource Basic Information

This section explains how to modify the basic information for disk resources.

The following settings can be changed.

- Label

- Comment

Use the following procedure to modify the basic information for disk resources

1. Select the target virtual storage in the ROR console storage tree.

   The disk resource list is displayed in the [Resource List] tab.

2. From the disk resource list, right-click the target disk resource, and select [Modify]-[Registration Settings] from the displayed menu.

   The [Resource Change Setting] dialog is displayed.

3. Modify the values for the following items:

   Label

   > Enter up to 32 alphanumeric characters or symbols.

   Comment

   > Enter up to 256 alphanumeric characters or symbols.

4. Click <OK>.

   The basic information for disk resources is modified.

9.9 Server Role Modification

Here is the description of server role modification.

9.9.1 Server Role Modification

Here is the description of server role setting modification.

Set the server role of the VM guest, which the ROR manger is running on, to "Manager".
The following operations or functions which might stop the ROR manager unintentionally are prevented.

- Operations of the VM guest which the ROR manger is running on:

  - Power operations

  - VM guest migration

    Migrating to a VM host registered in the server pool is not allowed.

- Operation of VMhost that VMguest operating ROR Manger is Running

  - Power operations

  - Backup restore

  - Server switchover(*1)

  - ping monitor (*2)

  - HBA address rename setting

  - Serve deletion(when HBA address rename is been used)

 *1: Auto-Recovery is not triggered. It will be excepted from the switch target in the spare server.
 *2: The setting was completed but recovery cannot be triggered.

For VM guests with the "Manager" server role, "[Manager]" is displayed after the name in the resource tree.

Modify the settings according to the following manual.

1. On the ROR console's server resource tree,right click the object's VMguest, and select [Modify settings]-[Server role] on the displaying menu.

2. Change radio button to "Manager".

3. Click the <OK>button.

   The settings of server role has been changed.

Or, modify the setting from menu bar according to the following manual.

1. On the ROR console's server resource tree, check the object's VMguest, and select the [Settings]-[Modify settings]-[Server role] on the menu bar.

2. Change radio button to "Manager".

3. Click the <OK>button.

   The settings of server role has been changed.

Note

It should make a note for the server of VM host which server role is set avoid all of the servers are powered off suddenly by blackouts. After the blackout restoration, start the server of VM host which server role is set, and then it can start other servers on ROR.

9.9.2 Cancel Settings of the Server Role

Here is the description of cancelling the setting of the server role.

Cancel the settings according to the following manual.

1. On the ROR console's server resource tree,right click the object's VMguest, and select [Modify settings]-[Server role] on the displaying menu.

2. Change radio button to "none".

3. Click the <OK>button.

   The settings of server role has been changed.

Or, modify the setting from menu bar according to the following manual.

1. On the ROR console's server resource tree, check the object's VMguest, and select the [Settings]-[Modify settings]-[Server role] on the menu bar.

2. Change radio button to "none".

3. Click the <OK>button.

   The settings of server role has been changed.

Chapter 10 Configuring the Operating Environments of Managed Servers

This chapter explains how to install software to the registered managed servers and set up their operating environment.

Figure 10.1 Procedure for Setting up Operating Environments (for Blade Servers and Rack Mount Servers)
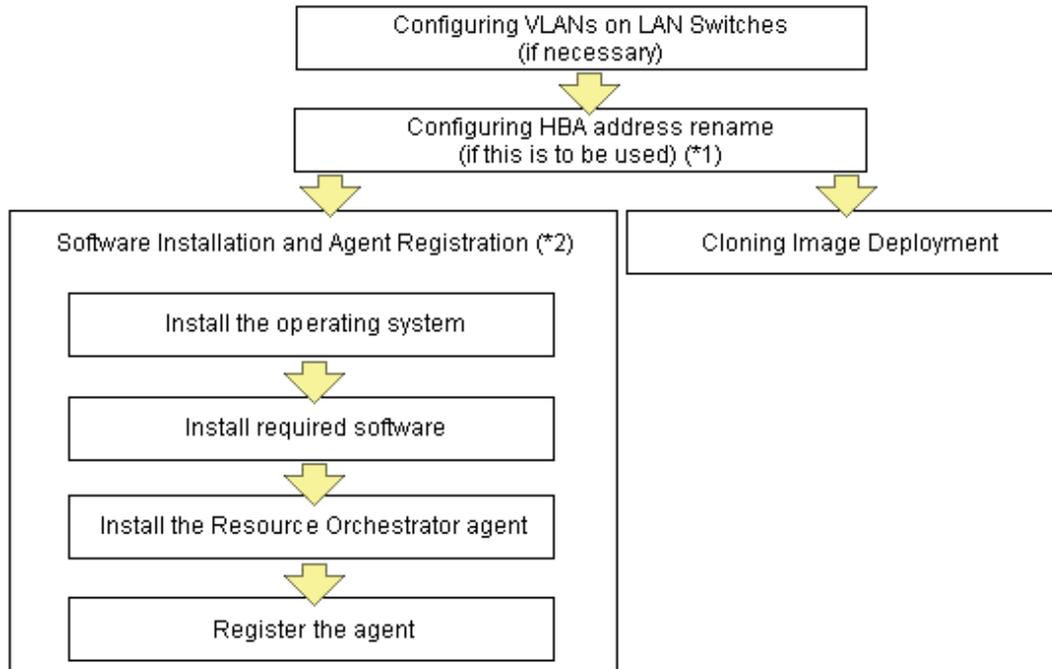
*1: HBA address rename and VIOM cannot be used together within the same chassis. I/O virtualization settings for all the servers mounted in one chassis must be made using either HBA address rename or VIOM.
*2: These settings can be omitted for resources that have already been installed or registered.

Figure 10.2 Procedure for Setting up Operating Environments (for Fujitsu M10/Enterprise)
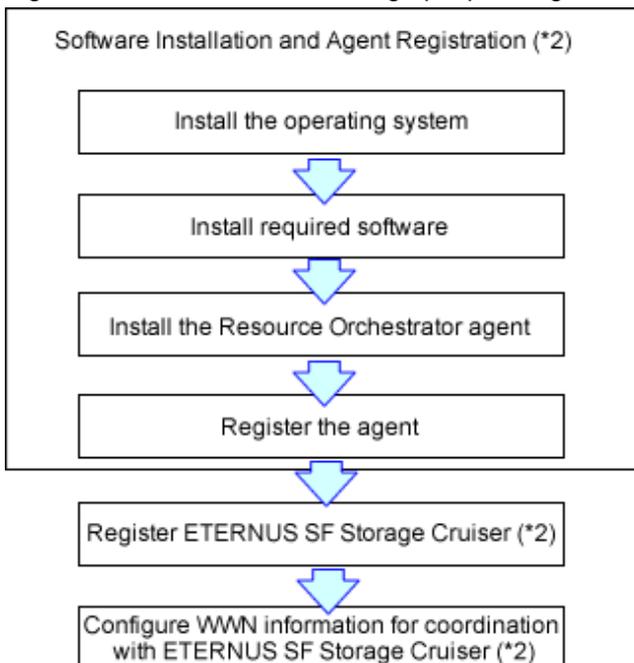
*1: These settings can be omitted for resources that have already been installed or registered.
*2: Necessary when performing server switchover using the storage affinity method.

- Configuring VLANs on LAN Switch Blades

    Refer to "7.3.4 Configuring VLANs on LAN Switch Blades".

- HBA address rename Settings

    Refer to "7.4.2 HBA address rename Settings".

- Installing Software and Registering Agents

    Refer to "Chapter 7 Installing Software and Registering Agents on Managed Servers" in the "Setup Guide VE".

- Deploying Cloning Images

    Refer to "Chapter 17 Cloning [Physical Servers]".

- Registering ETERNUS SF Storage Cruiser

    Refer to "5.13 rcxadm storagemgr" in the "Reference Guide (Command) VE".

- Configuring WWN Settings for ETERNUS SF Storage Cruiser Integration

    Refer to "10.1 Configuring WWN Settings for ETERNUS SF Storage Cruiser Integration".

10.1 Configuring WWN Settings for ETERNUS SF Storage Cruiser Integration

This section explains how to configure WWN settings for integration with ETERNUS SF Storage Cruiser.
Specifying HBA WWNs, storage WWNs, and AffinityGroup for ETERNUS SE Storage Cruiser enables configuration of the zoning settings of Fibre Channel switches and storage unit host affinity. When performing switchover on managed servers, using the WWN settings enables the admin server to automatically change settings of storage devices.
Use of this function requires registration of specific settings for ETERNUS SF Storage Cruiser in advance. Fibre Channel Switches and storage units connected to managed servers must be registered on ESC.

Note

- WWN settings for servers and HBAs are not performed by this function.

- Configuration cannot be performed for managed servers which are configured as spare servers or are used as spare servers. Therefore, perform this configuration before configuring spare servers.

Use the following procedure to configure the WWN settings.

When changing the current WWN information, configure the new WWN information after deleting Fibre Channel Switch zoning and storage unit host affinity in the currently configured WWN information.

1. In the ROR console server resource tree, right-click the target physical server, and select [Modify]-[WWN Settings] from the popup menu.
   The [WWN Settings] dialog is displayed.

2. Perform the following settings:

   HBA ports

       Select the following values according to the system configuration.

       - Procedures for Single-path Configurations

           Specify "1" for HBA ports.

- Procedures for Multi-path Configurations

Select the number of multi-paths for HBA ports.
However, it is necessary to select "1" during installation of the operating system. Select the number of paths and reconfigure HBA address rename settings after setting up the multi-path driver.

[OVM for SPARC]
While using an IO domain in OVM for SPARC environment, select the HBA port number of control domain and IO domain in HBA Port Number. But, when disks are shared in primary server and spare server, please do not contain the HBA port number used in sharing disks.

Port*n* WWPN

Enter or select the WWPN of an HBA collected from physical servers.
When using a multi-path configuration, enter the values of the HBAs and the corresponding CAs of servers in the same order, based on the values in "6.1.6 Settings when Switching Over Fujitsu M10/SPARC Enterprise Servers" in the "Design Guide VE".

When disks are shared in primary server and spare server, please do not enter in the HBA port used in sharing disks.

Target CA

Select WWPNs of storage CA and AffinityGroup.
Select hyphens ("-") to keep spare servers inactive.
Also, select a hyphen ("-") when deleting Fibre Channel Switch zoning and storage unit host affinity in the configured WWN information.

When using a server on which an agent is registered as a spare server, the server must meet all of the following conditions:

- When the WWPN of the target CA is the same value as that of the primary server

- When the AffinityGroup value is different from the value of the primary server

- When agents are not registered on ETERNUS SF Storage Cruiser

 Note

When using the storage affinity switchover method, if a hyphen ("-") is selected, the storage path settings will be deleted.

3. Click <OK>.

Perform configuration or deletion of Fibre Channel Switch zoning and storage unit host affinity based on the configured WWN information. When the target operation server is registered on ESC, the status should be as below:

- Configuration

The server should be turned on

- Deletion

The server should be turned off

When configuration and deletion of Fibre Channel Switch zoning and storage unit host affinity have been already executed, no operations will be performed on the devices.

 Note

- For WWPN value specification, check that the value does not overlap with the WWPN used for HBA address rename or VIOM. If the same WWPN is used, there is a chance data on storage units will be damaged.

- When configuration or deletion of Fibre Channel switches or storage units performed, a warning dialog is displayed. Make sure that there are no problems in the settings, then click <OK>.

- If the target CA is not displayed, confirm the status of the following settings:

- ESC is correctly registered on Resource Orchestrator.

- Fibre Channel switches and storage units are correctly registered.

- Only one access path is configured on ESC for each CA of an HBA.

10.2 Deploying Cloning Images

For the second and subsequent servers, operating systems are created using the cloning image collected from the first server.

For details on cloning, refer to "Chapter 17 Cloning [Physical Servers]".

Chapter 11 Deleting Resources

This chapter explains how to delete resources.

It is possible to register and delete a managed server and LAN switch as a single resource when they are in the same chassis.

Note that operation of a server cannot be performed while the LAN switch is being registered or removed.

If the operation is performed simultaneously for multiple resources, one of the following messages is displayed.

In this case, wait until the current operation is completed before executing the desired operation again.

```
FJSVrcx:ERROR:67210: LAN_switch_name(LAN switch):is busy
```

or

```
FJSVrcx:ERROR:67210: Managed_server_name (physical server):is busy
```

11.1 Deleting Chassis

This section explains how to delete chassis.

Use the following procedure to delete the chassis.

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

   The [Delete Resource] dialog is displayed.

2. Click <OK>.

   The target chassis is deleted from the server resource tree.

🔷 Note

・・・

If server blades and partitions within the chassis were already registered, delete these server blades and partitions before deleting the chassis.
If LAN switches have been registered, delete all LAN switches before deleting the chassis.

・・・

11.2 Deleting Managed Servers

This section explains how to delete managed servers.

Use the following procedure to delete managed servers.

1. In the ROR console server resource tree, right-click the target server (or the physical OS or the VM host on the server) and select [Delete] from the popup menu.

   The [Delete Resource] dialog is displayed.

   If a VM host is running on the server to be deleted, any VM guests running on that host are also deleted from the server resource tree at the same time. The VM guests to be deleted appear in the [Delete Resource] dialog, so check that it is safe to delete them.

2. Click <OK>.

   - If a physical OS or VM host exists on the target server and HBA address rename is set

     The server will be powered off and the target server will be unregistered when the resource is deleted. Resource Orchestrator does not delete the host affinity settings of storage units or the zoning settings of Fibre Channel switches.

   - If WWN information is set for the target server

     The host affinity settings of storage units and the zoning settings of Fibre Channel switches will be deleted when the Fujitsu M10/SPARC Enterprise is deleted.

   - If the deleted server is a PRIMERGY BX series, a PRIMEQUEST, a SPARC Enterprise M4000/M5000/M8000/M9000, or a SPARC M10-4S

     The target server will be unregistered and remain in the server resource tree.

Information

- If HBA address rename has already been set up on the managed server, the HBA WWN is reset to the factory default.
  When this occurs, the managed server is turned on temporarily, after the power is forcibly turned off once.
  When the operating system is running on a managed server, it is recommended to shut it down before deleting the server.
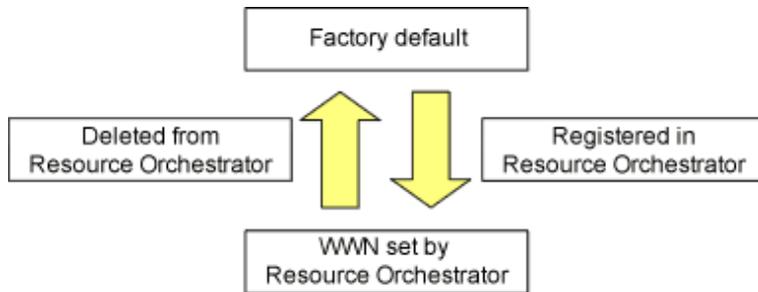
- VM guests can be deleted using the management console of the server virtualization software used. Doing so will automatically delete those VM guests from Resource Orchestrator as well.

- If the same storage device volume is to be used to operate the target server after the server has been deleted, use storage management software such as ETERNUS SF Storage Cruiser to reset the storage host affinity and fibre channel switch zoning with the factory default WWN.

- Any system images backed up from the target server are also deleted automatically.

- After the server has been deleted, the maintenance LED is switched OFF automatically.

- Deleting a server on which both the HBA address rename function and a VM high-availability feature (provided by the server virtualization software used) are enabled will produce the following behavior. The server will be powered off, causing the high-availability feature to trigger its VM recovery process. To avoid interruption of hosted applications during server deletion, it is recommended to move VM guests to another server beforehand. For more details on the high-availability features available for each server virtualization software, refer to "D.2 Configuration Requirements" in the "Design Guide VE".

- When a managed PRIMEQUEST 2000 series server is deleted, the result varies depending on the partition status, as follows:

  - When an Extended Partition configured on a PPAR with Extended Partitioning Mode set to "Disable" or on a PPAR partition with Extended Partitioning Mode set to "Enable" is deleted

    The target server will remain unregistered in the resource tree.

  - When an Extended Partition configured on a PPAR with Extended Partitioning Mode set to "Enable" or on a PPAR partition with Extended Partitioning Mode set to "Disable" is deleted

    The target server disappears from the server resource tree.

- Settings for target disks of image operations are also deleted. To re-register the server that was deleted, configure the target disks of image operations if necessary.

11.3 Canceling VIOM Integration

This section explains how to cancel VIOM integration.

Use the following procedure to cancel VIOM integration:

1. In the ROR console management software tree, right-click the target management software (VIOM), and select [Delete] from the popup menu.
   The [Delete Resource] dialog is displayed.

2. Click <OK>.
   The target management software (VIOM) is deleted.

To delete registered VIOM server profiles, follow the procedure described in "7.1.1 Registering VIOM Server Profiles" to open the Web interface of ServerView Virtual-IO Manager and delete the desired profiles from there.

> **⚠ Note**
> ⋅⋅⋅
>
> Integration with VIOM cannot be canceled in the following cases.
>
> - When there are spare server settings involving the VIOM server profile exchange method
>
> - When there are servers using the VIOM server profile exchange method that are in the following states
>
>   - Being switched over
>
>   - Have been switched over (prior to failback)
>
>   - Being failed back
>
> - Server blades that are managed using VIOM, and are currently the target of operations by Resource Orchestrator (power control, image-related processes, etc.)
>
> When using VIOM coordination as I/O virtualization with rack mount servers, if VIOM server profiles are left assigned when VIOM coordination is deleted, the MAC addresses on the target rack mount servers remain with I/O virtualization.
> When using rack mount servers, VIOM server profiles need to be unassigned before deleting VIOM coordination.
> ⋅⋅⋅

11.4 Deleting LAN Switches

This section explains how to delete LAN switches.
Based on the LAN switch registration method used, there are two methods for LAN switch deletion.

- Deleting LAN Switch Blades

- Deleting LAN Switches

11.4.1 Deleting LAN Switch Blades

This section explains how to delete LAN switch blades.

Use the following procedure to delete LAN switch blades.

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

   The [Delete Resource] dialog is displayed.

2. Click <OK>.

   The target LAN switch blade is unregistered.

11.4.2 Deleting LAN Switches

This section explains how to delete LAN switches.

Use the following procedure to delete LAN switches.

1. In the ROR console network resource tree, right-click the target LAN switch and select [Delete] from the popup menu.

   The [Delete Resource] dialog is displayed.

2. Click <OK>.

   The target LAN switch is deleted from the network resource tree.

11.5 Deleting VM Management Software

This section explains how to delete VM management software.

Use the following procedure to delete VM management software.

1. In the ROR console management software tree, right-click the target management software, and select [Delete] from the popup menu.

   The [Delete Resource] dialog is displayed.

2. Click <OK>.

   The target management software is deleted.

11.6 Clearing the Power Monitoring Environment

This section explains how to clear the power monitoring environment.

Clearing the power monitoring environment is done by deleting power monitoring targets.
For details on how to release collection settings, refer to "9.6.2 Canceling Collection Settings for Power Monitoring Environments".

11.6.1 Deleting Power Monitoring Devices

This section explains how to delete power monitoring devices.

Use the following procedure to delete power monitoring devices:

1. In the ROR console power monitoring devices tree, right-click the target power monitoring device and select [Delete] from the popup menu.

   The [Delete Resource] dialog is displayed.

2. Click <OK>.

   The target power monitoring devices are deleted from the tree view.

11.7 Deleting Admin LAN Subnets

This section explains how to delete admin LAN subnets.

Use the following procedure to delete an admin LAN subnet.

1. From the ROR console menu, select [Settings]-[Admin LAN Subnet].

   The [Admin LAN Subnet] dialog is displayed.

2. Select the subnet to delete.

3. Click <Delete>.

   The [Delete Admin LAN Subnet] dialog is displayed.

4. Click <OK>.

   The target subnet information is deleted.

Information
. . . .

When an admin LAN subnet is deleted, the simplified DHCP service for Resource Orchestrator will be disabled.

In this case, either use the OS standard DHCP service that was enabled when the admin LAN subnet was registered, or perform re-installation after uninstalling the manager.
. . . .

Note
. . . .

It is not possible to delete the information of subnets which have managed servers registered.

Before deleting subnet information, delete all managed servers that have been registered on the relevant subnet.
. . . .

11.8 Unregistering ETERNUS SF Storage Cruiser

This section explains how to unregister ETERNUS SF Storage Cruiser.

ETERNUS SF Storage Cruiser can be unregistered using the rcxadm storagemgr unregister command.
For details on the rcxadm storagemgr unregister command, refer to "5.13 rcxadm storagemgr" in the "Reference Guide (Command) VE".

11.9 VM Host Unregistration

This section explains unregistration of VM hosts in guest domains on Oracle VM for SPARC.

Use the following procedure to unregister a VM Host.

1. In the ROR console server resource tree, right-click the guest domain which is registered on the VM Host, and select [Unregister] from the popup menu.

   The [VM Host unregistration] dialog is displayed.

2. Click <OK>.

   When VM hosts are unregistered, they are converted back into VM guests.

11.10 Deleting Converged Fabric Management Software

This section explains how to delete Converged Fabric management software.

Use the following procedure to delete Converged Fabric management software.

1. In the ROR console management software tree, right-click the target management software, and select [Delete] from the popup menu.

   The [Delete Resource] dialog is displayed.

2. Click <OK>.

   The target management software is deleted.

Chapter 12 Pre-configuration for Resource Registration and Modification

This chapter provides an overview of the pre-configuration function and explains how to use system configuration files.

12.1 Overview

Using the Pre-configuration function, it is possible to create system definition files that can be later used to setup a Resource Orchestrator environment. Importing system configuration files makes it easy to perform various registration settings in one operation. This prevents the operating mistakes induced by sequences of individual, manual configuration steps.

The pre-configuration function can be used in the following situations.

- New Installation

    From a traditional work office (or another off-site location), define the various parameters required for Resource Orchestrator and record them in a system configuration file. Next, send this definition file to your actual system location (machine room), and import the file into Resource Orchestrator using the import functionality of the ROR console. This single operation automates the registration of all the servers defined in the system configuration file.

- Backing up a System Configuration

    Using the export function of the ROR console, the current Resource Orchestrator configuration can be exported to a system configuration file.

- Batch Reconfiguration

    The registration settings of already registered resources can be modified easily by exporting the current configuration to a system configuration file and editing the desired configuration items before re-importing that configuration file. The actual reconfiguration is then performed as a single import operation.

- Re-use of Existing Configurations

    Once a system has been fully setup, its configuration can be exported and re-used as a basis for the design of other systems. This makes it easy to design various systems located in different sites.

Figure 12.1 Examples of Use
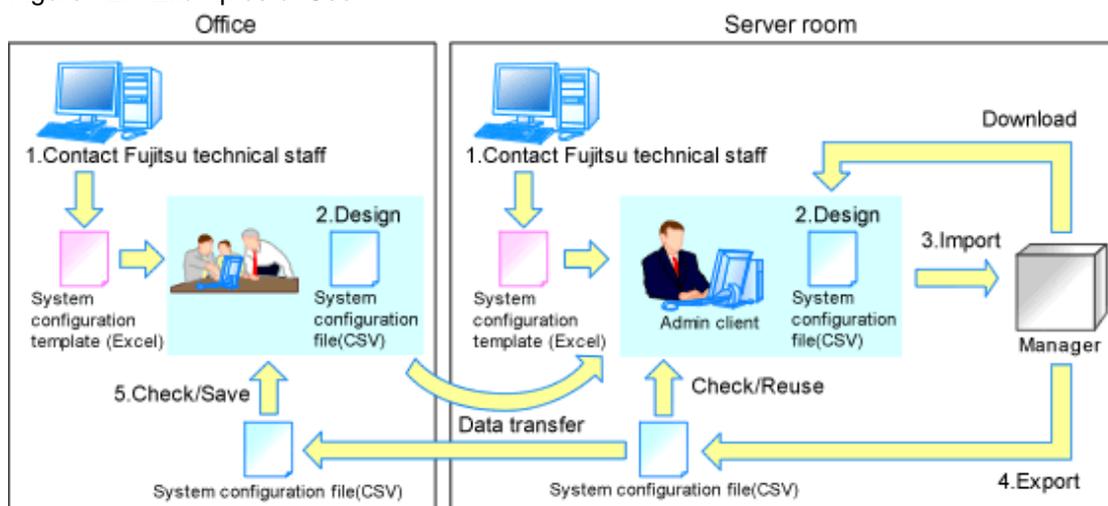
Only system configuration files in CSV format can be imported or exported. For details on the system configuration file's format, refer to "Appendix B Format of CSV System Configuration Files".

Resource Orchestrator provides a sample in CSV format. To obtain a copy of the Excel template (hereinafter system configuration template), contact Fujitsu technical staff. This system configuration template makes it easy to create system configuration files in CSV format.

- When loading a system configuration template from a CSV file, or importing a system configuration file from the ROR console

  Use the format described in "B.2 File Format" for the system configuration file.

- When saving a file in CSV format from the system configuration template, or exporting a system configuration file from the ROR console

  Export will be performed using the latest file format given in "B.2 File Format".

The following operations, usually performed from the ROR console, can be equally performed using the pre-configuration function.

- Registration

  - "7.1 Registering VIOM Coordination"

  - "7.3 When Using Blade Servers"

  - "7.10 Registering LAN Switches"

  - "7.2 Registering VM Management Software"

  - "7.7 Registering Power Monitoring Devices" (*1)

  - "7.8 Registering Admin LAN Subnets"

  - "7.3.4 Configuring VLANs on LAN Switch Blades"

  - "7.4.2 HBA address rename Settings" (*2)

  - "Chapter 8 Configuring Monitoring Information" in the "Setup Guide VE"

  - "Chapter 18 Server Switchover Settings"

- Modification

  - "8.1 Changing Admin IP Addresses" (*3)

  - "9.1.11 Changing Admin LAN Subnets"

  - "9.1.2 Changing Server Names"

  - "9.1.3 Changing Admin IP Addresses" (*3)

  - "9.1.4 Changing SNMP Communities"

  - "9.1.5 Changing Server Management Unit Configuration Settings"

  - "9.1.7 Changing VM Host Login Account Information"

  - "9.1.8 Changing the VLAN Settings of LAN Switch Blades"

  - "9.1.9 Changing HBA address rename Settings" (*2)

  - "9.1.10 Changing Boot Options"

  - "9.3 Changing VIOM Registration Settings"

  - "9.4 Changing LAN Switch Settings"

  - "9.5 Changing VM Management Software Settings"

  - "9.6 Changing Power Monitoring Environment Settings"

  - "9.7 Changing Monitoring Information Settings"

  - "18.3 Changing Server Switchover Settings"

*1: To start collecting environment data, the collection settings should be manually set from the ROR console's option dialog.
*2: Restart all the managed servers that were either registered or modified following an import operation.
*3: The pre-configuration's scope of configuration is the same as that of the ROR console.

Moreover, the pre-configuration function can perform the same labels and comments settings as those available in BladeViewer. Those settings are described in "Chapter 6 BladeViewer" and "6.5.1 Listing and Editing of Labels and Comments".

- The following operations cannot be performed by the pre-configuration function, and should be performed from the ROR console.

    - Deleting registered resources from Resource Orchestrator

    - Changing the name of a registered chassis, physical server (only for servers other than PRIMERGY BX servers) or a power monitoring device

    - Deleting registered admin LAN subnets

    - Discovering, registering, or changing registration settings of a LAN switch

    - Detecting physical link information from a LAN switch

    - Canceling VIOM Integration

    - Registration and deletion of SNMP trap destinations

    - Configuration and change of WWN information using ETERNUS SF Storage Cruiser integration

    - Agent registration of Oracle VM for SPARC guest domains

- The following operations cannot be performed by the pre-configuration function, and should be performed using commands.

    - Registration and deletion of ETERNUS SF Storage Cruiser integration

- Make sure that less than 200 resources are specified for registration or changing in the system configuration file specified for import.

    If it is necessary to specify more than 200 resources for registration or changing, do by importing multiple system configuration files.

- When using ServerView Deployment Manager on the admin LAN, the following settings cannot be defined using the pre-configuration function. For details on co-existence with ServerView Deployment Manager, refer to "Appendix B Co-Existence with ServerView Deployment Manager" in the "Setup Guide VE".

    - Spare server settings (using the backup and restore or HBA address rename method)

    - HBA address rename Settings

12.2 Importing the System Configuration File

This section explains how to import a system configuration definition file (saved in CSV format) from the ROR console.

Use the following procedure to import a system configuration definition file.

1. Prepare a system configuration file in CSV format.

    - System configuration templates in Excel format cannot be directly imported into Resource Orchestrator. Use the template's save to CSV function to produce a system configuration file in CSV format before importing.

    - Only system configuration files conforming to the format described in "B.2 File Format" can be imported. For details on the file format, refer to "Appendix B Format of CSV System Configuration Files".

    - Make sure that less than 200 resources are specified for registration or changing in the system configuration file.

        If it is necessary to specify more than 200 resources for registration or changing, do by importing multiple system configuration files.

    - When changing resources in different sections, perform import of the configuration definition files for each section.

    - When importing system configuration files which begins with "RCXCSV,V1.0" in the first line, the agent cannot automatically be registered. Moreover, the registration fails in cases where a spare server is defined to a VM host in the system configuration file.

2. Open and log in to the ROR console according to "Chapter 1 Login and Logout".

3. In the ROR console, select [File]-[System Configuration File]-[Import] from the menu.

   The [Import System Configuration File] dialog is displayed.

4. Specify a configuration file prepared in step 1.

5. Click <OK>.

   The import process starts. The system configuration file is verified first, and then resources are imported one by one, following the order defined by the system configuration file.

   The processing of resource registration or change is executed after the verification.
   The process status can be checked in the Recent Operations area of the ROR console.
   Clicking <Cancel> in the Recent Operations area displays a confirmation dialog and stops the import process. The <Cancel> button interrupts the import process after completing the current process. Note that the processing performed up to the error point is effective in the system.

P Point
. . . .

- The "SpareServer", "ServerAgent" and "ServerVMHost" sections must meet the conditions below when performing pre-configuration.

   a. Spare server section ("SpareServer")

      In cases where the specified spare server has no operating system installed
      The physical server which is defined as a spare server must not be defined in "ServerWWNN", "ServerAgent", or "ServerVMHost" sections.

      When configuring a server using I/O virtualization as a spare server
      The server must meet one of the following conditions:

      - HBA address rename information must already be configured on the physical server in which a spare server is defined

      - A VIOM server profile must already be configured on the physical server in which a spare server is defined

      In cases where the specified spare server is a VM host
      The physical server which is defined as a spare server must already be registered for the Resource Orchestrator agent.

      When configuring a server with WWN information set using storage affinity switchover as a spare server
      WWN information must already be configured on the primary server and the spare server.

      If the above conditions are not meet, divide the section as different CSV files, and import them one by one.

   b. Agent section ("ServerAgent" or "ServerVMHost")

      To register an agent, it must fulfill all of the following conditions. Please import agents only if they meet all these conditions.

      The agent of Resource Orchestrator must already be installed on the managed server.

      An OS must be running on the managed server.

      The agent of the target physical server must be registered, or the agent registration section defined in the system configuration file.

- In the "Server" section, when registering or changing managed servers in different subnets than the admin server, one of the following conditions must be fulfilled:

   - The target subnet information is registered.

   - The target subnet's information is defined in the "Subnet" section of the CSV format system configuration file.
. . . .

📝 Note

- When registering a new server with the registered primary server, and configuring it as a spare server, import the "Server" section and "SpareServer" section separately.

- When changing physical server names during pre-configuration, it cannot be performed at the same time as other pre-configuration operations. Import the "Server" section separately from other sections.

6. When the import is completed successfully, a message is displayed in the Recent Operations area.

🅿 Point

- Error handling

  The processing of resource registration or change is executed after the verification of the system configuration file during import.

  If an error occurs during the verification process, which means an invalid value exists in the system configuration file, an error message is displayed only in the event log. Correct the system configuration file, and import it again.
  Invalid content also includes invalid section headers.
  If there is an error message displayed, but the values in the specified line are all correct, check whether the section header is correct or not.

  If an error occurs during registration and change process, an error message is displayed in both the recent operations area and the event log. In this case, the process is finished up to the previous line setting, that is, before the system configuration file line number which message is displayed. Correct the system configuration file and rectify the problem, then import it again. The process will resume from the position where it stopped.

- Import log file

  The import log is saved in the following location on the manager.
  In cases where an error occurs in the verification step, which means the processing of registration or changing the resource has not started yet, no log file is created.

  [Windows Manager]
  Installation_folder\SVROR\Manager\var\log\config.log

  [Linux Manager]
  /var/opt/FJSVrcvmr/log/config.log

- Backing up the manager prior to import automatically

  When importing is performed by a user, exporting is also automatically executed. The export file is saved as the backup of the manager configuration. Use this file to return to the previous values if there is an input error in the system configuration file. Note that the backup can store the latest five versions.

  The system configuration file backup can be stored in the following folder on the manager.

  [Windows Manager]

  Folder

   Installation_folder\SVROR\Manager\var\config_backup

  File name

   rcxconf-*YYYYMMDDHHMMSS*.csv (the date and time are shown in *YYYYMMDDHHMMSS*)

  [Linux Manager]

  Directory

   /opt/FJSVrcvmr/var/config_backup

  File name

   rcxconf-*YYYYMMDDHHMMSS*.csv (the date and time are shown in *YYYYMMDDHHMMSS*)

7. Perform post-setting operations.

   If the import is completed successfully, perform the following procedures if required.

   - If HBA address rename is set, then restart the relevant managed server.

   - If the agent is registered, perform either one of the following to enable further backup or cloning operations.

     - Restart the managed server.

     - Restart the Related Service described in "2.2 Starting and Stopping Agents" in the "Operation Guide VE".

12.3 Exporting the System Configuration File

This section explains the method for exporting a system configuration file containing the current system settings.

Use the following procedure to export the system configuration file in CSV format from the ROR console.

1. Open and log in to the ROR console according to "Chapter 1 Login and Logout".

2. In the ROR console, select [File]-[System Configuration File]-[Export] from the menu.

3. The export process starts automatically.

4. When the process complete successfully, the [File Download] dialog is displayed.

   Click one of the following.

   - When clicking <Save>

     As the [Save As] dialog is displayed, specify the destination folder and file name, and then save the file. Note that the system configuration file can be exported only in the CSV format.

   - When clicking <Open>

     Open the file using an application (such as Excel) associated to CSV files.

   - When clicking <Cancel>

     Export operations will be canceled.

Note

- If any server is in switchover state, the server name is enclosed in parentheses, such as "(name)".

- The admin server subnet information is not output in the "Subnet" section.

- For a LAN switch blade PY CB DCB SW 10Gb 18/6/6, the VLAN settings of external ports are not exported.

- For the following LAN switch blades, VLAN settings are not exported.

  - PRIMERGY BX 900 and BX 400 LAN switch blades operating in IBP mode or Converged Fabric mode.

  - PY CB 10Gb FEX Nexus B22 LAN switch blades

Point

Error handling
If an error occurs during the export, an error message is displayed. Follow the message diagnostic to resolve the problem.

Chapter 13 NetworkViewer

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

13.1 Overview

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

- Network configuration of physical and virtual servers (including virtual switches and VM guests)

- Statuses of network links between all resources

- VLAN configuration affecting each physical and virtual server

- Resource information

When the [NetworkViewer] button displayed in the upper right of the [Resource] tab of the ROR console is clicked, the NetworkViewer is displayed in another window.

The relationships of connecting wires among the chassis, the rack mount server, and the adjoining LAN switch are displayed in the NetworkViewer initially.

When you click the [>>] button at the right of each displayed resource icon, connecting wires of the following resources in the selected resource (chassis and server), the resources that the wires are connected to, and the resources are displayed.

- Server blades

- LAN switch blades

- VM hosts

- VM guests

- Virtual switches

- Adjacent LAN switches in the connections

- Adjacent chassis with connections

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

See
. . . .

- For details on resource icons, refer to "13.4 Resource Icons".

- For details on link statuses, refer to "13.5 Network Links".

- The settings of [Extended Partitioning Mode] for PRIMEQUEST servers are not displayed in the Network View. They can be checked from the ROR console. Refer to "7.5.2 Registering PRIMEQUEST Servers".

- Internet Explorer 8 is not supported. Please use another web browser.

  For details on suported web browser, refer to "Required Software: Admin Clients" in "2.4.2.4 Required Software" in the "Design Guide VE".
. . . .

Information
. . . .

- The Network Viewer uses the Web browser's standard fonts and is designed to be viewed in a window of 1200 by 800 pixels or larger. When using a monitor with a higher resolution than this, it is recommended to enlarge the screen size. If the Web browser is resized by a significant amount, the display quality may deteriorate.

- NetworkViewer is updated automatically every ten seconds.

  When updating Network links manually, click the update button

- When the Ethernet Fabric switch that contains registered LAN switch blade PY CB Eth Switch 10/40Gb 18/8+2 in the hardware component is registered, the name of the switch blade is changed to the port name which corresponds to the Ethernet Fabric switch. Moreover, when either port is selected, the port which corresponds to the other LAN switch is selected.

. . . .

📌 Note

. . . .

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

- Chassis and servers are displayed for PRIMERGY BX series, PRIMEQUEST, and PRIMERGY RX/TX.

- The virtualization software that can display the network configuration in a virtual server is VMware and Hyper-V.

- For VMware and Hyper-V virtual switches, network links are only displayed when using the standard switches.

  When using switches other than the standard ones, such as distributed virtual switches, those virtual switches and their network links are not displayed.

- The display of Logical Networks in Hyper-V environments is not supported.

- When connecting wires between virtual LAN switches and VMware VM guests are not correctly displayed, log in to the VM management product, start the VM guest and then execute the update of the network information.

- When SCVMM is not registered with ROR, the resources of Hyper-V might not be correctly displayed.

- The network links between virtual lan switch and physical nic on server of PRIMERGY RX/TX is not displayed.

- Neither the logical port nor the relation of links of the link aggregation are displayed.

- When two or more VM hosts with the same name exist, the relation between the VM host and the Virtual LAN Switch might not be correctly displayed.

- VLAN is not displayed for ports where trunk VLANs or private VLANs are set and ports in promiscuous mode.

- The display of NIC teaming is not supported when the following NIC teaming software is used.

  - One Command NIC Teaming and Multiple VLAN Manager

  - NIC Teaming (LBFO)

- Virtual LAN Switches, Virtual NICs of Virtual Machine and network links are not displayed in Hyper-V 2012 R2 without SCVMM environment.

. . . .

The following operations are available in the NetworkViewer.

- Screen scrolling

  - Scroll button

  - Map drag and drop

  - Navigation map drag and drop

- Maximizing and minimizing of the display area

- Updating to show the latest status

- Hiding of the navigation map

- Maximizing and minimizing of the Utility Panel

- Opening and shutting of each box in Utility Panel, and vertical replacement of display positions

- Only error and the warning links are displayed.

- Resetting to the initial display of the Network view

- Filtering display information using Point-to-Point Route Search

- Searching of resources and VLAN IDs

- Highlighting of a selected resource and display of its details

- Displaying the menu from the upper right of a resource

- Showing or hiding of details for the following resources

    - Chassis

    - Rack mount servers (including VM hosts)

    - Servers (including VM hosts)

    - LAN switch blades

    - LAN switches

    - VM guests

    - Virtual switches

13.2 Preparations

The following preparations are required to add display content to the NetworkViewer.

1. Register LAN Switch Blades Included in a Chassis

   For details on the registration method, refer to "7.3.3 Registering LAN Switch Blades".

2. Register LAN Switches

   For details on the registration method, refer to "7.10 Registering LAN Switches".

   The following LAN switches are supported by the Network Map.

   - BX600 GbE Switch Blade 30/12

   - PY CB Eth Switch/IBP 1Gb 36/12

   - PY CB Eth Switch/IBP 1Gb 36/8+2

   - PY CB Eth Switch/IBP 1Gb 18/6

   - PY CB Eth Switch/IBP 10Gb 18/8

   - PY CB Eth Switch 10/40Gb 18/8+2

   - PY CB DCB SW 10Gb 18/6/6

   - PY CB 10Gb FEX Nexus B22

   - Cisco Catalyst 2950 series

   - Cisco Catalyst 2960 series

   - Cisco Catalyst 3560 series

   - Cisco Catalyst 3750 series

3. Detect physical network links

   a. From the ROR console menu, select [Tools]-[Topology]-[Detect physical links].

      The [Detect Physical Links] dialog is displayed.

   b. Click <OK>.

Note

- Only network links between LAN switch blades of PRIMERGY BX series and LAN switches are displayed. Network links between server of PRIMEQUEST and LAN switches or server of PRIMERGY RX/TX and LAN switches are not displayed.

- If no LAN switch blades have been registered, only network links between external LAN switches will be displayed. If only one LAN switch blade is registered, no network links will be displayed at all.

- If a non-supported LAN switch is registered, network links may not be properly displayed for that switch.

- The Network Map cannot display network links between BX600 GbE Switch Blade 30/12 and the following LAN switch blades:

    - PY CB Eth Switch/IBP 1Gb 36/12

    - PY CB Eth Switch/IBP 1Gb 36/8+2

    - PY CB Eth Switch/IBP 1Gb 18/6

- Network links between two supported LAN switches may not be displayed properly if an unregistered or un-supported LAN switch is placed between them.

Example

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

- The links of an external port are not displayed for LAN switch blades that operate in Converged Fabric mode or LAN switch blade PY CB 10Gb FEX Nexus B22.

- The links composing link aggregation might not be correctly displayed.

13.3 Screen Layout

This section describes the NetworkViewer's layout.

The main part of the NetworkViewer is the network view.

13.3.1 NetworkViewer Layout

This section describes the NetworkViewer's layout.

Network view

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

Resource Search(Search)

The area retrieved by the resource name.

VLAN ID Search(Marker)

The area retrieved by the VLAN ID.

Filter

Displays the checkbox for selecting links to display.

Update button

Update the NetworkViewer to show the latest status.

Utility Panel

Panel comprised of the Control Box, Detail box, and Route Search Box.

Control box

Scroll button

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

Magnification slider

Maximizes or minimizes the network view.

Display initialization button

The button that returns a window that has been moved using the move button to its default position.

Detail Box

Resource details are displayed.

Only information on the following resources is displayed.

- Chassis

- Rack mount servers

- Server blade

- LAN switch blades

- VM hosts

- VM guests

- LAN Switch

Route Search Box

The area that specifies the filter of the route is displayed.

Map navigation area

All areas are displayed, including those that cannot be displayed by NetworkView.

13.3.2 Network View

This section describes the information that is displayed in NetworkView.

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

Selecting a resource will highlight it in blue. Adjacent servers and LAN switches are indicated by light blue frames.
When a selected resource is expanded, information about links with other resources and the relations of links with resources in the expanded resource is displayed.

Expand button

When the following is selected, the button is displayed on the upper right and to the right of the icon.
When the upper right button is clicked, the menu is displayed.
When the button to the right is clicked, the content of the resource is expanded.

- Chassis

- Rack mount servers

- Server blade

- LAN switch blades

- VM hosts

- VM guests

- Virtual switches

- LAN switches

Close button

When the right button displayed in the icon of the expanded resource is clicked, the expander of each resource is closed.

13.4 Resource Icons

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

13.4.1 Resource Display

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

Table 13.1 Resource Icons

Icon	Meaning
	Chassis
	Server
	LAN switch blade
	LAN switch blade in IBP mode
	LAN switch blade in VCS mode
	LAN switch blade in Converged Fabric mode
	VM host
	VM guest
	Virtual switch
	LAN switch

Table 13.2 Resource Status Icons

Icon	Status	Meaning
	normal	No new errors, warnings, or stops were detected.
	warning	A warning was detected.
	unknown	The status could not be obtained.
	error	An error was detected.
	fatal	A fatal error was detected, the resource is now unusable.
	stop	The resource was detected to have been powered off.
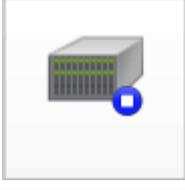
Table 13.3 Port Icons

Icon	Meaning
1	Connected port
1	Not connected port

Table 13.4 Port Status Icons

Icon	Status	Meaning
1	normal	No new errors or disabled status were detected. The state of the port is always displayed as normal status for LAN switch blades that operate in Converged Fabric mode or LAN switch blade PY CB 10Gb FEX Nexus B22.
1	error	An error was detected from the port (e.g. the opposite port of the NIC, LAN switch was disabled, or the cable between this link and its opposite port or NIC was disconnected). When ports of a network device other than a LAN switch blade are disabled, the state of the port is displayed as error.
1	disabled	The port was detected to have been disabled (offline).

13.4.2 VLAN Display

The icons displayed when a VLAN is displayed are those from "13.4.1 Resource Display" of enclosed with a green frame.

📖 Information

....

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

For details on status icons, refer to "13.4.1 Resource Display".

....

13.4.3 Other Icons

The following tables detail the icons displayed in the NetworkViewer.

Table 13.5 Admin Server Icon

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

13.5 Network Links

This section explains the network links displayed in the NetworkViewer.

13.5.1 Link Display

The following table details the physical and virtual links displayed between resources.
The color of links changes depending on resource status, VLAN search status, and the selection state of resources.

Table 13.6 Links related to Unselected Resources

Status	Default/VLAN	Link	Meaning
normal	Default		Represents a physical or virtual link.
	Selecting VLAN		
error	Default		Represents a link with an error status (e.g. an error occurred in the LAN switch blade or LAN switch port, or the cable between this link and its opposite port or NIC is disconnected).
	Selecting VLAN		
warning	Default		When error status is found in some links among multiple links connecting resources, the warning status is shown.
	Selecting VLAN		
Disabled	Default		Represents a disabled port.
	Selecting VLAN		

Table 13.7 Links related to the Selected Resource

Status	Default/VLAN	Link	Meaning
normal	Default		Represents a physical or virtual link.
	Selecting VLAN		
error	Default		Represents a link with an error status (e.g. an error occurred in the LAN switch blade or LAN switch port, or the cable between this link and its opposite port or NIC is disconnected).
	Selecting VLAN		
warning	Default		When error status is found in some links among multiple links connecting resources, the warning status is shown.
	Selecting VLAN		
Disabled	Default		Represents a disabled port.
	Selecting VLAN		

![Note]

VLAN search status is only displayed for port to port or port to NIC. If both ends are not port or NIC, the VLAN search status is not displayed.

13.6 Display Filters

This section explains how to use display filters.

Filter

The display filter area does not include the following filters (checkboxes).
Enabling this filter will display links with error and warning status between resources on the NetworkViewer.

13.7 Point-to-Point Route Search

Selecting two resources displayed in the network view displays a route with which point-to-point communication is possible.

![Information]

When there are multiple links in the selected resource, the resource and links other than the route of the point-to-point might be displayed.

The following resources can be selected by the point-to-point route search.

- Server

- VM hosts

- VM guests

- Virtual switches

- LAN switch blades

- LAN switches

The procedure for displaying the route point-to-point has the following two methods.

- Operation from the Utility Panel

- Operation from menu on the upper-right of an icon

The operation procedure is shown below.

1. Select the resource to use as the start and select [Route from here]

2. Select the resource to use as the end and select [Route to here]

3. Select [Route Search]

Example

Operation procedure from the utility panel

1. Select one of the resources to display the route for in NetworkViewer.

   The utility panel is displayed.

2. Select [Route from here] in the detail box of the utility panel.

   Or select [Route from here] in the route filter box of the utility panel.

   The (1) mark is displayed on the selected resource.

3. Select the other resource to use to display the route using NetworkViewer.

   The utility panel is displayed.

4. Select [Route to here] in the route filter box of utility panel.

   The (2) mark is displayed on the selected resource.

5. Select [Route Search] in the route filter box of utility panel.

   The resources and links along the route of the selected point-to-point are displayed.
   When two or more routes exist, all routes are displayed.

Note

- The display of resources included in the resource that has been selected cannot be closed while selecting the resources for the route search.

- The search results may differ according to whether or not the resource has been deployed.

   Execute Route Search when you want to search for a correct route with a deployed resource.

- Point-to-Point Route Search is not be able to search Network links that is not displayed on Network view.

Chapter 14 Power Control

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

14.1 Server Power Control

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

Use the following procedure to perform power control operations.

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

   ON

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

   OFF

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

   OFF (Forced)

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

   Reboot

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

   Reboot (Forced)

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

   The confirmation dialog is displayed.

2. Click <OK>.

   The specified power control operation is executed.

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

Information

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

Note

- VM guests must be properly configured in order to use the power off or reboot options.
  Attempting to shut down or reboot a VM guest that is not properly configured will result in an error.
  For details, refer to "D.2 Configuration Requirements" in the "Design Guide VE".

- Depending on the server virtualization environment, a VM guest may automatically migrate to another VM host when a power control operation is performed. This may cause power control operations to fail and return an error when used on VM guests.
  For details, refer to "D.3 Functional Differences between Products" in the "Design Guide VE".

- A VM guest can be configured to automatically start or stop whenever its VM host starts up or shuts down. This can be achieved by configuring the VM guest's startup and shutdown options in the server virtualization software used.
  For details, refer to the server virtualization software manual.

- Take caution regarding the following points when shutting down or rebooting a PRIMEQUEST managed server.

  - If rebooting is attempted for a server that has been placed into hardware maintenance mode, the operation fails and only powering-off is performed.

[Windows]

- Take caution regarding the following points when shutting down or rebooting a managed server running a Windows operating system.

    - If Windows is not configured to shut down when the computer's power button is pressed, the power operations in Resource Orchestrator may not function properly.
    To check this option, access the Control Panel, open the [Power Options], and check the settings of the [Advanced] tab in the [Power Options Properties] window.

    - If a file is being edited by a logged-in user, a dialog prompting the user to save the file is displayed, and the system may not shut down immediately.
    In such cases, shutdown does not take place until the user takes the appropriate action or a specified time (approximately five minutes) has elapsed.

[OVM for SPARC]
When the function is not supported by OVM for SPARC, stopping and rebooting of the VM guest cannot be performed.
Based on the virtual machine status, either directly operate the virtual machine, or perform a forced stop or forced reboot.
When executing power operations of VM guest using this product, binding / unbinding of resources is also executed.

- When starting a VM guest

  Binding of resources is executed.

- When stopping a VM guest

  Unbinding of resources is executed.

- When restarting a VM guest

  Binding/unbinding of resources is not executed.

In this product, VM guest configuration information is saved automatically after power operations are performed.
When you disable the auto-save function of configuration information in this product, add a definition to the definition file which configures the execution of configuration information preservation.
For details of a definition file, refer to "D.4 Definition Files of Each Product" in the "Design Guide VE".

[VMware] [Hyper-V] [Xen] [Citrix Xen] [KVM] [Solaris Zones] [OVM for x86 3.2] [OVM for SPARC]

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

    - When using a server virtualization software's high-availability feature, confirm that the server is set to VM maintenance mode within that virtualization software. This can be confirmed from the virtualization software client.

    - Perform power operations only after setting VM maintenance mode (either from the VM management software client or using the resource control command).
    Refer to the server virtualization software manual, or to "3.2 rcxadm server" in the "Reference Guide (Command) VE" for details.
    Depending on the server virtualization software used, some restrictions may apply to the use of VM maintenance mode settings.
    For details about such restrictions, refer to "D.3 Functional Differences between Products" in the "Design Guide VE".

14.2 Chassis Power Control

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

Power operations are only possible for PRIMERGY BX server chassis.
The power state of a blade chassis can be controlled using the rcxadm chassis command.
For details, refer to "3.1 rcxadm chassis" in the "Reference Guide (Command) VE".

Chapter 15 Control of VM Environments

This chapter explains the Resource Orchestrator functions that are specific to VM guests and VM hosts.
Some functions may or may not be available depending on the server virtualization software used. Refer to "D.1 Common Functions of Server Virtualization Software" in the "Design Guide VE" for details.
Other functions are similar in use to those available for regular physical OSs (without server virtualization software).

15.1 Migration of VM Guests between Servers

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

Two methods of VM guest migration are available in Resource Orchestrator. Although such methods are named differently depending on the server virtualization software used, Resource Orchestrator makes use of the following naming convention.
For details on migration pre-requisites and terminology, refer to "D.3 Functional Differences between Products" in the "Design Guide VE".

- Live Migration

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

- Cold Migration

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

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

Table 15.1 Migration Methods Available for Each Power Status

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

Default: This method is available and selected by default.
Available: This method is available.
N/A: This method is not available.

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

Use the following procedure to migrate a VM guest.

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

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

    Set the following items:

    Destination

        Select a destination VM host.

    Migration Method

        Select the desired migration type.

3. Click <OK>.

    The selected VM guest is migrated to its new host.

VM guests can be migrated from the command-line, using the rcxadm server migrate command.
For details, refer to "3.2 rcxadm server" in the "Reference Guide (Command) VE".

15.2 VM Maintenance Mode of VM Hosts

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

For details on VM maintenance mode, refer to "D.3 Functional Differences between Products" in the "Design Guide VE".
VM maintenance mode can also be set or released from the command-line, using the rcxadm server set command.
For details, refer to "3.2 rcxadm server" in the "Reference Guide (Command) VE".

15.3 VM Home Position

This section explains VM Home Position.

By configuring the VM Home Position in advance, it is possible to restore VM guests to their original VM host using only one operation when they have been migrated to a different VM host for operation or maintenance needs.
This enables restoration of multiple VM guests to their original locations without the need to record their original locations.

15.3.1 Setting VM Home Position

When configuring a VM Home Position, the relationships of operating VM guests and registered VM hosts are retained.
Setting is only available when more than one VM guest exists.

Information

- When registering a new VM host, as the relationship between the VM host and operating VM guests is not yet retained, reconfiguration of VM Home Position is necessary.

- When a new VM guest is detected, reconfigure the VM Home Position so the relationship between that VM guest and its VM host is set.

- When configuring the home position of a system, all VM Home Positions of VM guests are set to the current configuration.

- When configuring home positions for each VM host, VM guests will be associated with the VM host on which they are operating. The relationships are retained, even when a VM guest associated with the VM host is operating on another VM host.

- VM guests that have been migrated to somewhere other than the cluster set with the VM management product cannot be returned to their original VM host using the VM home position.

Configuring a System's VM Home Position

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

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

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

2. Click <OK>.

   The VM Home Position is set.

Configuring a VM Host's VM Home Position

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

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

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

2. Click <OK>.

   The VM Home Position is set.

15.3.2 Migrating to VM Home Position

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

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

Migrating all VM Guests to their VM Home Positions

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

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

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

2. Click <OK>.

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

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

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

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

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

2. Click <OK>.

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

When migrating VM guests to their VM Home Position, use the rcxadm server migrate command.
For details on the rcxadm server command, refer to "3.2 rcxadm server" in the "Reference Guide (Command) VE".

15.3.3 Clearing VM Home Position

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

Clearing a System's VM Home Position

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

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

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

2. Click <OK>.

   The VM Home Position settings are cleared.

Clearing a VM Host's VM Home Position

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

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

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

2. Click <OK>.

   The VM Home Position setting is cleared.

15.4 External Software

This section explains how to configure the settings required by Resource Orchestrator to interact with third party software.

VM Management Console

To launch an external VM management console (provided by the virtualization software used) from the ROR console, users must be granted the permission to launch this management console in the Java Plug-in policy settings. For details on the VM management consoles that can be started from the ROR console, refer to "D.2 Configuration Requirements" in the "Design Guide VE".

Use the following procedure to enable launch of the VM management console.

1. In the ROR console server resource tree, right-click the target VM host or VM guest, and select [VM Management Console] from the menu that is displayed.

   The [Launch VM Management Console] dialog is displayed.

2. Click <OK>.

   If launch of the VM management console from the ROR console has not been enabled yet, a [Download] dialog for the Java policy setup script is displayed.

3. Click <OK>.

   This will download the Java policy setup script. Save the script to an arbitrary location.

4. Execute the saved Java policy setup script. This will configure Java policy settings and allow launch of the VM management console.

5. Close all Web browsers.

   After closing all open Web browsers, start a new Web browser and re-log into the ROR console. The VM management console can now be launched from the ROR console.

Information

. . . .
Depending on script-related settings, the command prompt opened by the Java policy setup script may close right after finishing its execution, making it impossible to confirm whether the script ended successfully.
In this case, select [start]-[Run] from the Windows start menu, and execute the following command.

wscript "*Full_path_name_of_the_Java_policy_setup_script*"

. . . .

Note

. . . .
If the VM management screen is started on VMware vSphere 5.0 or later, it may connect with the VM management product or the VM host, and login may fail.
In this case, input the password from the VM management screen, and log in.
. . . .

Chapter 16 Backup and Restore

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

16.1 Overview

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

The system image backup and restore function enables backup of images of physical OSs and VM hosts over the network, and stores them on a disk on the admin server.
A system image backup can be used for the following purposes.

- Software maintenance

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

- Hardware maintenance

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

Note

- Regardless of the boot environment (local/SAN/iSCSI) and RAID configurations, only the contents of the first disk (boot disk) recognized by the managed server's BIOS can be backed up and restored.
  For a server using local boot with a SAN data configuration, it is necessary to configure the target disk of image operations.
  For details, refer to "9.1.13 Changing Target Disks of Image Operations".
  The contents of other disks (data disks) cannot be backed up and restored. To properly backup and restore such data disks, it is recommended to use dedicated backup software, or the copy functions available in storage devices.
  When the first disk contains multiple partitions (Windows drive, Linux/VMware partition), all partitions are backed up.

Table 16.1 Examples of system image backup and restore targets

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

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

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

- The first partition must be the boot partition.

- The operations for backup and restore of VM hosts differ depending on the server virtualization software used.
  For an explanation of the behavior differences that occur when VM guests are included in the VM host's boot disk, refer to "D.3 Functional Differences between Products" in the "Design Guide VE".
  If VM guests on the boot disk are not to be backed up (and restored), VM guest files should be moved to another disk.

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

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

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

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

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

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

- Deleting a managed server will delete its backed up system images at the same time.

- It is not possible to backup, restore, or delete a system image from a managed server for which a system image (including different versions) is already being backed up, restored, or deleted.

- When restoring a system image on a server whose name was changed after the deployment of a cloning image, check that the "*server_name*" displayed on the server resource tree and the System Image List match the new server name before restoring the system image.

- For managed servers on which the Watchdog function is enabled, backup or restore operations on that server may be aborted by an automatic restart or shutdown. The Watchdog is a function which automatically restarts or shuts down non-responsive servers when their operating system does not respond for a given period.
  Therefore, it is highly recommended to disable the Watchdog function before a backup or restore operation.
  For details on the Watchdog function, refer to the server manual.

- If the disk size of the source (backed up) server differs from that of the destination (restored) server, restore is possible only in cases where the disk size of the destination server is larger than that of the source server.
  In that case, unused disk space will remain on the destination server. To use this unused disk space, a partition should first be created from it.

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

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

- When backing up or restoring system images, or collecting and deploying cloning images, up to four processes can be executed simultaneously. If four processes are already being executed, any additional image operations will enter a standby state.
  Moreover, server switchover which is executed using the backup and restore method or any restore process performed during failback will also enter a standby state. When Auto-Recovery or manual switchover using the backup and restore method is used, please limit the number of image operations (backup or restore of system images, or collection and deployment of cloning images) performed at the same time to 3.

- When using backup and restore for PRIMEQUEST servers, check that the boot option settings and BIOS settings of the target servers match. When the settings are different, execute the function after changing the settings so they match. For details on how to change boot options, refer to "9.1.10 Changing Boot Options".
  When using PRIMEQUEST 1000 Type2, disable the x2APIC mode of the UEFI.

- For the PRIMEQUEST 2000 series, backup and restore is only possible when using Windows managers. PXE boot is only supported by on-board LAN NICs.

- For Linux managed servers, when the disks are recognized by using by-id name, the collected system images cannot be restored after replacing the disks.

16.2 Backup

This section explains how to collect a system image backup.

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

System images can also be backed up using commands.

Refer to "Chapter 4 Image Operations" in the "Reference Guide (Command) VE" for details.

Preparations

If the managed server has the following configuration, configure the target disk of image operations before performing backup.

- Local boot with a SAN data environment

    For the configuration procedure, refer to "9.1.13 Changing Target Disks of Image Operations".

Execute the command below before performing backup if the managed server has the following configuration.

- When using the Red Hat Enterprise Linux 6 ext4 file system, and one of the following conditions is met

    - In a SAN boot environment using HBA address rename

    - When using a rack mount or tower server and the server is registered with "Disable" of "Association with server management software (ServerView)" is selected

    [Windows Manager]

    > *Installation_folder***SVROR\Manager\bin\rcxadm server set -name** *physical server* **-attr bootagt=winpe** <RETURN>

    [Linux Manager]

    #**/opt/FJSVrcvmr/bin/rcxadm server set -name** *physical server* **-attr bootagt=winpe** <RETURN>

- In a SAN boot environment using HBA address rename, and the following model or OS

    - PRIMERGY BX960 S1

    - XenServer6 or later

    [Windows Manager]

    > *Installation_folder***SVROR\Manager\bin\rcxadm server set -name** *physical server* **-attr bootagt=winpe** <RETURN>

    [Linux Manager]

    #**/opt/FJSVrcvmr/bin/rcxadm server set -name** *physical server* **-attr bootagt=winpe** <RETURN>

Backing up a System Image

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

1. Place the target server into maintenance mode and stop all of its applications.

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

       The [Set Maintenance Mode] dialog is displayed.

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

    b. Click <OK>.

       The target server is placed into maintenance mode.

2. Back up a system image from the target server.

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

       The [Backup] dialog is displayed.

    b. Set the following items as necessary:

       Comment

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

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

    c. Click <OK>.

       Backup of the system image is started.

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

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

       After backing up a VM host, stop and back up all of its VM guests.
       For details on VM guest backup, refer to the server virtualization software manual.

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

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

       The [Release Maintenance Mode] dialog is displayed.

    b. Click <OK>.

       The target server is released from maintenance mode.

> **Note**
>
> - The number of system image versions that can be kept for a managed server is limited.
>   If a new system image backup is collected when this limit has already been reached, the oldest version will be deleted.
>   By default, the maximum number of system images is 3.
>   This setting can be changed by following the instructions given in "8.3 Changing the Maximum Number of System Image Versions".
>
> - When backing up a new system image, its version number will be increased by one. The version number of the first backed up system image of a managed server will always be 1.
>
> - When backing up a VM host in a high-availability configuration, all VM guests stored on shared disks should be migrated to another VM host beforehand.
>   During backup, because the target VM host will be automatically set to VM maintenance mode, the VM host should be in a state that allows VM maintenance mode to be set.
>   After backing up the VM host, migrate the VM guests back to their original VM host.
>
>   Refer to the server virtualization software manual and "D.3 Functional Differences between Products" in the "Design Guide VE" for information on how to migrate VM guests, or about the VM maintenance mode.
>
> - When using PRIMECLUSTER GLS for admin LAN redundancy, backup of a system image may fail if the following message is displayed in the event log.

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

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

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

16.3 Restore

This section explains how to restore a system image backup.

System images can also be restored using commands.
Refer to "Chapter 4 Image Operations" in the "Reference Guide (Command) VE" for details.

Restoring a System Image

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

1. Place the target server into maintenance mode.

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

   The [Set Maintenance Mode] dialog is displayed.

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

   b. Click <OK>.

   The target server is placed into maintenance mode.

2. Restore a system image.

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

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

     The [Restore] dialog is displayed.

     b. Select the system image to be restored.

     c. Click <OK>.

     Restoration of the system image is started.

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

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

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

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

     The System Image List is displayed.

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

     The [Restore] dialog is displayed.

     c. Click <OK>.

     Restoration of the system image is started.

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

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

     When restoring a VM host, be sure to also restore the VM guest backups that correspond to the restored VM host backup version.
     For details on restoring VM guests, refer to the server virtualization software manual.

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

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

   The [Release Maintenance Mode] dialog is displayed.

   b. Click <OK>.

   The target server is released from maintenance mode.

ⓘ Note

. . . .

If the target VM host is in a high-availability configuration, all VM guests stored on shared disks should be migrated to another VM host beforehand.
During restore, because the target VM host will be automatically set to VM maintenance mode, the VM host should be in a state that allows VM maintenance mode to be set.
After restoring the VM host, migrate the VM guests back to their original VM host.

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

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

When the managed server has the following configuration, restoration may not be performed correctly unless the target disk of image operations has been configured.

- Local boot with a SAN data environment

  For the configuration procedure, refer to "9.1.13 Changing Target Disks of Image Operations".

When the managed server is in the following configuration, if the following command has not been executed before restore, restore may not be executed correctly.

- When using the Red Hat Enterprise Linux 6 ext4 file system, and one of the following conditions is met

  - In a SAN boot environment using HBA address rename

  - When using a rack mount or tower server and the server is registered with "Disable" of "Association with server management software (ServerView)" is selected

  [Windows Manager]

  ```
  >Installation_folder\SVROR\Manager\bin\rcxadm server set -name physical server -attr bootagt=winpe <RETURN>
  ```

  [Linux Manager]

  ```
  #/opt/FJSVrcvmr/bin/rcxadm server set -name physical server -attr bootagt=winpe <RETURN>
  ```

- In a SAN boot environment using HBA address rename, and the following model or OS

  - PRIMERGY BX960 S1

  - XenServer6 or later

  [Windows Manager]

  ```
  >Installation_folder\SVROR\Manager\bin\rcxadm server set -name physical server -attr bootagt=winpe <RETURN>
  ```

  [Linux Manager]

  ```
  #/opt/FJSVrcvmr/bin/rcxadm server set -name physical server -attr bootagt=winpe <RETURN>
  ```

. . . .

16.4 Viewing

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

System images can also be listed using commands.
Refer to "Chapter 4 Image Operations" in the "Reference Guide (Command) VE" for details.

In the ROR console, select the [Image List] tab.
The System Image List is displayed.

Figure 16.1 System Image List
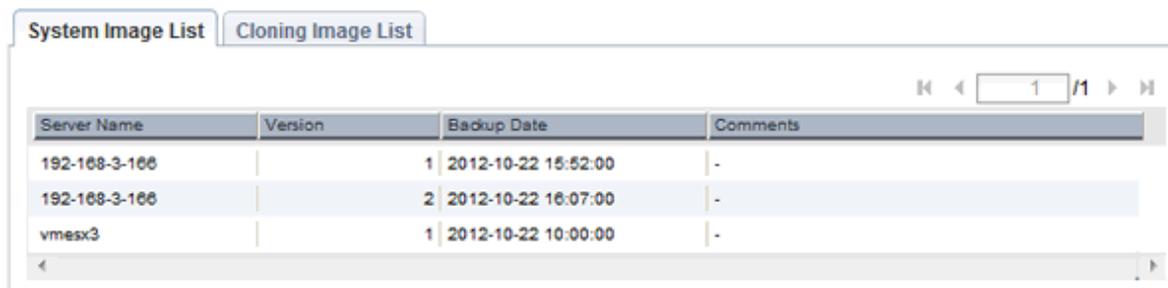
Server Name	Version	Backup Date	Comments
192-168-3-166	1	2012-10-22 15:52:00	-
192-168-3-166	2	2012-10-22 16:07:00	-
vmesx3	1	2012-10-22 10:00:00	-

Refer to "A.8 [Image List] Tab" for details on the System Image List.

To view the most recent system image backup of a managed server, select a server OS from the server resource tree and click the [Resource Details] tab.
The latest system image backup collected from the selected server is displayed under "Latest System Image".
For details about system image information, refer to "A.6 [Resource Details] Tab".

16.5 Deleting

This section explains how to delete system image backups.

System images can also be deleted using commands.
Refer to "Chapter 4 Image Operations" in the "Reference Guide (Command) VE" for details.

Deleting a System Image

Use the following procedure to delete a system image.

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

   The System Image List is displayed.

2. In the System Image List, right-click the system image to delete and select [Delete] from the popup menu.

   The [Delete a System Image] dialog is displayed.

3. Click <OK>.

   The selected system image is deleted.

Note

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

Chapter 17 Cloning [Physical Servers]

This chapter explains how to use the server cloning function.

17.1 Overview

Cloning is a function used to deploy a cloning image collected from a single managed server (source server) to other managed servers (destination servers).

This function shortens the time required for an initial installation as it can be used to install the same operating system and software on multiple servers.
Software maintenance can also be performed quickly and easily by deploying a cloning image collected from a server on which patch application or software addition or modification has been performed.

The information below is not copied when the cloning image is collected from the managed server; and will be automatically reconfigured when the cloning image is deployed. This enables a single cloning image to be deployed to different servers.

- Hostname

- IP address and subnet mask for the admin LAN

- Default gateway for the admin LAN

Settings other than the above (such as those for applications and middleware) are not automatically reconfigured, please set them manually before and after the cloning operation when necessary.

The public LAN settings (IP address and redundancy settings) for servers to which the cloning image is deployed can be configured easily by using the network parameter auto-configuration function.
For details on the network parameter auto-configuration function, refer to "17.6 Network Parameter Auto-Configuration for Cloning Images".

Cloning cannot be performed for Linux managed servers on which iSCSI disks have been configured.

Note

- When using ServerView Deployment Manager on the admin LAN, this function is disabled. Use the cloning function of ServerView Deployment Manager. For details, refer to "Appendix B Co-Existence with ServerView Deployment Manager" in the "Setup Guide VE".

- When using server cloning, regardless of the boot environment (local/SAN/iSCSI) or RAID configurations, only content from the boot disk (first disk recognized by the BIOS on managed servers) is actually cloned.
  Data disk content (second disk onwards) cannot be cloned. It is recommended to use other backup software, or copy features available in storage systems for such purposes.
  For a server using local boot with a SAN data configuration, it is necessary to configure the target disk of image operations.
  If cloning images are deployed without configuring the target disk for image operations, data may be overwritten on an unintended disk.

  For details, refer to "9.1.13 Changing Target Disks of Image Operations".

  Note that all partitions (Windows drives or Linux partitions) included in the boot disk will be cloned.

Table 17.1 Cloning Target Examples

Disk	Windows Drive	Cloning Target
First	C:	Yes
	E:	Yes
Second	D:	No
	F:	No

- Because managed servers are restarted during the cloning process, it is necessary to stop all applications running on those servers beforehand.

- The first partition must be a primary partition.

  When multiple partitions exist within the disk of the cloning target, the drive letters for the drives other than the system drive may be changed after cloning images are deployed. Change the drive letter back to the original letter, after deploying cloning images.

- Dynamic disks cannot be used.

- Cloning images can be collected with the following file systems. Note that LVM (Logical Volume Manager) partitions are not supported.

    - NTFS

    - EXT3

    - EXT4

    - LinuxSwap

- When using Windows Server 2012 as a managed server, cloning images cannot be collected from system disks that include ReFS data areas.

- All of the following conditions must be met for the managed server to collect the cloning image from and the managed server to deploy the cloning image to.

    - All server models must be identical.

    - The hardware configuration of each server must be identical, including optional cards, expansion boards, and the slots they are mounted in.

    - The same BIOS settings must have been made for all servers according to the procedure in "6.2.7 Configuring BIOS Settings of Managed Servers" in the "Design Guide VE".

    - All servers must use the same redundancy configuration (if any) and the same number of redundant paths for LAN and SAN connections. All servers must also be able to access the same network and storage devices.
      Note that LAN or fibre channel switches connected in a cascade configuration are viewed as a single device.

- Some applications may require manual adjustments to function properly after cloning.
  If necessary, manually perform such adjustments before or after the cloning process.

- When backing up or restoring system images, or collecting and deploying cloning images, up to four processes can be executed simultaneously. If four processes are already being executed, any additional image operations will enter a standby state.
  Moreover, server switchover which is executed using the backup and restore method or any restore process performed during failback will also enter a standby state. When using auto-recovery and manual switchover operations with the backup/restore method, execute a maximum of three system image backup/restore or cloning image collection/deployment operations at the same time.

- After collecting or deploying a cloning image, software required for connecting to external servers, etc. when the OS is started may not start correctly.
  In this case, restart the operating system after collecting or deploying the cloning image.

- For managed servers on which the Watchdog function is enabled, cloning operations on that server may be aborted by an automatic restart or shutdown. The Watchdog is a function which automatically restarts or shuts down non-responsive servers when their operating system does not respond for a given period.
  It is therefore highly recommended to disable the Watchdog function before a cloning operation.
  For details, refer to the manual of the managed server.

- When using MAK license activation with Windows Server 2008 or Windows Server 2008 R2, Sysprep can be executed a maximum of three times.
  Since Sysprep is executed when deploying a cloning image, cloning image collection and deployment cannot be executed four or more times.
  Therefore, it is recommended not to collect cloning images from managed servers that have had cloning images deployed, but to collect them from a dedicated master server.

- As there is a chance that data will be damaged, do not perform collection or deployment of a cloning image while performing an iSCSI connection using a software initiator.
  When using data disks, use the hardware initiator.

- For Linux managed servers, when the disks are recognized by using by-id name, cloning cannot be performed.

17.2 Collecting

When installing servers using the cloning function, first collect a cloning image from a source server. Collected cloning images can later be used for the deployment of other servers.

A cloning image can be collected only from a managed server on which an agent has been registered.
For details on registering agents, refer to "Chapter 7 Installing Software and Registering Agents on Managed Servers" in the "Setup Guide VE".

A cloning image can be collected from a managed server that satisfies all of the following conditions:

- The status is either "normal" or "warning"

- Has been placed into maintenance mode

Cloning images cannot be collected from VM hosts or VM guests.

Preparations

- Install the desired operating system and necessary applications on the managed server from which a cloning image will be collected.
  Additionally, apply any required patches and other necessary settings.
  Make sure that the source server operates properly after those steps.

- If the managed server has the following configuration, configure the target disk of image operations before collecting cloning images.

  - Local boot with a SAN data environment

    For the configuration procedure, refer to "9.1.13 Changing Target Disks of Image Operations".

- When the configurations of managed servers are as below, execute the following commands before collecting cloning images.

  - When using the Red Hat Enterprise Linux 6 ext4 file system, and one of the following conditions is met

    - In a SAN boot environment using HBA address rename

    - When using a rack mount or tower server and the server is registered with "Disable" of "Association with server management software (ServerView)" is selected

    [Windows Manager]

    > >*Installation_folder***SVROR\Manager\bin\rcxadm server set -name** *physical server* **-attr bootagt=winpe** <RETURN>

    [Linux Manager]

    > **#/opt/FJSVrcvmr/bin/rcxadm server set -name** *physical server* **-attr bootagt=winpe** <RETURN>

  - In a SAN boot environment using HBA address rename, and the following model

    - PRIMERGY BX960 S1

    [Windows Manager]

    > >*Installation_folder***SVROR\Manager\bin\rcxadm server set -name** *physical server* **-attr bootagt=winpe** <RETURN>

    [Linux Manager]

    > **#/opt/FJSVrcvmr/bin/rcxadm server set -name** *physical server* **-attr bootagt=winpe** <RETURN>

- Check whether the DHCP client is enabled on the managed server to collect the cloning image from.

- Cloning images with the same name can be saved up until the maximum number of image versions.
  When collecting a new cloning image when the maximum number of image versions has already been reached, select the cloning image to delete.
  The maximum number of image versions is three by default.

This setting can be changed by following the instructions given in "8.4 Changing the Maximum Number of Cloning Image Versions".

- When deploying cloning images, the destination server temporarily starts up with its hostname set to either the physical server name or the source server's hostname.
  If the same server names are detected on the same network, a network duplication error will occur.
  Some programs may experience problems when started with a different hostname. If such programs have been installed, configure their services not to start automatically. This has to be configured before collecting the cloning image.

  Some programs may experience problems when the same server name exists. If such programs have been installed, configure their services not to start automatically. This has to be configured before collecting cloning images.

- When using the network parameter auto-configuration function, check the operation before performing collection.
  For details, refer to "17.6.1 Operation Checks and Preparations".

- When the target of operation is a PRIMEQUEST server, confirm that the boot option settings on the target server and the boot option set in BIOS are configured for Legacy boot.
  When the settings of one of the servers are UEFI, configure the settings after changing to Legacy boot.
  For details on how to change boot options, refer to "9.1.10 Changing Boot Options".

- When using local disks as system disks, and iSCSI storage as data disks, refer to the advisory notes described in "Table 8.1 Supported Storage Configurations" in "8.1.1 Storage Configuration" in the "Design Guide VE".

[Windows]

- Enable NetBIOS over TCP/IP

- A volume license is required for cloning, and must be entered during the installation of Resource Orchestrator Agent.
  Refer to "2.2.1.2 Collecting and Checking Required Information" and "2.2.2 Installation [Windows] [Hyper-V]" in the "Setup Guide VE" for details.

  If no volume license is entered during the agent installation, or if this information is changed after installation, edit the following license configuration file on the source server. Note that the structure and location of this file depend on the version of Windows that is being used.

  - For Windows Server 2003

    Installation_folder\Agent\scw\SeparateSetting\sysprep\sysprep.inf

    Edit the following line to enter a valid product ID.

    ```
    ProductID=Windows product key (*)
    ```

    * Note: 5-digit values separated by hyphens

    ## 💡 Example
    ....
    ```
    ProductID=11111-22222-33333-44444-55555
    ```
    ....

    ## 📋 Note
    ....
    If there is a mistake in the product ID value or format, an error occurs when the collected cloning image is deployed. Make sure to enter a valid product ID when editing the definition file.
    ....

  - For Windows Server 2008 or later

    Installation_folder\Agent\scw\SeparateSetting\ipadj\activation.dat

    In the [ActivationInfo] section, set the following parameters using a "parameter=value" syntax.
    Refer to the following table for details on each parameter.

Table 17.2 Structure of the Definition File

Format	Parameters	Value

KMS	.cmd.remotescript.
	1.params.kmscheck
	(Mandatory)
		KMS host search type.
		Select one of the following:
		
		- AUTO
		
		  Automatically searches KMS hosts.
		
		- MANUAL
		
		  Specify the KMS host.
		
		When "MANUAL" is selected, make sure to set .cmd.remotescript.
		1.params.kmsname.

	.cmd.remotescript. 1.params.kmsname	The host name (FQDN), computer name, or IP address of the KMS host.
	.cmd.remotescript. 1.params.kmsport	KMS host port number. The default is 1688.
MAK	.cmd.remotescript. 1.params.makkey (Mandatory)	MAK key.
Comm on	.cmd.remotescript. 1.params.ieproxy	Host name (FQDN) and the port number of the proxy server. The host name and port number are separated by a colon (":").
	.cmd.remotescript. 1.params.password	Administrator password. An existing password setting will be displayed as an encrypted character string. To edit the password, overwrite it with plain text, delete the "encrypted=yes" line, and perform the encryption procedure indicated in the example. If this parameter is not set, the password will be re-initialized.
	encrypted	The encryption status of the Administrator password. "yes" means that the password is encrypted. If this line exists, the rcxadm deployctl command does not operate.

Example

- With KMS (Automatic Search)

```
[ActivationInfo]
.cmd.remotescript.1.params.kmscheck=AUTO
.cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080
.cmd.remotescript.1.params.password=PASSWORD
```

- With KMS (Manual Settings)

```
[ActivationInfo]
.cmd.remotescript.1.params.kmscheck=MANUAL
.cmd.remotescript.1.params.kmsname=fujitsu.activation.com
.cmd.remotescript.1.params.kmsport=4971
.cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080
.cmd.remotescript.1.params.password=PASSWORD
```

- With MAK

```
[ActivationInfo]
.cmd.remotescript.1.params.makkey=11111-22222-33333-44444-55555
```

```
.cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080
.cmd.remotescript.1.params.password=PASSWORD
```

If the Administrator password has been changed, execute the following command. The password specified in the .cmd.remotescript.1.params.password parameter of the definition file is changed to the encrypted string, and the line "encrypted=yes" is added to indicate that the password is encrypted.
For details, refer to "5.6 rcxadm deployctl" in the "Reference Guide (Command) VE".

>"*Installation_folder***Agent\bin\rcxadm**" **deployctl passwd -encrypt** <RETURN>

- With MAK (Already Encrypted Password)

```
[ActivationInfo]
.cmd.remotescript.1.params.makkey=11111-22222-33333-44444-55555
.cmd.remotescript.1.params.ieproxy=proxy.activation.com:8080
.cmd.remotescript.1.params.password=xyz123456
encrypted=yes
```

Collecting Cloning Images

Use the following procedure to collect cloning images:

1. Place the target server into maintenance mode.

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

      The [Set Maintenance Mode] dialog is displayed.

   b. Click <OK>.

      The target server is placed into maintenance mode.

2. Stop all operations running on the source server.

   When a cloning image is collected, the source server is automatically restarted. Therefore, all operations running on the source server should be stopped before collecting the image.

   Cancel the settings in the following cases:

   - NIC redundancy has been configured for admin LANs and public LANs (*)

   - Tagged VLANs have been configured on NICs

   * Note: However, there is no need to cancel public LAN redundancy settings made via the network parameter auto-configuration function.

   The following settings are disabled during cloning image collection, which may result in services failing to start on server startup. To avoid this, automatic startup should be disabled for any service that depends on the following settings.

   - Hostname

   - IP address and subnet mask for the admin LAN

   - Default gateway for the admin LAN

🖙 Note

When using SUSE Linux Enterprise Server, it is necessary to configure the managed server so that only the NIC used for the admin LAN is active when the server is started. For details on how to modify the configuration, refer to the operating system manual. If this procedure is not performed, startup of network interfaces will take time, and errors may occur during the process.

3. Collect a cloning image.

   a. In the ROR console server resource tree, right-click the physical OS of the source server and select [Cloning]-[Collect] from the popup menu.
   The [Collect a Cloning Image] dialog is displayed.

   b. Perform the following settings:

   Cloning Image Name

   Enter a name to identify the collected cloning image.

   New
   When creating a new cloning image, select [New] and enter a new cloning image name.
   For a cloning image name, enter a character string beginning with an alphabetic character and containing up to 32 alphanumeric characters and underscores ("_").

   Update
   When updating an existing cloning image, select [Update] and select a cloning image from the list.
   Cloning images with the same name can be saved up until the maximum number of image versions.
   If the selected cloning image has already reached this limit, it is necessary to delete one of its existing versions in order to create a new cloning image. This can be done directly in this dialog by selecting the version to be deleted from the displayed list.
   The selected version will be automatically deleted when collection of the new cloning image completes.
   The maximum number of image versions is three by default.
   This setting can be changed by following the instructions given in "8.4 Changing the Maximum Number of Cloning Image Versions".

   Comment (Optional)

   Enter a comment that identifies the cloning image.
   Up to 128 characters other than percent signs ("%"), back slashes ("\"), double quotes ("), and line feed characters can be specified.
   If [Update] was selected for the [Cloning Image Name] option, the comment of the most recent image version is displayed.
   If no comment is specified, a hyphen ("-") will be displayed in the ROR console.

   It is recommended to enter comments with information such as hardware configuration (server model, disk size, and number of network interfaces), software configuration (names of installed software and applied patches), and the status of network parameter auto-configuration function.

   [Release Maintenance Mode after collection] checkbox

   Enable this option to automatically release the source server from maintenance mode after image collection and maintenance work.
   If this option disabled, maintenance mode should be released manually after collecting the cloning image.

   c. Click <OK>.

   The process of collecting the cloning image starts.
   The process status can be checked in the Recent Operations area of the ROR console.
   Clicking <Cancel> in the Recent Operations area displays a confirmation dialog and stops the process.

4. Restart applications on the source server.

   Restore the settings of any service whose startup settings were changed in step 2 and start these services.

   Restore the settings for the following cases:

   - NIC redundancy for admin LANs and public LANs has been released

   - The settings of tagged VLANs for NICs have been released

   Check that applications are running properly on the source server.

5. Release the source server from maintenance mode.

   This step is not required if the [Release Maintenance Mode after collection] checkbox was enabled in the [Collect a Cloning Image] dialog.

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

The [Release Maintenance Mode] dialog is displayed.

b. Click <OK>.

The target server is released from maintenance mode.

- While a cloning image is being collected, no other operations can be performed on that image or other versions of that image (images sharing the same image name).

- Communication errors between the admin and source servers (resulting in an image collection failure or an [unknown] status on the source server) may be caused by improper use of the network parameter auto-configuration function (described in "17.6 Network Parameter Auto-Configuration for Cloning Images").

  - Auto-configuration settings were made for the admin LAN

  - Auto-configuration settings were made for the public LAN using IP addresses contained within the admin LAN subnet range

Log in to the source server and check for the presence of such settings in the definition file for the network parameter auto-configuration function.
If incorrect settings were made, perform the following operations to fix communication errors.

  - Fix network settings on destination servers

    Run the rcxadm lanctl unset command described in "17.6.3 Clearing Settings" to reset network settings to their original values.

    If the admin LAN IP address is not set on the source server, set it manually to restore communications between the admin server and the source server.

  - Re-collect the cloning image

    Correct any errors found in the source server's network parameter auto-configuration function definition file and re-collect the cloning image from the source server.
    Delete any cloning image that was collected with incorrect network parameters.

17.3 Deploying

Once collected, cloning images can be deployed to one or more destination servers.

Cloning images collected from the source server can only be deployed to destination servers which satisfy all of the following conditions:

- Destination servers should be in either "normal", "warning", "unknown", or "stop" status.

- Destination servers should have been placed into maintenance mode.

- Destination servers should be of the same model as the source server.

- I/O virtualization should be used, when destination servers are spare servers.

Cloning images cannot be deployed to managed servers where VM hosts or VM guests are running.

Preparations

- If the managed server has the following configuration, configure the target disk of image operation before deploying cloning images.

  - Local boot with a SAN data environment

    For the configuration procedure, refer to "9.1.13 Changing Target Disks of Image Operations".

- When the configurations of managed servers are as below, execute the following commands before deploying cloning images.

  - When using the Red Hat Enterprise Linux 6 ext4 file system, and one of the following conditions is met

    - In a SAN boot environment using HBA address rename

    - When using a rack mount or tower server and the server is registered with "Disable" of "Association with server management software (ServerView)" is selected

[Windows Manager]

> *Installation_folder***SVROR\Manager\bin\rcxadm server set -name** *physical server* **-attr bootagt=winpe**
> <RETURN>

[Linux Manager]

#/opt/FJSVrcvmr/bin/rcxadm server set -name *physical server* **-attr bootagt=winpe** <RETURN>

- In a SAN boot environment using HBA address rename, and the following model

- PRIMERGY BX960 S1

[Windows Manager]

> *Installation_folder***SVROR\Manager\bin\rcxadm server set -name** *physical server* **-attr bootagt=winpe**
> <RETURN>

[Linux Manager]

#/opt/FJSVrcvmr/bin/rcxadm server set -name *physical server* **-attr bootagt=winpe** <RETURN>

If the above command has not been executed on the server from which the cloning image is being collected, the cloning image may not be collected correctly. Delete that cloning image and then redo the cloning image collection.

- It is recommended to back up destination servers before deploying cloning images, as this will simplify the recovery procedure in case of the deployed cloning image is faulty.

For details on backing up, refer to "16.2 Backup".

📝 Note
. . . .

- Cloning images cannot be deployed to servers that have been set up as spare servers for other managed servers, when not using I/O virtualization. Cancel any such settings before deploying a cloning image.

- When deploying cloning images to servers for which the target disks for image operations have been specified, deploy to one server at a time.
  If cloning images are deployed without configuring the target disk for image operations, data may be overwritten on an unintended disk.

- VLAN settings (on adjacent LAN switch ports) cannot be deployed during server cloning. LAN switch VLAN settings should be set up before deploying a cloning image.
  For details on how to configure VLAN settings on LAN switches, refer to "7.3.4 Configuring VLANs on LAN Switch Blades".

- When deploying a cloning image back to its source server, the source server should be backed up before deployment.

  For details on backing up, refer to "16.2 Backup".

  If the deployed cloning image is faulty and causes deployment errors, use the following procedure to collect a new cloning image.

  1. Restore the system image that was backed up before cloning image deployment.

  2. Fix any incorrect settings on the source server

  3. Collect a new cloning image

  4. Delete the faulty cloning image

- When deploying cloning images to multiple managed servers, if the managed servers belong to different subnets, cloning images cannot be deployed.

- When using PRIMEQUEST servers, cloning images cannot be deployed to partitions for which UEFI has been set.
  When collecting and deploying cloning images, configure the BIOS settings and boot option settings after changing to Legacy boot.
  For details on how to change boot options, refer to "9.1.10 Changing Boot Options".

- When using local disks as system disks, and iSCSI storage as data disks, refer to the advisory notes described in "Table 8.1 Supported Storage Configurations" in "8.1.1 Storage Configuration" in the "Design Guide VE".

. . . .

Deploying a Cloning Image

Use the following procedure to deploy a cloning image to one or more destination servers:

1. Place the destination server(s) into maintenance mode (only for agent-registered servers).

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

       The [Set Maintenance Mode] dialog is displayed.

    b. Click <OK>.

       The target server is placed into maintenance mode.

2. Deploy a cloning image.

    - Deploying a cloning image to a single destination server

       a. In the ROR console server resource tree, right-click the destination server (or its physical OS) and select [Cloning]-[Deploy] from the popup menu.

          The [Deploy a Cloning Image] dialog is displayed.
          The available cloning images are displayed.
          Only cloning images that have been collected from a server of the same model as the destination server are available for deployment.

       b. Select the cloning image to deploy, and set the following items.

          Server name after deployment
          Enter the name of the server to which the cloning image is to be deployed.
          By default, the physical OS name is entered if the physical OS is registered. If the physical OS is not registered, the physical server name is entered.

          [Windows]
          A string composed of up to 63 alphanumeric characters, underscores, ("_"), and hyphens, ("-").
          The string cannot be composed solely of numbers.

          [Linux]
          A string composed of up to 64 alphanumeric characters, and the following symbols:

          "%", "+", ",", "-", ".", "/", ":", "=", "@", "_", "~"

          Note

. . . .

          When using SUSE Linux Enterprise Server, it is not possible to configure server names that include periods (".") for the post-deployment server names of cloning images.

. . . .

          Information

. . . .

          Since the entered server name is also used as the hostname of its corresponding destination server, it is recommended to use only characters defined in RFC (Request For Comments) 952:

          - Alphanumeric characters

          - Hyphens, ("-")

          - Periods, (".") [Linux]

. . . .

[Release from Maintenance Mode after deployment] checkbox
Enable this option to automatically release the destination server from maintenance mode after cloning image deployment.
If this option disabled, maintenance mode should be released manually after collecting the cloning image.

c. Click <OK>.

The cloning image deployment process starts.
The process status can be checked in the Recent Operations area of the ROR console.
Clicking <Cancel> in the Recent Operations area displays a confirmation dialog and stops the process.

🔔 Note

Please note that canceling the deployment of a cloning image does not restore the destination server to the state before the deployment took place.

- Deploying a cloning image to multiple destination servers

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

    A list of cloning images is displayed under the cloning image list.

    b. Right-click the cloning image to deploy and select [Deploy] from the popup menu.

    The [Deploy a Cloning Image] dialog is displayed.
    A server that can be deployed is displayed.

    c. Check the checkbox of the server to deploy a cloning image to, and set the following items:

    [Release from Maintenance Mode after deployment] checkbox
    Enable this option to automatically release the destination server from maintenance mode after cloning image deployment.
    If this option disabled, maintenance mode should be released manually after collecting the cloning image.
    The [Server Name] column displays the names of each destination servers.
    By default, server names (computer name or hostname) or physical server names are displayed.
    The names specified in this column will be assigned to destination servers as their computer names (for Windows systems) or system node names (for Linux systems).

    Those names can be changed using the following procedure.

    1. Double-click the [Server name after deployment] cell of a server.

    The [Server name after deployment] cell becomes editable.

    2. Enter a new server name.

    [Windows]
    A string composed of up to 63 alphanumeric characters, underscores, ("_"), and hyphens, ("-").
    The string cannot be composed solely of numbers.

    [Linux]
    A string composed of up to 64 alphanumeric characters, and the following symbols:

    "%", "+", ",", "-", ".", "/", ":", "=", "@", "_", "~"

📖 Information

Since the entered server name is also used as the hostname of its corresponding destination server, it is recommended to use only characters defined in RFC (Request For Comments) 952:

- Alphanumeric characters

- Hyphens, ("-")

- Periods, (".") [Linux]

d. Click <OK>.

The cloning image deployment process starts.
The process status can be checked in the Recent Operations area of the ROR console.
Clicking <Cancel> in the Recent Operations area displays a confirmation dialog and stops the process.

⬇ Note

When this process is canceled, cloning image deployment to all destination servers is canceled.

Please note that canceling the deployment of a cloning image does not restore the destination server to the state before the deployment took place.

3. Restart applications on the destination server(s).

Perform the following settings if necessary:

- The settings of NIC redundancy for admin LANs and public LANs

- The settings of tagged VLANs for NICs

After deployment, destination servers are set to use the admin server as their default gateway.
Reconfigure such network settings if necessary. Check that applications are running properly on destination servers.
At this point, if an application is still using the source server's hostname or IP address (e.g. within application-specific settings or configuration file), manually update such settings with the destination server values.

⬇ Note

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

4. Release maintenance mode.

This step is not required if the [Release from Maintenance Mode after deployment] checkbox was enabled in the [Deploy a Cloning Image] dialog.

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

The [Release Maintenance Mode] dialog is displayed.

b. Click <OK>.

The target server is released from maintenance mode.

⬇ Note

- When deploying a cloning image that was collected from a Windows server, the following information is reset on each destination server. This is a result of the execution of Microsoft's System Preparation (Sysprep) tool.
  If necessary, restore the following settings to their original values after the cloning image has been deployed:

  - Desktop icons and shortcuts

  - Drive mappings

  - The "Startup and Recovery" settings accessed from the [Advanced] tab of the [System Properties] window

  - Virtual memory settings

  - TCP/IP-related settings

  - The "What country/region are you in now?" settings in the locations defined in the [Location Information] window

  - Disk quota settings

  - Storage Provider settings

- Microsoft Internet Explorer settings (RSS feeds subscription information, information stored by the Autocomplete function, saved passwords)

- Microsoft Outlook Express settings (mail/directory server passwords)

- Network card driver settings (drivers without a digital signature should be replaced by the latest updated drivers with a digital signature)

- Access rights to the '\Documents and Settings\Default User' folder

- While a cloning image is being deployed, collection, deployment, and deletion cannot be performed simultaneously on the cloning images with the same name.

- If a cloning image is deployed to a system with a larger disk capacity than the disk space required for the cloning image, any excessive disk space becomes unused disk space. This unused disk space can be used for other purposes.

- Destination servers are rebooted several times during cloning image deployment. Make sure that deployment has completed before restarting operations and making further settings.

- The number of reboots during deployment increases when using the HBA address rename function.

- Communication errors between the admin and destination servers (resulting in an image deployment failure or an [unknown] status on the destination server) may be caused by improper use of the network parameter auto-configuration function (described in "17.6 Network Parameter Auto-Configuration for Cloning Images"). Examples of improper use are given below.

    - Auto-configuration settings were made for the admin LAN

    - Auto-configuration settings were made for the public LAN using IP addresses contained within the admin LAN subnet range

Log in to the destination servers on which errors occurred and check for the presence of such settings in the definition file for the network parameter auto-configuration function.
If incorrect settings were made, perform the following operations to fix communication errors.

    - Fix network settings on destination servers

        - If the source and destination servers are the same

        Restore the system images backed up before cloning image deployment.

        - If the destination server is different from the source server

        Run the rcxadm lanctl unset command described in "17.6.3 Clearing Settings" to reset network settings to their original values.

If the admin LAN IP address is not set on the source server, set it manually to restore communications between the admin server and the source server.

    - Re-collect the cloning image

    Correct any errors found in the definition file for the network parameter auto-configuration function and re-collect the cloning image.
    Re-deploy the cloning image to the destination servers for which deployment failed.
    Delete any cloning image that failed to deploy.

- If activation of Windows Server 2008 or later failed during deployment, message number 47233 is displayed.
This message indicates that deployment of Windows Server 2008 or later completed, but activation failed.
For details on the appropriate corrective action, refer to "Message number 47233" in "Messages".

- When a cloning image is deployed to multiple servers, it may be necessary to enable IGMP snooping on admin LAN switches. If IGMP snooping is not enabled, transfer performance may deteriorate when ports with different speeds co-exist in the same network, or multiple image operations are run simultaneously.

17.4 Viewing

This section explains how to display collected cloning images.

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

A list of cloning images is displayed under the cloning image list.

Use this list to manage the cloning images used by Resource Orchestrator.

Figure 17.1 Cloning Image List

System Image List	Cloning Image List			
			I◀ ◀ 1 /1 ▶ ▶I	
Cloning Image Name	Version	Collection Date	OS	Comments
BX900_1_clone	1	2012-10-22 10:51:00	Microsoft Windows Server 2003	-

For details on the "Cloning Image List", refer to "A.8 [Image List] Tab".

17.5 Deleting

This section explains how to delete a cloning image.

Use the following procedure to delete cloning images:

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

   A list of cloning images is displayed under the cloning image list.

2. In this list, right-click the name of the cloning image to delete and select [Delete] from the popup menu.

   The confirmation dialog is displayed.

3. Click <OK>.

   The selected cloning image is deleted.

📖 Note

....
While the cloning image is being deleted, no operations can be performed on other versions of the same cloning image (images that share the same image name).
....

17.6 Network Parameter Auto-Configuration for Cloning Images

This section explains the network parameter auto-configuration function for cloning images.

Defining public LAN network parameters for each managed server before collecting cloning images enables automatic configuration of the cloned servers' public LAN network interfaces when later deploying those cloning images.
This speeds up the deployment of multiple managed servers, as public LAN IP addresses no longer need to be manually and separately configured on each cloned server.

Perform the following settings:

- When not Using LAN Redundancy

    - IP address

    - Subnet mask

- When Using LAN Redundancy [Linux]

  - The "NIC switching mode (Physical IP address takeover function)" of PRIMECLUSTER Global Link Services

Figure 17.2 Setup Procedure When Using the Network Parameter Auto-configuration Function
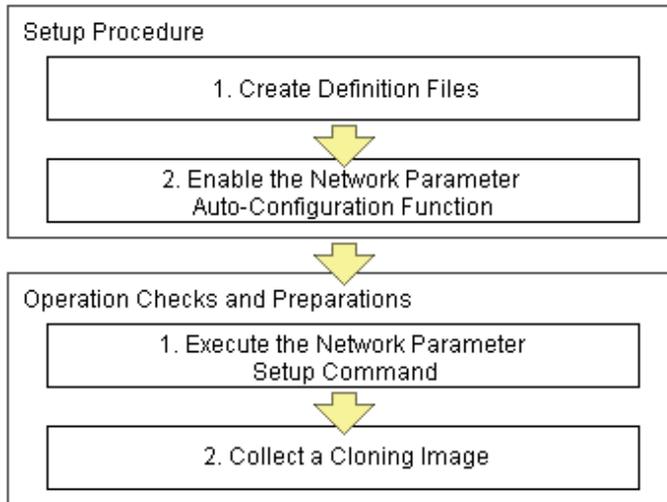
Note

[Physical Servers]

The network parameter auto-configuration function cannot be used on the admin LAN. If it is used, deployment commands may fail when deploying new servers may fail, or communication issues may occur during collection or deployment of cloning images.

[Windows]

- When the OS of the managed server is Windows Server 2012, this function is not supported.

- When Windows OS is installed on a PRIMERGY RX600 S6/RX200 S7/RX200 S8/RX300 S7/RX300 S8/RX2520 M1/RX2530 M1/RX2540 M1/RX4770 M1/BX920 S3/BX2560 M1/BX924 S3/BX924 S4, and the server is used as a managed server of Resource Orchestrator, if the automatic network parameter setting function of cloning is used, it is necessary to execute the following procedures.

  Perform the following procedure before setting network parameters through cloning image collection.

  It is not necessary to execute it again on managed servers on which this procedure has already been executed.

  1. As the network settings of managed servers may be changed when step 2 is performed, make a note of the current network settings.

  2. Execute Sysprep on the managed server.

     Refer to the manual of the OS for the method of starting Sysprep.

     Specify the following options when executing Sysprep.

     [System Cleanup Action]

     - Select "Enter System Out-of-Box Experience (OOBE)"

     - Check the "Generalize" checkbox.

     [Shutdown Option]

     - Select "Reboot"

  3. After Sysprep is executed, the OS of the managed server is rebooted, and then Mini setup of the OS is executed.

     Configure the OS following the instructions on the screen.

  4. Restore the network settings of the managed server referring to the information recorded in step 1.

[Linux]

When using LAN redundancy, cancel any network redundancy settings that were made on managed servers using PRIMECLUSTER Global Link Services before deploying new servers.

If not canceled, deployment commands may fail when deploying new servers.

Once the deployment of new servers has completed, redundancy network configurations (for the admin LAN or other networks) that are not handled by the network parameter auto-configuration feature should be set up manually.

PRIMECLUSTER Global Link Services cannot be used to enable admin LAN redundancy on servers running SUSE Linux Enterprise Server or Oracle Enterprise Linux operating systems.

Setup Procedure

Use the following procedure to set up network parameters for a public LAN:

P Point

Using a specific managed server (reference server) to collect and update cloning images is recommended in order to centrally manage the network parameters definition files.

1. **Definition File Settings**

   This section explains how to setup the following definition files.

   - FJSVrcx.conf

   - ipaddr.conf

   Create those definition files under the following folder on the reference server:

   [Windows]
   Installation_folder\Agent\etc\FJSVrcx.conf
   Installation_folder\Agent\etc\ipaddr.conf

   [Linux]
   /etc/FJSVrcx.conf
   /etc/opt/FJSVnrmp/lan/ipaddr.conf

   Sample configuration of the definition file (FJSVrcx.conf)

   ```
   admin_LAN=192.168.1.11
   hostname=node-A
   ```

   - admin_LAN

     Enter the IP address used by the reference server on the admin LAN.

   - hostname

     Enter the physical server name of the reference server.

   Format of the definition file (ipaddr.conf)

   The definition file is made up of the following entries:

   - One or more node entries

- One or more interface entries (with or without redundancy) under each node entry

Figure 17.3 Sample configuration of the definition file (ipaddr.conf)


```
NODE_NAME="node-A"

IF_NAME0="eth1"
IF_IPAD0="192.168.10.11"
IF_MASK0="255.255.255.0"

NODE_NAME="node-B"

VIF_NAME0="sha0"
VIF_IPAD0="192.168.20.11"
VIF_MASK0="255.255.255.0"
PRI_NAME0="eth2"
SCD_NAME0="eth3"
POL_ADDR0="192.168.20.100,192.168.20.200"
PAT_NAME0="sha1"
POL_HUBS0="ON"
```
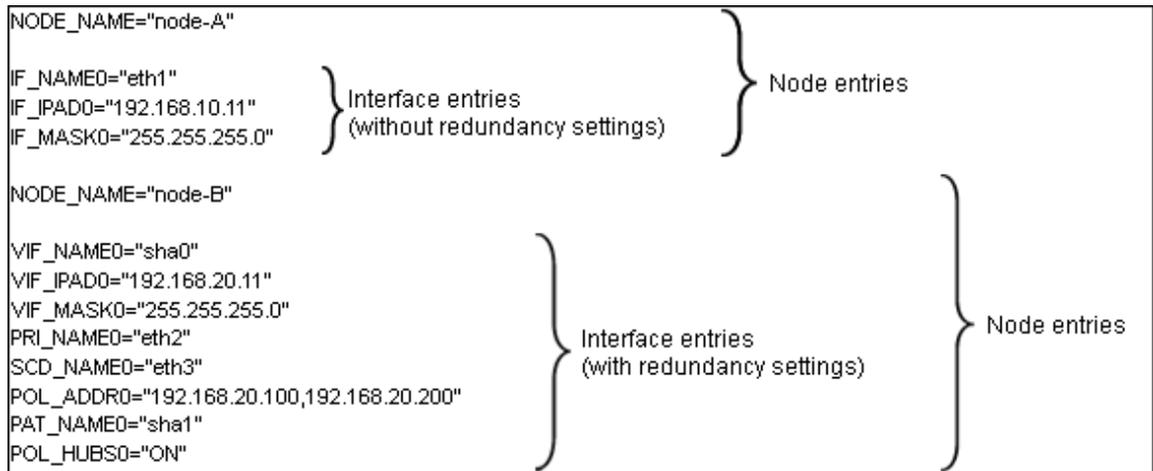
Refer to the following sample file for details of how to set the definition file (ipaddr.conf).

[Windows]
Installation_folder\Agent\etc\ipaddr.sample

[Linux]
/etc/opt/FJSVnrmp/lan/ipaddr.sample

🛈 Note

Blank spaces and comment lines (lines starting with a comment symbol (#) are ignored.

The expected content of each entry is explained below.

- Node Entries

The following table explains how to define each node entry.

Table 17.3 Node Entry Settings

Setting	Keyword	Expected Values:	Description
Managed server name	NODE_NAME	Physical server name	Physical server name that was set when registering the managed server.

🛈 Note

Specify additional entries for any node (server) that may be added in the future (one entry per server).

- Interface Entries (without Redundancy)

The following table explains how to define each interface entry.
Keywords for interface entries should be appended with a number between 0 and 99.

🛈 Note

The number appended to each entry's keyword should start with 0 and increase incrementally.

Table 17.4 Interface Entry Settings (without Redundancy)

Setting	Keyword	Expected Values:	Description
Interface name	IF_NAME	Interface name	Specify the interface name as displayed by the operating system. (*) Example [Windows] Local area connection 2 [Linux] eth$X$ (where X is an integer equal to or greater than 0)
IP address	IF_IPAD	IP address in xxx.xxx.xxx.xxx format	-
Subnet mask	IF_MASK	Subnet mask in xxx.xxx.xxx.xxx format	-

* Note: As Windows allows interface names to be changed, ensure that the names defined here match those displayed in Windows.

- Interface entries (with redundancy) [Linux]

The following table explains how to define each interface entry.
Keywords for interface entries should be appended with a number between 0 and 99.

This setting uses the "NIC switching mode (Physical IP address takeover function)" of the PRIMECLUSTER Global Link Services product, which requires a virtual interface set with its own IP address.

Within a same node entry, it is possible to define interface entries both with and without redundancy settings as long as interface names differ.

Note
. . . .

The number appended to each entry's keyword (including both entries with and without redundancy settings) should start with 0 and increase incrementally.
When there is a mixture of interfaces with and without redundancy, assign values in ascending order to the interfaces without redundancy as well.
. . . .

Interface entries with redundancy settings are only activated with Linux. With Windows, these interface entries will be ignored.

Table 17.5 Interface Entry Settings (with Redundancy)

Setting	Keyword	Expected Values:	Description
PRIMECLUSTER GLS virtual interface name	VIF_NAME	sha$X$	X is an integer between 0 and 255.
IP address specified for virtual interface	VIF_IPAD	IP address in xxx.xxx.xxx.xxx format	-
Subnet mask	VIF_MASK	Subnet mask in xxx.xxx.xxx.xxx format	-
Name of primary interface	PRI_NAME	Interface name (eth$X$)	X is an integer equal to or greater than 0. This setting specifies the primary interface

Setting	Keyword	Expected Values:	Description
			name when a pair of interface names exists. <Example> eth2
Name of secondary interface	SCD_NAME	Interface name (eth *Y*)	*Y* is an integer equal to or greater than 0. This setting specifies the secondary interface name when a pair of interface names exists. <Example> eth3
IP address of monitored destination	POL_ADDR	IP address in xxx.xxx.xxx.xxx format	Up to two IP addresses can be specified, separated by a comma. When hub-to-hub monitoring is to be performed, specify two monitored destinations. Hub-to-hub monitoring will not be performed if only one destination is specified. In this case, the value specified in POL_HUBS (whether to perform hub-to-hub monitoring) will not be referenced.
Virtual interface name for standby patrol	PAT_NAME	sha *Y*	*Y* is an integer between 0 and 255. Specify a name that is different from the virtual interface name. Do not set anything unless standby patrolling is set.
Hub-to-hub monitoring ON/OFF	POL_HUBS	ON/OFF	Specify "ON" to enable hub-to-hub monitoring, or "OFF" otherwise. This setting is valid only if two monitoring destinations are specified. If only one monitoring destination is specified, this setting is disabled (set to "OFF").

Refer to the PRIMECLUSTER Global Link Services manual for details on each setting.

2. **Enable the Network Parameter Auto-Configuration Function**

Enable the network parameter auto-configuration function by executing the following command.
Execute this command from a managed server.

[Windows]

>"*Installation_folder***Agent\bin\rcxadm" lanctl enable** <RETURN>

[Linux]

/opt/FJSVrcxat/bin/rcxadm lanctl enable <RETURN>

For details on the command, refer to "5.9 rcxadm lanctl" in the "Reference Guide (Command) VE".

17.6.1 Operation Checks and Preparations

Use the following procedure to actually apply the definition file's settings on the reference server and prepare a cloning image to be used for further server deployments. The definition file's settings applied from the definition file should be validated before image collection by checking the reference server's behavior and configuration.

1. **Manually Execute the Network Parameter Setup Command**

   Execute the network parameter configuration command on the reference server holding the prepared definition file and check that the defined settings are applied correctly.

   Executing the Command

   Before collecting the cloning image, run the following command to apply the definition file and verify that the defined settings are actually reflected on the reference server. This command also activates network parameter auto-configuration for any cloning image subsequently collected. Once this command has been executed, the network configuration that was described in the definition file will be performed automatically.

   [Windows]

   > **"***Installation_folder***\Agent\bin\rcxadm" lanctl set** <RETURN>

   [Linux]

   # **/opt/FJSVrcxat/bin/rcxadm lanctl set**<RETURN>

   For details on the command, refer to "5.9 rcxadm lanctl" in the "Reference Guide (Command) VE".

   Validating settings (without LAN redundancy)

   Use a command provided by the operating system (ipconfig for Windows and ifconfig for Linux) to confirm that network interface settings (without redundancy) were correctly applied.

   Validating settings (with LAN redundancy) [Linux]

   Use the following commands to confirm that network interface settings (with redundancy) were correctly applied.

   - Using the /opt/FJSVhanet/usr/sbin/dsphanet Command

   ```
   # /opt/FJSVhanet/usr/sbin/dsphanet <RETURN>
   [IPv4,Patrol]
    Name         Status   Mode CL   Device
   +---------+--------+----+----+-----------------------------------------------+
    sha0        Active    e   OFF  eth0(ON),eth1(OFF)
    sha2        Active    p   OFF  sha0(ON)
    sha1        Active    e   OFF  eth2(ON),eth3(OFF)
   [IPv6]
    Name         Status   Mode CL   Device
   +---------+--------+----+----+-----------------------------------------------+
   ```

   Items to confirm

   - The status of the virtual interface must be "Active".

   - When the standby patrol function is used ("p" mode), the status of the virtual interface set in standby patrol ("sha2" in the output example above) must be "Active".

   - Using the /opt/FJSVhanet/usr/sbin/dsppoll Command

   ```
   # /opt/FJSVhanet/usr/sbin/dsppoll <RETURN>

    Polling Status    =  ON
    interval(idle)    =   5( 60)
    times             =   5
    repair_time       =   5
    link detection    =  NO
    FAILOVER Status   = YES

    Status  Name  Mode Primary Target/Secondary Target          HUB-HUB
    +------+------+----+----------------------------------------+-------+
   ```

```
ON    sha0    e    192.168.1.101(ON)/192.168.1.102(WAIT)         ACTIVE
ON    sha1    e    192.168.1.101(ON)/192.168.1.102(WAIT)         ACTIVE
```

Items to confirm

- The monitoring status (Polling Status) must be "ON" (monitoring in progress)

- If one monitoring destination is specified, the status of that destination (Primary Target) must be "ON" (monitoring in progress)

- If two monitoring destinations are specified, the status of the primary destination (Primary Target) must be "ON" (monitoring in progress) and the status of the secondary destination (Secondary Target) must be "WAIT" (on standby)

- When HUB-HUB monitoring is set to "ON", the status (HUB-HUB) must be "ACTIVE" (monitoring in progress)

If the interface settings have not been configured correctly, clear the settings using the rcxadm lanctl unset command, and then correct the definition file before executing the rcxadm lanctl set command again.
If anything (including user-defined checks) does not turn out as expected even though the settings were applied correctly, check the network connections and the monitoring target, and take appropriate action.

Another test is to either deactivate the port on the LAN switch blade corresponding to the network interface where communications are actually being performed, or disconnect the cable from an external port on the LAN switch blade, to check whether the spare network interface automatically takes over communication. If the standby patrol function is enabled, check the port status or check that the status of the standby network interface changes to "WAIT" after reconnecting the cable.

2. **Collect a Cloning Image**

Collect a cloning image from the managed server checked in step 1.

For details on how to collect cloning images, refer to "17.2 Collecting".

📝 **Note**
. . . .

[Linux]
When a cloning image is collected, any LAN redundancy settings on managed servers are canceled, and only network parameters for the defined public LAN are set up again when collection completes.
If LAN redundancy has been manually set up, set the LAN redundancy settings again manually.
. . . .

17.6.2 Maintenance

If the network parameter auto-configuration function fails, an error message is output together with error details to the following file:

[Windows]
Installation_folder\Agent\var\log\error_lan.log

[Linux]
/var/opt/FJSVnrmp/logs/error_lan.log

For details on meanings of message and the appropriate corrective actions, refer to "Messages".

The file size limit is 32 KB and only one version is maintained. Old logs will have the extension ".old" appended to the file name and remain in the same directory.

17.6.3 Clearing Settings

This section explains how to disable the network parameter auto-configuration function and clear the settings that were applied.

Disabling the Network Parameter Auto-Configuration Function

The network parameter auto-configuration function of the cloning image being collected can be disabled by executing the following command.
After disabling it, collect a new cloning image to update the existing image.

[Windows]

> ```
> >"Installation_folder\Agent\bin\rcxadm" lanctl disable <RETURN>
> ```

[Linux]

> ```
> # /opt/FJSVrcxat/bin/rcxadm lanctl disable <RETURN>
> ```

Clearing Network Parameter Settings

If network settings must be added or changed due to the addition of a new server, first clear the existing settings. Clear the network parameter settings of managed server by executing the following command:

[Windows]

> ```
> >"Installation_folder\Agent\bin\rcxadm" lanctl unset <RETURN>
> ```

[Linux]

> ```
> # /opt/FJSVrcxat/bin/rcxadm lanctl unset <RETURN>
> ```

For details on the command, refer to "5.9 rcxadm lanctl" in the "Reference Guide (Command) VE".

🖘 Note

. . . .

[Physical Servers]
Network parameter settings for interfaces not designated in the definition file cannot be released.

[Linux]
When this command is executed, any LAN redundancy settings for managed servers are unset. If LAN redundancy has been set up for the admin LAN, set the LAN redundancy settings again manually.

. . . .

17.6.4 Modifying the Operating Environment

Use the following procedures to modify the operating environment.

Deploying New Managed Servers with Automated Public LAN Configuration

Use the following procedure to add new managed servers and automate their public LAN settings using the network parameter auto-configuration function:

1. Register the newly added servers.

2. Perform the following procedure on a reference server chosen between already running servers:

    a. Clearing Network Parameter Settings

       Execute the rcxadm lanctl unset command to clear the network parameters configuration.

    b. Editing the definition file

       Set up a node entry in the definition file (ipaddr.conf) with the server name, interface entries, and other information for the server to be added.

    c. Manually execute network parameter settings

       Execute the rcxadm lanctl set command to apply the network parameters and ensure that the resulted configuration (induced from the definition file) is correct.

    d. Collect the cloning image again.

3. Deploy the collected cloning image to the newly added servers.

Modifying Managed Server Settings

If network settings must be modified due to the addition or removal a public LAN, or a change of IP address, perform the following on an arbitrary reference server (chosen between already running servers).

1. Execute the rcxadm lanctl unset command to clear the network parameters configuration.

2. Edit the definition file to add, modify, or delete network parameters.

3. Execute the rcxadm lanctl set command to apply the network parameters and ensure that the resulted configuration (induced from the definition file) is correct.

4. Collect a new cloning image from the reference server.

Chapter 18 Server Switchover Settings

This chapter explains how to use server switchover settings and automatically recover from server failures.

18.1 Status Display

Current recovery settings can be confirmed by selecting a physical OS or VM host in the server resource tree of the ROR console and from the spare server settings displayed in the [Resource Details] tab.

The following information is displayed:

Primary server

　　Displays the name of the physical server that will be replaced when server switchover occurs.

Active server

　　Displays the name of the physical server that is currently running.

Server switchover method

　　Displays the specified server switchover method.

Automatic server recovery

　　Shows whether automatic server recovery is enabled or not.

Network switchover

　　Shows whether network settings will be automatically adjusted during server switchover.

Spare server

　　Displays the name of the physical server that will replace the current active server when server switchover occurs.
　　More than one spare server will be displayed if more than one has been specified.

[OVM for SPARC]
While in OVM for SPARC environment, you can confirm the save status of OVM configuration information's XML file from the VM host information in [resource details] tab.
Please reference the details of XML save status of VM host information's OVM configuration information in "A.6.3 Property of the Physics OS, VM host or VM guest".

18.2 Settings for Server Switchover

Use the following procedure to configure server switchover settings:

When using local disks as system disks, and iSCSI storage as data disks, refer to the advisory notes described in "Table 8.1 Supported Storage Configurations" in "8.1.1 Storage Configuration" in the "Design Guide VE".

1. In the ROR console server resource tree, right-click a server (or a physical OS or VM host on the server) and select [Modify]-[Spare Server Settings] from the popup menu.

   The [Spare Server Settings] dialog is displayed.

2. Perform the following settings:

   Spare server

   　　From the spare server list, select the checkbox in the [Select] column of the server that is to be used as the spare server.
   　　One or more spare servers can be specified, including spare servers from different chassis.

   　　If more than one is specified, an unused spare server will be selected from the list of available candidates when a server switchover occurs.

....

For SPARC Enterprise servers or the FUJITSU M10, only the storage affinity switchover method can be selected. In the storage affinity switchover method, configuration of WWN information is necessary. For how to configure WWN information, refer to "10.1 Configuring WWN Settings for ETERNUS SF Storage Cruiser Integration".

When using the storage affinity switchover method, it is necessary to configure the target CA so that it matches the WWPN value in the access path settings of the primary server.

Servers that have agents registered can be used as spare servers. When using a server on which an agent is registered as a spare server, the server must meet one of the following conditions:

- When the AffinityGroup value is different from the value of the primary server

- When agents are not registered on ETERNUS SF Storage Cruiser

ETERNUS SF Storage Cruiser cannot perform event monitoring of spare servers. For details on event monitoring, refer to the "ETERNUS SF Storage Cruiser Event Guide".

In server configurations using I/O virtualization, servers on which server OSs are operating can be used for spare servers.

- Register the agent

- I/O virtualization

- Server switchover settings

To change a server with the above settings, which does not use I/O virtualization, to a spare server, delete the server and then re-register it. Note that if the server is registered while it is running, an agent will be registered automatically. For this reason, it should be registered while it is stopped.

To delete a spare server that has been added, refer to "18.4 Canceling Server Switchover Settings".

When using the storage affinity switchover method, after switchover to spare servers, if failback is performed the storage settings for spare servers will be deleted. For how to restore storage settings, refer to "4.2 Switchover" and "4.3 Post-Switchover Operations" in the "Operation Guide VE".

....

[Local-boot with SAN data (Backup and restore method)] checkbox

This checkbox is available only if the WWN of the servers selected from the server resource tree are being virtualized using HBA address rename or VIOM.
The checkbox is unavailable if the WWN is not being virtualized or boot configuration is set for a VIOM server profile.
Select this option for servers that boot from a local disk while using SAN storage to store data. If selected, spare server(s) will also be able to boot locally and access the same SAN storage data space after a switchover.
Do not select this option for servers that boot from a SAN disk.

[Apply network settings when the server is switched over] checkbox

Select this option to enable automatic adjustment of VLAN ID or port group settings during a server switchover. If selected, the internal LAN switch ports connected to the spare server will be set with the same VLAN settings as those of the ports connected to the primary server.
This option is selected by default.
This feature is available only for PRIMERGY BX blade servers.
When VIOM is used, it is available only when a LAN switch is in switch mode or end-host mode.

 📖 Note

....

- Do not select this option if VLAN settings are to be manually adjusted from the LAN switch's management interface (either graphical or command-line interface).

- Do not select this option for internal ports of LAN switches when Automatic Migration of Port Profile (AMPP) has been configured.

- For LAN switch blades operating in Converged Fabric mode or a LAN switch blade PY CB 10Gb FEX Nexus B22, VLAN settings on LAN switches are not configured even if this checkbox is checked.

....

[Automatically switch over when a server fault is detected] checkbox

Select this option to enable Auto-Recovery.
Server failures are detected when the server's status changes to [error] or [fatal] and its operating system stops functioning.
Do not select this option if primary servers are to be manually switched over.
This option is selected by default.

[Power off forced when the server is switched over] checkbox

Check this checkbox if the spare server is to be turned off forcibly when the spare server in started before switchover takes place.
When shutting down the spare server, clear this checkbox.
This option is not selected by default.

[Switchover to server where VM guest exists] checkbox

When a spare server is a VM host, check this checkbox if switching to a spare server in which the VM host contains a VM guest.
When not switching to a VM host which contains a VM guest, clear this checkbox.
This option is not selected by default.

When "Manager" server role has been set in a VM guest, it will be expected from spare server even though it has been checked in the checkbox.

3. Click <OK>.

   The server switchover settings are configured.

4. Set the boot agent for the spare server.

   If the primary server is in a configuration with a local boot environment, execute the following command on all servers that have been set as spare servers.

   - When using the ext4 file system of Red Hat Enterprise Linux 6, and registering the server by selecting "Disable" in "Association with server management software (ServerView)" for using rack mount or tower servers

   [Windows Manager]

   ```
   >Installation_folder\SVROR\Manager\bin\rcxadm server set -name physical server -attr bootagt=winpe
   <RETURN>
   ```

   [Linux Manager]

   ```
   #/opt/FJSVrcvmr/bin/rcxadm server set -name physical server -attr bootagt=winpe <RETURN>
   ```

   - In a SAN boot environment using HBA address rename, and the following model

     - PRIMERGY BX960 S1

   [Windows Manager]

   ```
   >Installation_folder\SVROR\Manager\bin\rcxadm server set -name physical server -attr bootagt=winpe
   <RETURN>
   ```

   [Linux Manager]

   ```
   #/opt/FJSVrcvmr/bin/rcxadm server set -name physical server -attr bootagt=winpe <RETURN>
   ```

5. Configure the image operation target disk for the spare server.

   If the primary server is a local boot environment with the following configuration, configure the target disk of image operations.

   - For a local boot and SAN data environment

   For the configuration procedure, refer to "9.1.13 Changing Target Disks of Image Operations".

Point

. . . .

The conditions specified in "9.3 Server Switchover Conditions" in the "Setup Guide VE" must be satisfied for server switchover to be executed correctly.

Once settings are complete, perform switchover and failback on each spare server that has been set up to verify that these operations can be executed correctly.

A function to check the server operations after auto-recovery has been activated (by causing a dummy failure to occur) is not provided with Resource Orchestrator.

The testing method for automatic server recovery is the same as for manual server switchover. Make sure the server is operational by performing the manual server switchover test.

For details on switchover and failback methods, refer to "Chapter 4 Server Switchover" in the "Operation Guide VE".

. . . .

Note

. . . .

For servers other than those using I/O virtualization and those with WWN settings registered, the following checks will not be enabled.

- [Power off forced when the server is switched over] checkbox

- [Switchover to server where VM guest exists] checkbox

. . . .

[VMware] [Hyper-V] [Xen] [Citrix Xen] [KVM] [Solaris Zones] [OVM for x86 3.2] [OVM for SPARC]

The automatic startup of VM guests after the switchover of their VM host depends on their virtual machines' startup configuration within the server virtualization software used.

For details, refer to the manual of server virtualization software.

Depending on the server virtualization product used, a newly created VM guest may require some reconfiguration before running a server switchover.

Refer to "D.2 Configuration Requirements" in the "Design Guide VE" for details on such settings.

[Solaris] [Solaris Zone]

While ZFS storage pool has been used in Solaris, Solaris zone environment, it may be necessary to create a definition file.

For details, refer to "18.5.1 Definition File of ZFS Storage Pool [Solaris] [Solaris Zone]" and "18.5.2 Definition File of ZFS Storage Pool Information [Solaris] [Solaris Zone] [OVM for SPARC]".

[OVM for SPARC]

It may be necessary to create a setting and definition file in OVM for SPARC environment. For details, refer to "18.5 Definition File of Server Switchover".

18.3 Changing Server Switchover Settings

The procedure used to change server switchover settings is the same as that described in "18.2 Settings for Server Switchover".
For details, refer to "Chapter 18 Server Switchover Settings".

18.4 Canceling Server Switchover Settings

Use the following procedure to cancel server switchover settings.

1. In the ROR console server resource tree, right-click a server (or a physical OS or VM host on the server) and select [Modify]-[Spare Server Settings] from the popup menu.

   The [Spare Server Settings] dialog is displayed.

2. Clear the checkbox in the [Select] column for the desired spare server.

3. Click <OK>.

   The selected spare server is no longer set as a spare server.

18.5 Definition File of Server Switchover

This section explains definition files for server switchover.

18.5.1 Definition File of ZFS Storage Pool [Solaris] [Solaris Zone]

While building Solaris zone environment, and creating zone in ZFS storage pool, the ZFS storage pool importing in target of server switchover, and the status of zone on ZFS storage pool both can be changed after server switching over.
When changing the status, create the following definition files:

Use the zpool command to check ZFS storage pools.
Use the zoneadm command to check zones.
For details, refer to the manuals provided by Oracle.

Storage Location of the Definition File

> [Windows Manager]
> *Installation_folder*\SVROR\Manager\etc\customize_data
>
> [Linux Manager]
> /etc/opt/FJSVrcvmr/customize_data

Definition File Name

> zpool_and_zone_recovery.rcxprop

Definition File Format

> Describe the definition file as below:
>
> 1. Enter the admin IP address of the switchover source server for ADMIN_IP key value.
>
> 2. Insert a line break, and enter the ZFS storage pool on the server and the zone in the ZFS storage pool, separated by commas (",").
>
>   If it is not necessary to boot the zone, the zone specification can be omitted.
>   When specifying two or more ZFS storage pools, enter the pools in separate lines using line breaks.
>
> Until the following is specified, everything will be considered the ZFS storage pool and the zone of the server described in the ADMIN_IP key value.
>
> - Another ADMIN_IP key
>
> - End of the file
>
> The format of each line is given below:

> ```
> ADMIN_IP=failover_admin_ip
> zfs_storage_pool[,zone_name,zone_name2]
> ```

> - Blank spaces before and after commas (",") are ignored.
>
> - When adding comments, start the line with a number sign ("#").

Definition File Items

> Specify the following items.
>
> failover_admin_ip
>
>> Enter the admin IP address of the switchover source server.
>
> zfs_storage_pool
>
>> Enter the name of the ZFS storage to import to the switchover destination server
>
> zone_name
>
>> Enter the zone on the ZFS storage. When specifying multiple zones, separate them with commas (",").

```
ADMIN_IP=192.168.10.123
pool-1,zone1,zone2
pool-2,zone3,zone4,zone5

ADMIN_IP=192.168.10.124
pool-3,zone1,zone5
pool-4
```

Change Procedure for Definition Files

Create a definition file when necessary, before server switchover.
It is not necessary to restart the manager.

Note

This definition file is valid only when the server is registered as a physical OS or a VM host in a Solaris zone. It is invalid when the guest domain of a server which has been registered as an OVM for SPARC VM host is registered as a VM host in the Solaris zone.

When there are no definition files, after server switchover, all ZFS storage pools of the server switchover source are imported, and the zones can be used.

When there are definition files, only the ZFS storage pools and the zones of the switchover source server described in the definition files are restored.

When importing ZFS storage pools which are not specified in the definition files after server switchover, execute the zpool command on the server after the switchover.
Execute "attach" and "boot" using the zoneadm command to enable use of the zones on the ZFS storage pools after import.
For details, refer to the manuals provided by Oracle.

18.5.2 Definition File of ZFS Storage Pool Information [Solaris] [Solaris Zone] [OVM for SPARC]

After switching over the server, ZFS storage pool become able to be exported. While using ZFS storage pool in Solaris, Solaris Zone and each domain of OVM for SPARC, it's necessary to create definition file of ZFS storage pool information in order to import the ZFS storage pool. Please store the definition file into the domain in which ZFS storage pool has been used after installing ROR agent.

It's unnecessary to create definition file in the domain in which ZFS storage pool is not used.

Information

- When configure zpool_info file in Solaris, Solaris Zone environment of manage object server, it's no use even if zpool_and_zone_recovery.rcxprop file is configured in manager.
  ZFS storage pool has been imported according to definition of zpool_info.

- It is also necessary to create this file when a guest domain of a server which is registered as an OVM for SPARC VM host is registered as a VM host in the Solaris zone and then a ZFS storage pool is used on that guest domain.

Definition File's Save Address

[Solaris]
/etc/opt/FJSVrcvat/config

Definition File's Name

zpool_info

Definition File's Form

Please record the definition files as follows.

```
File's limits of authority: 644
```

Record ZFS storage pool name imported in the domain, or ZFS storage pool's guid When there are more than one items, please record in multiple lines.

Example

. . . .

```
ZFS_pool_1
ZFS_pool_2
13230972464300563126
```

. . . .

Definition File's Changing Manual

Please create definition files in each domain that ZFS storage pool has been used.
It's unnecessary to restart agent.

Information

. . . .

- It can be ignored even if there is blank front and rear.

- The first character should be recorded with sharp("#") in a command.

- While creating ZFS storage pool with the same name in a control domain, a guest domain, please appoint ZFS storage pool's guid.

- It's unnecessary to appoint rpool which was created in default while OS install.

. . . .

18.5.3 Definition File of IO domain

After switching over the server, startup an IO domain first than a guest domain by creating definition file that an IO domain is appointed. When the IO domain is not used, it's unnecessary to create definition file.

Point

. . . .

The startup order of a control domain, IO domain, and guest domain is not guaranteed by the OVM for SPARC specifications.

Therefore, if this definition file is not created, the guest domain will be started before the IO domain and there is a chance that starting of the IO domain will fail.

. . . .

Definition File's Save Address

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

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

Definition File's Name

ovm_iodomain_poweron.rcxprop

Definition File's Form

Please record the definition files as follows.

1. Record a control domain's management IP address of switchover source server in value of ADMIN_IP key.

2. Type the IO domain names of the server in the desired startup order, separating with line breaks.

    Before the follows has been recorded, it will become the IO domain of the server which was recorded in value of ADMIN_IP key.

    - The other ADMIN_IP keys

    - file terminal

Example

```
ADMIN_IP=192.168.10.123
A-IOdomain
ADMIN_IP=192.168.10.124
B-IOdomain
C-IOdomain
```

Definition Files' Change Manual

Before switching over server, please create the definition files according to need.
It's unnecessary to restart manager.

Information

- It can be ignored even if there is blank front and rear.

- The first character should be recorded with sharp("#") in a command.

18.5.4 XML file of OVM Configuration Information

It's necessary to save OVM configuration information at XML form before executing server switchover for OVM for SPARC environment. There are methods of GUI, CLI, automatic saving.

Please confirm the save status of OVM configuration information's XML files, and refer to "18.1 Status Display".

OVM configuration information's XML files are saved under a control domain.

Save Address of the File

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

Definition File's Name

ovm_config.xml

Note

OVM configuration information's XML file saving can only be used in primary server. Even though when spare server is used as OVM for SPARC environment the saving operation can be successful, but the configuration information will be overwritten by the incomplete configuration information when switchover is happening.
Therefore the XML file of the spare server can not be used to restore the spare server.
Use the ldm list-constraints command to save the OVM configuration information of spare servers.
For details, refer to the "Oracle VM Server for SPARC Administration Guide".

Point

When server power source is on, and server status is normal, configuration information can be saved as a XML file.

18.5.4.1 Saving from GUI

This is a method to save configuration information by using GUI.

1. On ROR console's server tree, right click on VM host of object control domain, and select [OVM configuration information's XML saving] from displayed menu.

   Save configuration information as XML file in a control domain. Configuration information saving for service processor can be carried out.

18.5.4.2 Saving from CLI

This is a method to save configuration information by using CLI.

Run the rcxadm server backup command to save configuration information's XML files in a control domain. Configuration information saving for service processor can be carried out.

For details on command, refer to "3.2 rcxadm server" in the "Reference Guide (Command) VE".

18.5.4.3 Automatic Saving

OVM configuration information is saved at the following timings:

Automatic saving can both save configuration information for service processor and save XML files for a control domain.

- When the following operations are carried out from this product

    - power source operations of VM Guest/ Virtual L-Server (Power ON/ Power OFF/ Forced power OFF /Reboot/ Forced Reboot)

    - VM Guest/ Virtual L-Server's Movement between the server

    - Virtual L-Server's specifications change (number of CPU, memory size)

    - Virtual L-Server's disk enlargement/reduction

- When the following operations are carried out for a guest domain on a control domain

    - Creation/ deletion of guest domain

    - Bind/unbind of resource

    - Stop/start of guest domain

    - Number of Virtual CPU, memory size changing

    - Additional / deletion of the Virtual disks

    - Movement of guest domain

Note

As a time lag of several minutes occurs during saving of OVM configuration information, do not perform server switchover immediately after performing the above operations.
The saving status of OVM configuration information can be confirmed from Resource Details.
For details, refer to "A.6.3 Physical OS, VM Host, and VM Guest Attributes".

Chapter 19 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.

19.1 Exporting Power Consumption Data

This section explains how to export power consumption data.

The power consumption data for each power monitoring target that is registered in the power monitoring environment can be exported in CSV format.
The exported data can be selected by specifying the desired data types (power and energy), time spans, and sampling rate.

Use the following procedure to export power consumption data.

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

   The [Export Environmental Data (*power_monitoring_target*)] dialog is displayed.

2. Set the following items:

   Figure 19.1 [Export Environmental Data (power_monitoring_target)] Dialog

Target Resources

Specify the power monitoring target to export the power consumption data of.
Select the checkboxes of each desired target. More than one target can be selected.

Data Type

Specify the type of data to export.
Check the checkbox of each desired data type. More than one data type can be selected.

Output time span

Select the time span for which to export data from the drop-down menu.
Select one of the following options:

- Last hour

- Last day

- Last week

- Last month

- Last year

- Custom

When "Custom" is selected, the following fields must all be specified:

- Start day

- Start time

- End day

- End time

Rate

Select the data sampling rate to export from the drop-down menu.

Select one of the following options:

- Finest sampling

- Hourly

- Daily

- Monthly

- Annual

3. Click <OK>.

In the download dialog that is displayed, specify the name of the export file. The data will be exported to the specified file.

📝 **Note**

. . . .

Exporting large amounts of data will take time.
The operation will fail when it takes over five minutes.
If the operation fails, as processing on the server may not have finished, wait for a while before performing the operation again. In that case, change the settings of "Target Resources" and "Output time span" to reduce the amount of data output.

The recommended export settings for environmental data are as listed below.

Table 19.1 Recommended Export Settings

Rate	Output time span	Output device count
Finest sampling	Last day	12
Hourly	Last month	30

Rate	Output time span	Output device count
Daily	Last year	30
Monthly	Select "Custom" and specify 5 years	60
Annual	Select "Custom" and specify 5 years	60

19.2 Displaying Power Consumption Data Graphs

This section explains how to display power consumption data as graphs.

The power consumption data for each power monitoring target that is registered in the power monitoring environment can be displayed as graphs.
The collected power consumption data and average values of the specified time span and rate can be displayed in line graphs.
Use the following procedure to display power consumption data as graphs.

1. Select [Tools]-[Environmental Data Graph] from the ROR console menu.

   The [Environmental Data Graph] dialog is displayed.

2. Set the following items:

   Figure 19.2 [Environmental Data Graph] Dialog

Target Resources

Specify the power monitoring target name to display the power consumption data graph of.
Select the checkboxes of each desired target.
Up to 18 targets can be selected.

Graph Settings

Data Type

Specify the type of data to display the graph.
Specify either one of the following for the data type:

- Power (Instantaneous power consumption)

- Average power (Average power consumption during the selected time span)

Output Time Span

Select the time span for the data from the drop-down menu.

Select one of the following options:

- Last hour

- Last day

- Last week

- Last month

- Last year

- Custom

When "Custom" is selected, the following fields must all be specified:

- Start day

- Start time

- End day

- End time

Rate

Select the graph output interval to export from the drop-down menu.

Select one of the following options:

- Finest sampling

- Hourly

- Daily

- Monthly

- Annual

3. Click <Graph Output>.

   After switching to the graph display window, the selected power consumption data can be displayed in line graphs.

   Figure 19.3 Graph Display Window
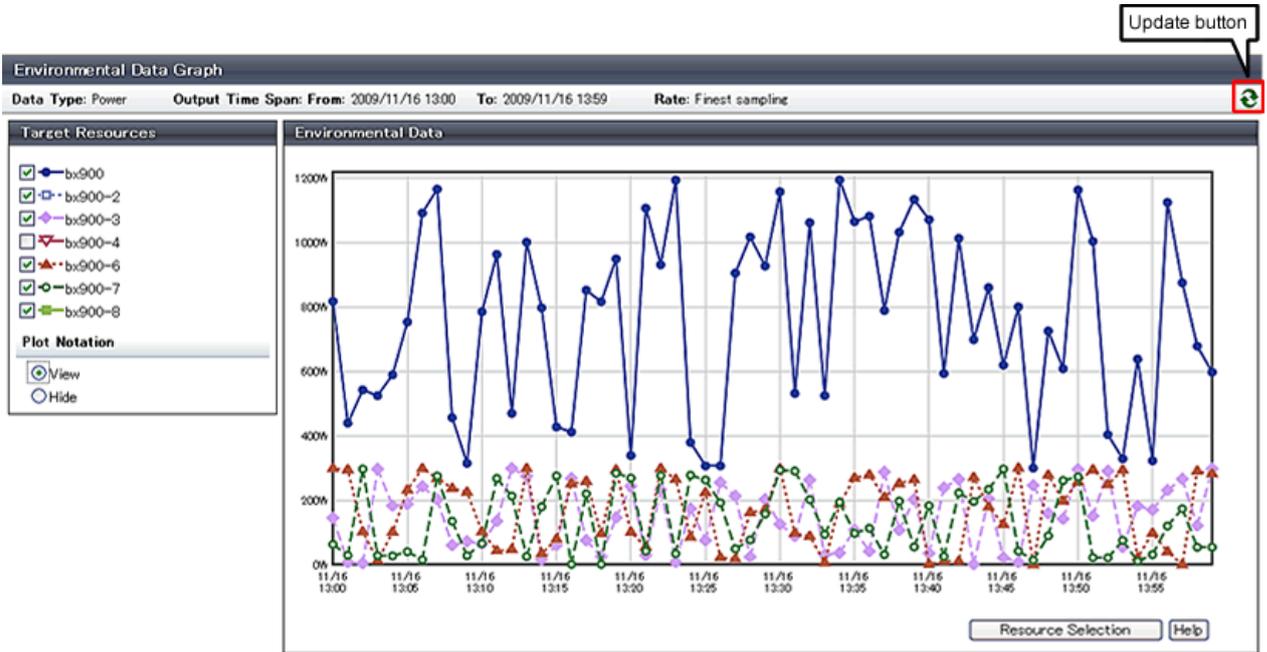
The following operations can be performed from the graph display window.

   - Switching resource display

     By selecting and clearing the checkbox of the [Target Resources], it is possible to display or hide the corresponding graph.

   - Switching plot symbol display

     Selecting the [View] or [Hide] radio button of [Plot Notation] switches between displaying and hiding plot symbols in line graphs.

   - Data update

     Clicking the update button on the upper right of the screen updates the displayed graph.

   - Return to resource selection window.

     Clicking <Resource Selection> displays the [Environmental Data Graph] dialog.

![Note icon] **Note**
. . . .
If you change the size of the web browser when displaying graphs, click the update button after doing so.
. . . .

Appendix A User Interface

Resource Orchestrator provides three graphical user interfaces: the ROR console, BladeViewer and NetworkViewer.
This appendix provides an overview of the ROR console.

For details on how to open and close the ROR console, refer to "Chapter 3 Login to the ROR Console" in the "Setup Guide VE".
For details on BladeViewer, refer to "Chapter 6 BladeViewer".
For details on the NetworkViewer, refer to "Chapter 13 NetworkViewer".

A.1 ROR Console

This section explains how the [Resource] tab of the ROR console is organized.

The [Resource] tab of the ROR console is sometimes referred to as the ROR console.

Figure A.1 ROR Console
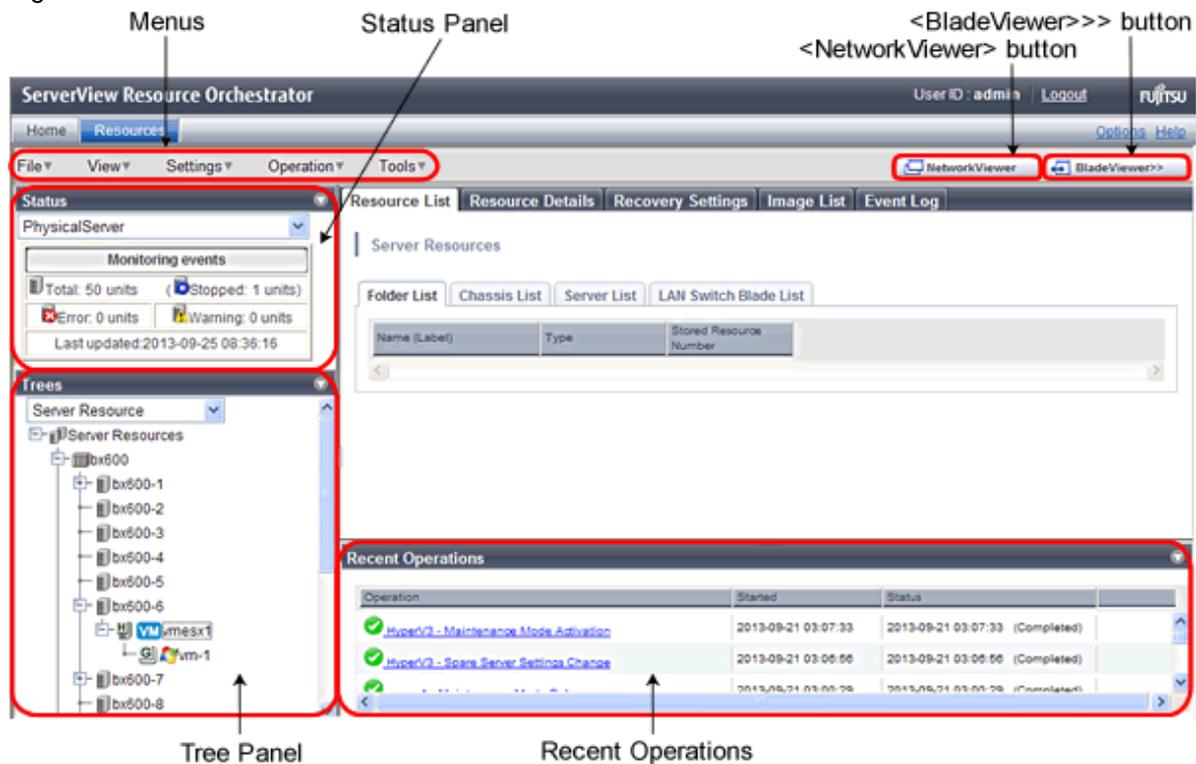
Menus

> Operations can be performed either from the menu bar or popup menus.

Status Panel

> The Status Panel displays the status of managed servers.

> If a warning or error event occurs on a managed server, the status monitoring area starts to blink.

Tree Panel

> By switching between tree types, it is possible to select from the following 4 types of trees.

> Server Resources

>> The resources below are shown in a tree view. A status icon is displayed over each resource's icon.

>> - Chassis

>> - Server

>> - Physical OS

- VM Host

- VM Guest

- LAN Switch (LAN Switch Blades)

Network

The resources below are shown in a tree view. A status icon is displayed over each resource's icon.

- LAN switch (excluding LAN switch blades)

Power Monitoring Devices

The following power monitoring devices are shown in a tree view.

- PDU (Power Distribution Unit)

- UPS (Uninterruptible Power Supply)

Management Software

The following management software which can be used in coordination with Resource Orchestrator are shown in a tree view. A status icon is displayed over each resource's icon.

- Management Software (vCenter Server)

- Management Software (SCVMM)

- Management Software (VIOM)

Main Panel

The Main Panel displays information on resources selected in the tree.

- [Resource List] Tab

  Displays information on resources related to the resource selected in the resource tree.

- [Resource Details] Tab

  Displays more detailed information on the resource selected in the tree, or a resource that was double-clicked in the [Resource List] tab.

- [Recovery Settings] Tab

  Displays information on the spare servers assigned to the resource selected in the resource tree.

- [Image List] Tab

  Displays system and cloning image information.

- Events

  Resource Orchestrator events and related information are displayed.

  The event log displays a history of events that have occurred on managed resources.

Recent Operations

Displays the progress statuses and results of operations performed in Resource Orchestrator.

<NetworkViewer> Button

Displays the NetworkViewer showing the network configuration in another window or tab.
The browser settings determine whether another window or tab is used.

<BladeViewer>>> Button

Opens the BladeViewer interface.
BladeViewer is a management interface specially designed for blade servers. It can only be used in conjunction with PRIMERGY BX servers registered as managed servers.

A.2 Menus

This section describes the menus available in the ROR console.

Figure A.2 Menu

A.2.1 List of Menus

The menus provided on the menu bar of the ROR console are listed in the table below.
Options available vary according to the authority level of the user account.

Table A.1 Menu Items

Menu	Submenu		Privileged User	General User	Function
File	Import	-	Yes	No	Imports the system configuration file for pre-configuration.
	Export	-	Yes	No	Exports the system configuration file for pre-configuration.
	Download Template	CSV Format	Yes	Yes	Downloads a sample of the system configuration file (CSV format) for pre-configuration.
	Export Environmental Data	Chassis	Yes	Yes	Exports environmental data collected from chassis.
		Server	Yes	Yes	Exports environmental data collected from servers.
		Power Monitoring Devices	Yes	Yes	Exports environmental data collected from power monitoring devices.
	Logout	-	Yes	Yes	Logs out of the ROR console. (*1)
View	Reset Layout	-	Yes	Yes	Returns the layout of the ROR console to its initial state.
Settings	Register	Chassis	Yes	No	Registers a chassis.
		Server	Yes	No	Registers a server.
		SPARC Enterprise (M3000/T Series)	Yes	No	Registers a SPARC Enterprise (M3000/T series) server.
		SPARC Enterprise (Partition Model)	Yes	No	Registers SPARC Enterprise M4000/M5000/M8000/M9000 servers.
		SPARC M10-1/M10-4	Yes	No	Registers a SPARC M10-1/M10-4.
		SPARC M10-4S	Yes	No	Registers a SPARC M10-4S.
		PRIMEQUEST	Yes	No	Registers a PRIMEQUEST.
		LAN switch	Yes	No	Registers a LAN switch.
		Agent	Yes	No	Register the agent.
		Power Monitoring Device	Yes	No	Registers a power monitoring device.
		Management Software (vCenter Server)	Yes	No	Registers VM management software (VMware vCenter Server).

Menu	Submenu		Privileged User	General User	Function
		Management Software (SCVMM)	Yes	No	Registers VM management software (System Center Virtual Machine Manager).
		Management Software (VIOM)	Yes	No	Registers VM management software (VIOM).
	Delete	-	Yes	No	Deletes a resource.
	Modify (*2)	Registration Settings	Yes	No	Modifies a resource's registration settings.
		HBA address rename settings (*3)	Yes	No	Modifies the HBA address rename settings of a server.
		Network Settings (*4, *5, *6)	Yes	No	Modifies the network settings of a LAN switch.
		Spare Server Settings (*7)	Yes	No	Modifies a server's recovery settings.
		Monitoring Settings	Yes	No	Modifies the monitoring information for a server.
		WWN Settings (*8)	Yes	No	Modifies the WWN settings for a server.
		VM Host Login Account	Yes	No	Modifies the registered login account used to communicate with the VM host.
	User Accounts	-	Yes	Yes	Adds, changes, and deletes user accounts.
	Admin LAN Subnet	-	Yes	Yes (*9)	Performs viewing, registration, changing or deletion of the admin LAN subnet information.
Operation	Update	-	Yes	Yes	Updates a resource.
	Power	ON	Yes	No	Powers on a server.
		OFF	Yes	No	Powers off a server after shutting down its operating system.
		OFF (Forced)	Yes	No	Powers off a server without shutting down its operating system.
		Reboot	Yes	No	Reboots a server after shutting down its operating system.
		Reboot (Forced)	Yes	No	Reboots a server without shutting down its operating system.
	LED (*4)	ON	Yes	No	Turns the maintenance LED on.
		OFF	Yes	No	Turns the maintenance LED off.
	Spare Server (*2, *7)	Switchover	Yes	No	Switches over a server with one of its spare servers.
		Failback	Yes	No	Switches back a server to its pre-switchover state.
		Takeover	Yes	No	Accepts a switched over configuration as final (without switching back to the original configuration).

Menu	Submenu		Privileged User	General User	Function
	Hardware Maintenance	Re-configure	Yes	No	Detects and reconfigures the properties of a replaced server.
		Restore LAN Switch (*10, *11)	Yes	No	Restores a LAN switch configuration.
	Maintenance Mode (*2)	Set	Yes	No	Places a server into maintenance mode.
		Release	Yes	No	Sets a server to active mode.
	Backup/Restore (*2)	Backup	Yes	No	Backs up a system image from a server.
		Restore	Yes	No	Restores a system image to a server.
	Cloning (*2, *12)	Collect	Yes	No	Collects a cloning image from a server.
		Deploy	Yes	No	Deploys a cloning image to a server.
	Migrate VM Guest	-	Yes	No	Migrates a VM guest to a different VM host.
	VM Home Position	Settings	Yes	No	Sets VM Home Position.
		Clear	Yes	No	Clears VM Home Position.
		Back to Home	Yes	No	Migrates a VM guest to VM Home Position.
	Save OVM Configuration XML	-	Yes	No	Save OVM configuration information in XML file. (*14)
Tools	Topology	Discover LAN switches	Yes	No	Discovers LAN switches within the admin LAN.
		Detect physical links	Yes	No	Acquires physical link data from registered LAN switches.
	Licenses	-	Yes	No	Displays license settings and registered licenses.
	Options	-	Yes	Yes (*13)	Modifies client and environmental data settings.
	Environmental Data Graph	-	Yes	Yes	Displays environmental data graphs.

*1: If multiple ROR consoles or BladeViewer sessions exist, the login sessions may be terminated.
*2: Cannot be selected for a VM guest.
*3: Cannot be selected for PRIMEQUEST or Fujitsu M10/SPARC Enterprise.
*4: Available only for PRIMERGY BX servers.
*5: Cannot be set for PRIMERGY BX900/BX400 LAN switch blades operating in IBP mode or Converged Fabric mode.
*6: Cannot be set for LAN switch blade PY CB 10Gb FEX Nexus B22.
*7: Cannot be selected for PRIMEQUEST.
*8: Only available for Fujitsu M10/SPARC Enterprise.
*9: Only the admin LAN subnet information can be displayed with general user privileges.
*10: Not available for PRIMERGY BX900/BX400 LAN switch blades operating in IBP mode or Converged Fabric mode.
*11: Not available for LAN switch blade PY CB 10Gb FEX Nexus B22.
*12: Cannot be selected for a VM host.
*13: General users cannot change environmental data settings.
*14: VM host can only be selected in the case of OVM for SPARC.

A.2.2 Popup Menus

Right-clicking an object displayed in the resource tree or in the [Image List] tab displays a popup menu with a list of options available for that object.

The tables below detail the popup menus provided for each object.
Available menus vary according to user account privileges.

- Server Resource

- Network Resource

- Power Monitoring Device

- Management Software

- Cloning Image List

- System Image List

Server Resource

Figure A.3 Server Tree
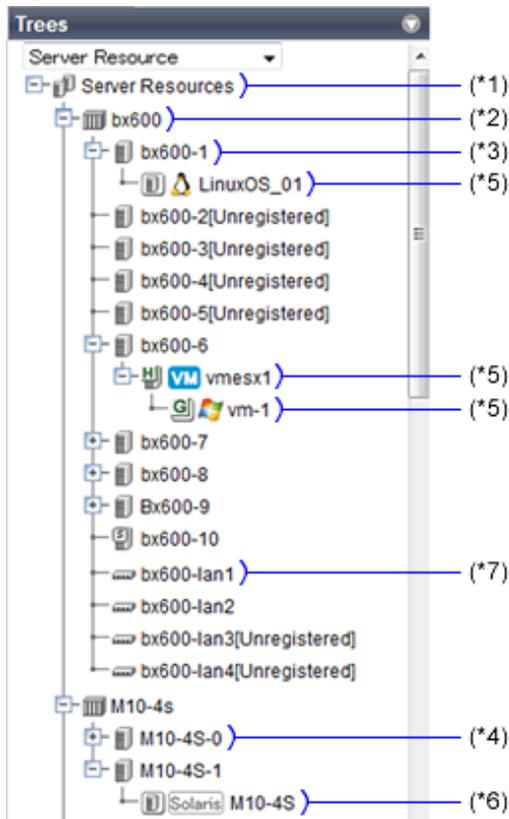
*1: Refer to "Table A.2 Popup Menus Available for the "Server Resources" Tree Node".
*2: Refer to "Table A.3 Popup Menus Available for Chassis".
*3: Refer to "Table A.4 Popup Menus Available for Servers".
*4: Refer to "Table A.5 Popup Menus Available for Fujitsu M10/SPARC Enterprise".
*5: Refer to "Table A.6 Popup Menus Available for Physical OSs [Physical Servers], VM Hosts, and VM Guests".
*6: Refer to "Table A.7 Popup Menus Available for Physical OSs [Solaris]".
*7: Refer to "Table A.8 Popup Menus Available for LAN Switches".

Table A.2 Popup Menus Available for the "Server Resources" Tree Node

Popup Menu		Function
Menu	Submenu	
Register	Chassis	Registers a chassis.
	Server	Registers a server.

Popup Menu		Function
Menu	Submenu	
	SPARC Enterprise (M3000/T Series)	Registers a SPARC Enterprise (M3000/T series) server.
	SPARC Enterprise (Partition Model)	Registers the chassis of a SPARC Enterprise M4000/M5000/M8000/M9000 server.
	SPARC M10-1/M10-4	Registers a SPARC M10-1/M10-4.
	SPARC M10-4S	Registers a SPARC M10-4S.
	PRIMEQUEST	Registers the chassis of a PRIMEQUEST.
Export	Environmental Data (Chassis)	Exports environmental data collected from chassis.
	Environmental Data (Servers)	Exports environmental data collected from servers.

Table A.3 Popup Menus Available for Chassis

Popup Menu		Function
Menu	Submenu	
Delete	-	Deletes a chassis.
Update	-	Updates a chassis.
Modify	Registration Settings	Modifies a chassis' registration settings.
External Management Software	-	Opens a Management Blade's Web interface.
Export (*)	Environmental Data	Exports environmental data collected from chassis.

* Note: This option is only available for chassis equipped with power monitoring capabilities.

Table A.4 Popup Menus Available for Servers

Popup Menu		Function
Menu	Submenu	
Register	Server (*1)	Registers a server.
	Agent	Register the agent.
Delete	-	Deletes a server.
Update	-	Updates a server.
Modify	Registration Settings	Modifies a server's registration settings.
	HBA address rename settings (*2)	Modifies the HBA address rename settings of a server.
	Network Settings (*3, *4)	Modifies the network settings of a server.
	Spare Server Settings (*2)	Modifies a server's recovery settings.
Maintenance Mode	Set	Places a server into maintenance mode.
	Release	Sets a server to active mode.
Power	ON	Powers on a server.
	OFF	Powers off a server after shutting down its operating system.
	OFF (Forced)	Powers off a server without shutting down its operating system.

Popup Menu		Function
Menu	Submenu	
	Reboot	Reboots a server after shutting down its operating system.
	Reboot (Forced)	Reboots a server without shutting down its operating system.
LED (*3)	ON	Turns the maintenance LED on.
	OFF	Turns the maintenance LED off.
Hardware Maintenance	Re-configure	Detects and reconfigures the properties of a replaced server.
Backup/Restore	Restore	Restores a system image to a server.
Cloning	Deploy	Deploys a cloning image to a server.
Console Screen (*5)	-	Opens the server console.
External Management Software (*6)	-	Opens external server management software.
Export (*7)	Environmental Data	Exports environmental data collected from servers.

*1: Available only for PRIMERGY BX series and PRIMEQUEST servers.
*2: Available only for VM hosts when using PRIMEQUEST.
*3: Available only for PRIMERGY BX servers.
*4: Available only for VM guests.
*5: In order to open the console screen of managed server, register the account of Remote Management Controller in ServerView Operations Manager. When opening the L-Server console screen at the second time or later, a window for iRMC management may be opened instead of the console screen. If an iRMC management screen is displayed, close that screen and then start the console screen again.
*6: Available only for PRIMERGY series, PRIMEQUEST, SPARC Enterprise M series, and FUJITSU M10 servers.
*7: This option is only available for chassis equipped with power monitoring capabilities.

Table A.5 Popup Menus Available for Fujitsu M10/SPARC Enterprise

Popup Menu		Function
Menu	Submenu	
Register	Server (*1)	Registers a server.
	Agent	Register the agent.
Delete	-	Deletes a Fujitsu M10/SPARC Enterprise.
Update	-	Updates a Fujitsu M10/SPARC Enterprise.
Modify	Registration Settings	Modifies a Fujitsu M10/SPARC Enterprise's registration settings.
	WWN Settings	Modifies the WWN settings for a server.
	Spare Server Settings	Modifies a server's recovery settings.
Maintenance Mode	Set	Places a server into maintenance mode.
	Release	Sets a server to active mode.
Power	ON	Powers on a Fujitsu M10/SPARC Enterprise.
	OFF	Powers off a Fujitsu M10/SPARC Enterprise after shutting down its operating system.
	OFF (Forced)	Powers off a Fujitsu M10/SPARC Enterprise without shutting down its operating system.

Popup Menu		Function
Menu	Submenu	
	Reboot	Reboots a Fujitsu M10/SPARC Enterprise after shutting down its operating system.
	Reboot (Forced)	Reboots a Fujitsu M10/SPARC Enterprise without shutting down its operating system.
External Management Software	-	Opens external server management software for Fujitsu M10/SPARC Enterprise.
Export (*2)	Environmental Data	Exports environmental data collected from servers.

*1: Available only for SPARC Enterprise M4000/M5000/M8000/M9000 or FUJITSU M10-4S.
*2: This option is only available for chassis equipped with power monitoring capabilities.

Table A.6 Popup Menus Available for Physical OSs [Physical Servers], VM Hosts, and VM Guests

Popup Menu		Function
Menu	Submenu	
Delete (*1)	-	Deletes a physical OS or VM host.
Update	-	Updates a physical OS, VM host, or VM guest.
Modify (*1, *2)	HBA address rename settings (*3, *4)	Modifies the HBA address rename settings of a server.
	Network Settings (*4, *5, *6, *7)	Modifies the network settings of a server.
	Spare Server Settings (*3, *4)	Modifies a server's recovery settings.
	Monitoring Settings	Modifies the monitoring information for a server.
	VM Host Login Account (*8)	Modifies the registered login account used to communicate with the VM host.
Power	ON	Powers on a server.
	OFF	Powers off a server after shutting down its operating system.
	OFF (Forced)	Powers off a server without shutting down its operating system.
	Reboot	Reboots a server after shutting down its operating system.
	Reboot (Forced)	Reboots a server without shutting down its operating system.
Spare Server (*1, *3, *4)	Switchover	Switches over a server with one of its spare servers.
	Failback	Switches back a server to its pre-switchover state.
	Takeover	Accepts a switched over configuration as final (without switching back to the original configuration).
Maintenance Mode (*1, *4)	Set	Places a server into maintenance mode.
	Release	Sets a server to active mode.
Backup/Restore (*1, *4)	Backup	Backs up a system image from a server.
	Restore	Restores a system image to a server.
Cloning (*1, *9)	Collect	Collects a cloning image from a server.
	Deploy	Deploys a cloning image to a server.
VM Home Position (*1, *8)	Settings	Sets VM Home Position.

Popup Menu		Function
Menu	Submenu	
	Clear	Clears VM Home Position.
	Back to Home	Migrates a VM guest to VM Home Position.
External Management Software (*1, *10)	-	Opens external server management software.
VM Management Console (*4, *8, *11, *12)	-	Opens the VM management console installed on the client machine.
Migrate VM Guest (*13)	-	Migrates a VM guest to a different VM host.
Save OVM Configuration XML (*14)	-	Save OVM configuration information in XML file.

*1: Cannot be selected for a VM guest.

*2: Available only for VM hosts when using PRIMEQUEST.

*3: Cannot be selected for PRIMEQUEST.

*4: This option may or may not be available according to the server virtualization software used. For details, refer to "D.1 Common Functions of Server Virtualization Software" in the "Design Guide VE".

*5: Available only for PRIMERGY BX servers.

*6: Cannot be set for PRIMERGY BX900/BX400 LAN switch blades operating in IBP mode or Converged Fabric mode.

*7: Cannot be set for LAN switch blade PY CB 10Gb FEX Nexus B22.

*8: This menu is not available for a physical OS.

*9: Cannot be selected for a VM host.

*10: Available only for PRIMERGY series, PRIMEQUEST, SPARC Enterprise M series, and FUJITSU M10 servers.

*11: If the VM management screen is started on VMware vSphere 5.0 or later, it may connect with the VM management product or the VM host, and login may fail. In this case, input the password from the VM management screen, and log in.

*12: To use this feature, a VM management console must be installed and the admin client must be configured properly.

After installing the VM management console, select this menu item and follow the instructions shown in the displayed dialog.

*13: Available only for VM guests.

*14: VM host can only be selected in the case of OVM for SPARC.

Table A.7 Popup Menus Available for Physical OSs [Solaris]

Popup Menu		Function
Menu	Submenu	
Delete	-	Deletes a Fujitsu M10/SPARC Enterprise.
Update	-	Updates a Fujitsu M10/SPARC Enterprise.
Modify	Spare Server Settings	Modifies a server's recovery settings.
	Monitoring Settings	Modifies a Fujitsu M10/SPARC Enterprise's monitoring settings.
Power	ON	Powers on an operating system.
	OFF	Powers off a server after shutting down its operating system.
	OFF (Forced)	Powers off a server without shutting down its operating system.
	Reboot	Reboots a server after shutting down its operating system.

Popup Menu		Function
Menu	Submenu	
	Reboot (Forced)	Reboots a server without shutting down its operating system.
Spare Server	Switchover	Switches over a server with one of its spare servers.
	Failback	Switches back a server to its pre-switchover state.
	Takeover	Accepts a switched over configuration as final (without switching back to the original configuration).
Maintenance Mode	Set	Places a server into maintenance mode.
	Release	Sets a server to active mode.
External Management Software	-	Opens external server management software for Fujitsu M10/SPARC Enterprise.

Table A.8 Popup Menus Available for LAN Switches

Popup Menu		Function
Menu	Submenu	
Register	LAN Switch	Registers a LAN switch.
Delete	-	Deletes a LAN switch.
Update	-	Updates a LAN switch.
Modify	Registration Settings	Modifies a LAN switch's registration settings.
	Network Settings (*1, *2)	Modifies the VLAN settings of a LAN switch's external ports.
Restore (*1, *2)	-	Restores a LAN switch configuration.
External Management Software	-	Opens a LAN switch's Web interface.

*1: Not available for PRIMERGY BX900/BX400 LAN switch blades operating in IBP mode or Converged Fabric mode.
*2: Not available for LAN switch blade PY CB 10Gb FEX Nexus B22.

Network Resource

Figure A.4 Network Devices Tree
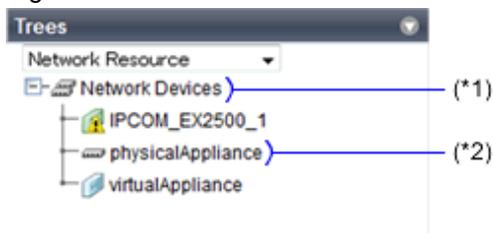
*1: Refer to "Table A.9 Popup Menus Available for Network Devices".
*2: Refer to "Table A.10 Popup Menus Available for Network Devices".

Table A.9 Popup Menus Available for Network Devices

Popup Menu		Function
Menu	Submenu	
Topology	Discover LAN switches	Discovers LAN switches within the admin LAN.

Popup Menu		Function
Menu	Submenu	
	Detect physical links	Acquires physical link data from registered LAN switches.

Table A.10 Popup Menus Available for Network Devices

Popup Menu		Function
Menu	Submenu	
Register	-	Registers selected network devices.
Delete	-	Deletes selected network devices.
Update	-	Obtains and updates the information on the selected network devices.
Modify	Basic Information	Modifies basic information of a network device.
Maintenance Mode	Set	Places a server into maintenance mode.
	Release	Releases maintenance mode.
External Management Software	-	Starts the management screen (Web console) provided by the network device.

Power Monitoring Device

Figure A.5 Power Monitoring Device Tree

*1: Refer to "Table A.11 Popup Menus Available for the "Power Monitoring Devices" Tree Node".
*2: Refer to "Table A.12 Popup Menus Available for Power Monitoring Devices".

Table A.11 Popup Menus Available for the "Power Monitoring Devices" Tree Node

Popup Menu		Function
Menu	Submenu	
Register	Power Monitoring Device	Registers a power monitoring device.
Export	Environmental Data	Exports environmental data.

Table A.12 Popup Menus Available for Power Monitoring Devices

Popup Menu		Function
Menu	Submenu	
Delete	-	Deletes a power monitoring device (PDU or UPS).
Update (*)	-	Updates a power monitoring device (PDU or UPS).
Modify	Registration Settings	Modifies a power monitoring device's registration settings.

Popup Menu		Function
Menu	Submenu	
Hardware Maintenance	Re-configure	Detects and reconfigures the properties of a replaced power monitoring device (PDU or UPS).
Export	Environmental Data	Exports environmental data.

*1: Unlike other resources, the properties of a power monitoring devices are not automatically updated. Use this option to update them manually when necessary.

Management Software

Figure A.6 Management Software Tree
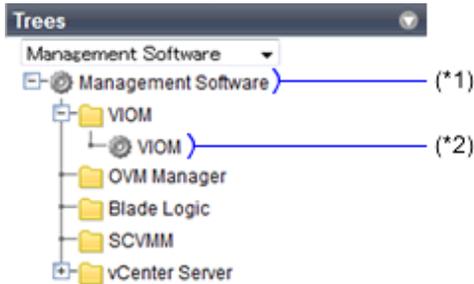
*1: Refer to "Table A.13 Popup Menus Available for Management Software".
*2: Refer to "Table A.14 Popup Menus Available for Management Software (vCenter Server/SCVMM/OVM Manager/Blade Logic/VIOM)".

Table A.13 Popup Menus Available for Management Software

Popup Menu		Function
Menu	Submenu	
Register	Management Software (vCenter Server)	Registers VM management software (VMware vCenter Server).
	Management Software (SCVMM)	Registers VM management software (System Center Virtual Machine Manager).
	Management Software (OVM Manager)	Registers management software (OVM Manager).
	Management Software (Blade Logic)	Registers management software (Blade Logic).
	Management Software (VIOM)	Registers VM management software (VIOM).

Table A.14 Popup Menus Available for Management Software (vCenter Server/SCVMM/OVM Manager/Blade Logic/VIOM)

Popup Menu		Function
Menu	Submenu	
Delete	-	Deletes management software.
Update	-	Updates management software information.
Modify	Registration Settings	Modifies registration settings for management software.

Cloning Image List

Figure A.7 Cloning Image List (server tree)
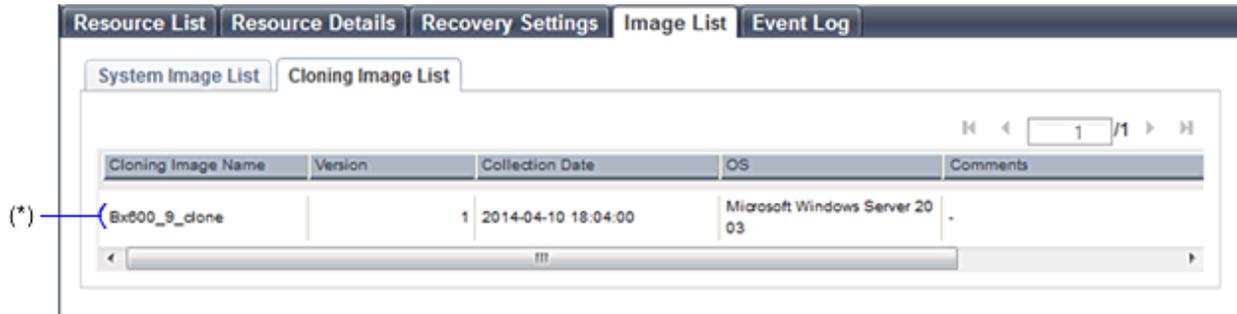
* Note: Refer to "Table A.15 Popup Menus Available for Cloning Images".

Table A.15 Popup Menus Available for Cloning Images

Popup Menu		Function
Menu	Submenu	
Deploy	-	Deploys a cloning image to a server.
Delete	-	Deletes a cloning image.

Note
. . . .
If ServerView Deployment Manager is used on the admin LAN, the popup menu for cloning images cannot be used.
. . . .

System Image List

Figure A.8 System Image List
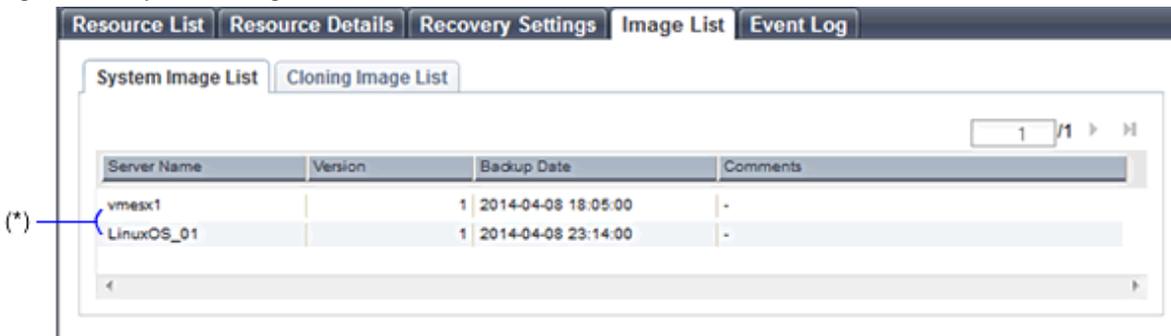
* Note: Refer to "Table A.16 Popup Menus Available for System Images".

Table A.16 Popup Menus Available for System Images

Popup Menu		Function
Menu	Submenu	
Restore	-	Restores a system image to a server.
Delete	-	Deletes a system image.

A.3 Status Panel

This section explains the different statuses that are displayed in the ROR console.

Figure A.9 Status Panel

Status Monitoring Area

The Event Log monitors a history of events that have occurred on managed resources.
Based on detected events, the status monitoring area will change color and blink. Clicking the status monitoring area will stop the blinking.
The following table details the different statuses and their associated corrective actions.

Table A.17 Monitor Status List

Monitoring Status	Background Color	Details	Corrective Action
Monitoring events	Grey	This indicates a normal state. No warning or error-level events have occurred on the displayed resources.	No action is necessary.
Warning event detected	Yellow	This indicates a warning state. A warning-level event has occurred on one or more of the displayed resources.	Click the status monitoring area to stop the blinking and fix the cause of the problem.
Error event detected	Red	This indicates an error state. An error-level event has occurred on one or more of the displayed resources.	Click the status monitoring area to stop the blinking and fix the cause of the problem.

Resource Status Area

This area displays the number of registered servers experiencing each status.
The resource status area lights up when there is at least one server in either "Error" or "Warning" status.
Clicking a lit up status area will display a list of resources with that status in the [Resource List] tab. Double-click a displayed resource to switch to its [Resource Details] tab and open either its external management software or the Management Blade's Web interface to investigate the problem.

A.4 Tree Panel

This section describes the trees used in the ROR console.

Figure A.10 Tree Panel
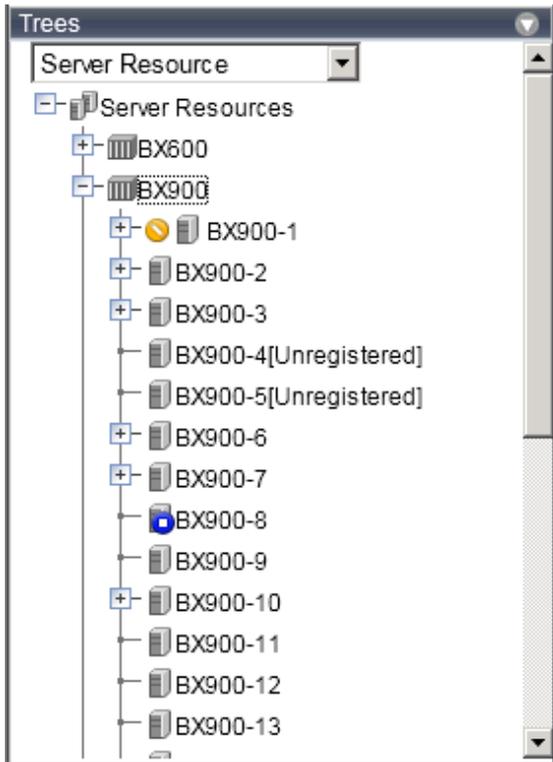
In the tree panel, clicking the upper area displays the following trees:

- Server Resources

- Network Devices

- Power Monitoring Devices

- Management Software

Server Resources

Chassis, servers, physical OSs, VM hosts, VM guests, and LAN switches managed in Resource Orchestrator are displayed in a tree view. Resources are primarily displayed in registration order. However, for blade servers within a common chassis, the order by which Resource Orchestrator detects server blades takes precedence.

Resources displayed in the resource tree are represented by an icon and their resource name. For details on the icons used to indicate different resources, refer to "11.2 Resource Status" in the "Operation Guide VE".

For a non-registered resource, one of the following registration states is displayed at the end of the resource's name.

Table A.18 Resource Registration States

[Unregistered]	The resource was automatically detected, but has not been registered yet
[Registering]	The resource is being registered
[Admin Server]	This server is the admin server itself

If a label was set for a resource (in BladeViewer), that label is displayed after the resource name.

Display Format

resource_name(label)

Clicking a resource in the resource tree displays information related to that resource in the Main Panel. Right-clicking a resource displays a list of available operations in a popup menu.

For details on popup menus, refer to "A.2.2 Popup Menus".

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

For details on status icons, refer to "11.2 Resource Status" in the "Operation Guide VE".

Clicking a resource icon will show information related to that resource in the Main Panel. Use this information to investigate the problem.

Information

. . . .

For a VM host coordinated with VMware vCenter Server, the name (IP address or host name) entered when registering with VMware vCenter Server will be displayed.

. . . .

Network

External LAN switches (those other than LAN switch blades) managed in Resource Orchestrator are shown in a tree view. Resources are sorted and displayed by name in alphabetical order.

Resources displayed in the resource tree are represented by an icon and their resource name.

For details on the icons used to indicate different resources, refer to "11.2 Resource Status" in the "Operation Guide VE".

For a non-registered resource, one of the following registration states is displayed at the end of the resource's name.

Table A.19 Resource Registration States

[Unregistered]	The resource was automatically detected, but has not been registered yet
[Registering]	The resource is being registered

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

For details on status icons, refer to "11.2 Resource Status" in the "Operation Guide VE".

Clicking a resource icon will show information related to that resource in the Main Panel. Use this information to investigate the problem.

Power Monitoring Devices

The power monitoring devices (PDU or UPS) used by Resource Orchestrator to monitor power consumption are displayed in a tree view.

For details on icons used to represent power monitoring devices, refer to "11.2 Resource Status" in the "Operation Guide VE".

Clicking a power monitoring device displayed in the resource tree will display its attributes in the Main Panel. Right-clicking a power monitoring device will display a list of available operations in a popup menu.

For details on popup menus, refer to "A.2.2 Popup Menus".

Management Software

Management software (vCenter Server, SCVMM, , VIOM,) used in coordination with Resource Orchestrator is displayed in a tree view.

For details on the icons used to indicate different management software, refer to "11.2 Resource Status" in the "Operation Guide VE".

Clicking a management software on the tree displays information related to it in the Main Panel. Right-clicking a management software will display a list of available operations in a popup menu.

For details on popup menus, refer to "A.2.2 Popup Menus".

Sorting the Resources in the Tree

The tree displays the resources in ascending order of name, by resource type.

To sort the resource list within the same type of resource, use the following method.

Storage Location of the Definition File

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

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

Definition File Name

gui_config.rcxprop

Definition File Format

RESOURCE_TREE_SORT_ORDER=*RESOURCE_TREE_ORDER*

Definition File Items

RESOURCE_TREE_ORDER

Specify either one of the following options:

name: Displays the resource list in ascending (alphabetical) order of resource names.

registered: Displays the resource list in the order in which the resources were registered or created.

Note

. . . .

- To enable the above mentioned setting, restart the manager after editing the definition file.

- The orders of some lists, such as for blade servers in the server tree, cannot be changed.

. . . .

A.5 [Resource List] Tab

The [Resource List] tab in the Main Panel displays a list of resources related to the resource that was selected in the resource tree.
For details on the icons used to indicate different resources, refer to "11.2 Resource Status" in the "Operation Guide VE".

The table below shows the information displayed in the Resource List for each selectable resource.

Server Resources

Information on all registered chassis, servers, and LAN switches.

Chassis

Information on registered servers and LAN switch blades mounted in the selected chassis is displayed.
For PRIMEQUEST, SPARC Enterprise M4000/M5000/M8000/M9000, or SPARC M10-4S, information on the partitions configured on the chassis is displayed.

Server

Information on the physical OSs, VM hosts, and VM guests running on the selected server.

Physical OS

Information on the selected physical OS.

VM Host

Information on the VM guests running on the selected VM host.

VM Guest

Information on the selected VM guest.

Network Devices

Information on the selected network device is displayed.

Unregistered Server

Information on the selected unregistered server.

Network Resources

Information on all registered network resources is displayed.

Power Monitoring Devices

Information on all registered power monitoring devices.

Management Software

Information on all registered management software.

Management Software (vCenter Server, SCVMM, or VIOM)

Information on the selected management software.

Double-clicking a resource in the [Resource List] tab displays its [Resource Details] tab in the Main Panel. This tab shows detailed information on the selected resource.
In the [Resource List] tab, resources experiencing problems are shown with a status icon displayed on top of their resource icon. Switch to the [Resource Details] tab to check the faulty component or open external management software to investigate the problem.
For details, refer to "Chapter 11 Monitoring Resources" in the "Operation Guide VE".

The initial display is not sorted.
Clicking a column heading in the [Resource List] tab will sort the displayed resources in ascending or descending order.
In each page of the list, 10 items can be displayed. It is possible to move forwards and backwards by single pages, and to the first or last page.

Physical servers, physical OSs, VM hosts, and VM guests are displayed under the "Server List".
Resources displayed in the [Server List] can be filtered by selecting or deselecting their corresponding checkboxes.

A.6　[Resource Details] Tab

The [Resource Details] tab displays detailed information on registered resources.
This information is displayed by double-clicking any of the following resources in the resource tree:

- Chassis

- Server

- Physical OS

- VM Host

- VM Guest

- Network Device

- PDU or UPS

- Management Software (vCenter Server, SCVMM, or VIOM)

🛈 Note

....
For items that there is no content to display the details for, a hyphen ("-") is displayed.
....

Selecting a blade server displays the following chassis image in the [Resource Details] tab. This image shows the slot positions of all server blades installed in the chassis.

Figure A.11 Chassis
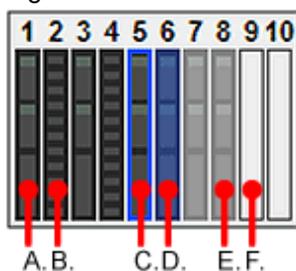
The resource images shown in the above chassis image are explained in the table below.

Table A.20 Meaning of the Resources Shown in the Chassis Image

Image	Meaning
A.	Registered server blade.
B.	Detected storage blade.
C.	Currently displayed server blade.
D.	Server blade selected within the chassis image.
E.	Server blade that has not been registered yet.
F.	Empty slot.

Attributes of Displayed Resources

The [Resource Details] tab displays different attributes for each resource, as described below.

A.6.1 Chassis Attributes

General Area

Chassis name

The name used to identify a chassis is displayed.

System Name

The system name of the chassis is displayed.

Displayed only for PRIMEQUEST servers.

Model name

The model name of the chassis is displayed.

Admin LAN (IP address)

The chassis admin IP address is displayed.

Status

The status of the chassis is displayed.

Server blades

The number of server blades mounted in the chassis is displayed.
Displayed only when the chassis of a blade server is selected.

Partition count

The number of mounted partitions is displayed.
Displayed only when the chassis of a PRIMEQUEST, SPARC Enterprise M4000/M5000/M8000/M9000, or FUJITSU M10-4S is selected.

LAN Switch blades

The number of LAN switches mounted in the chassis is displayed.
Displayed only when the chassis of a blade server is selected.

 See
....
Refer to "11.2 Resource Status" in the "Operation Guide VE" for details on resource statuses.
....

Hardware Details Area

Launch Management Blade Web UI

The link to the management blade's Web interface is displayed.
Not displayed for SPARC Enterprise M4000/M5000/M8000/M9000 or FUJITSU M10-4S.

Launch XSCF Web UI

The link to the remote management controller (XSCF) Web UI is displayed.
Only displayed for SPARC Enterprise M4000/M5000/M8000/M9000 or FUJITSU M10-4S.

Partition Configuration

The following information is only displayed when the chassis of a PRIMEQUEST 1000 series, SPARC Enterprise M4000/M5000/M8000/M9000, or SPARC M10-4S is selected.

Partition ID

The partition number is displayed.

Partition name

The name used to identify a partition is displayed.

SB

The ID of the system board used to configure a partition is displayed.

IOB

The ID of the IO board used to configure a partition is displayed.

GSPB (Giga-LAN SAS and PCI_Box Interface Board)

The ID of the GSPB used to configure a partition is displayed.

Reserved SB

The ID of the Reserved SB assigned to a partition is displayed.

LSB

The partition logical system board (LSB) number is displayed.
Only displayed for SPARC Enterprise M4000/M5000/M8000/M9000 or FUJITSU M10-4S.

XSB

The partition eXtended System Board (XSB) number is displayed.
Only displayed for SPARC Enterprise M4000/M5000/M8000/M9000 servers.

PSB

The partition physical system board (PSB) number is displayed.
Only displayed for SPARC M10-4S.

PPAR Configuration

This is only displayed for the PRIMEQUEST 2000 series.

Partition ID

The partition number is displayed.

Partition name

The name used to identify a partition is displayed.

Availability

The availability of the PPAR partition is displayed. When usable, "OK" is displayed. When not usable, "NG" is displayed.

Extended Partition ID

The Extended Partition number is displayed.

SB

The ID of the system board used to configure a partition is displayed.

IOU

The ID of the IOU used to configure a partition is displayed.

DU

The ID of the DU used to configure a partition is displayed.

LPCI_Box

The ID of the PCI_BOX_LH used to configure a partition is displayed.

Reserved SB

The ID of the Reserved SB assigned to a partition is displayed.

Extended Partitioning Configuration

This is only displayed for the PRIMEQUEST 2000 series.

Partition ID

The partition number is displayed.

Physical server name

The name used to identify a server is displayed.

Partition name

The name used to identify a partition is displayed.

Availability

The availability of the Extended Partition is displayed. When usable, "OK" is displayed. When not usable, "NG" is displayed.

PPAR ID

The number of the PPAR to which the Extended Partition is allocated is displayed.

CPU core count

The CPU core count is displayed.

Memory capacity (DIMM)

The total capacity of server memory is displayed.

Memory EXCL

The information of memory EXCL is displayed.

SKT Binding

The information of SKT Binding is displayed.

PCI Express Slot

PCI Express slot information is displayed.

On-board VGA/USB

The information of on-board VGA/USB is displayed.

GbE

GbE information is displayed.

Disk Unit

Disk unit information is displayed.

A.6.2 Server Attributes

General Area

Physical server name

The name used to identify a server is displayed.

Model name

The model name of the server is displayed.
When the server has been registered as a managed server and powered on, the server model name obtained from ServerView Operations Manager is displayed. For other servers, no model name is displayed.

Product name

The product name of the server is displayed.
For PRIMERGY BX servers, the product name obtained from the management blade is displayed. For other servers, the model name is displayed.

Status

Server status is displayed.

Slot

A slot number representing the mounted location is displayed.
Displayed only for PRIMERGY BX servers.

Partition ID

The partition number is displayed.
Only displayed when a PRIMEQUEST, or a SPARC Enterprise M4000/M5000/M8000/M9000 server, or a server in a FUJITSU M10-4S is selected.

Maintenance Mode

The operational status of the server is displayed.

One of the following is displayed:

- active

- maintenance

Not displayed when Fujitsu M10/SPARC Enterprise are selected.

LED status

The illumination status of the maintenance LED is displayed.
Displayed only for PRIMERGY BX servers.

Admin LAN (MAC address 1)

The MAC address of the NIC used for the admin LAN is displayed.
Not displayed when Fujitsu M10/SPARC Enterprise are selected.

CPU core count

The CPU core count is displayed.

CPU type

The type of CPU is displayed.
When using servers other than the following, a hyphen ("-") is displayed.

- PRIMERGY BX Series Servers

- SPARC Enterprise M-Series

- SPARC M10

- PRIMEQUEST

CPU clock speed

CPU clock speed (frequency) is displayed.
When using servers other than the following, a hyphen ("-") is displayed.

- PRIMERGY BX Series Servers

- SPARC Enterprise M-Series

- SPARC M10

- PRIMEQUEST

Memory Size

The total capacity of server memory is displayed.
When using servers other than the following, a hyphen ("-") is displayed.

- PRIMERGY BX Series Servers

- SPARC Enterprise M-Series

- SPARC M10

- PRIMEQUEST

For PRIMEQUEST 2000 series Extended Partition servers, "Memory capacity (DIMM)" is displayed.

Admin LAN (MAC address 2)

The MAC address of the network interface used for the HBA address rename setup service or for admin LAN redundancy is displayed.
For PRIMERGY RX series servers and TX series servers, the MAC address is displayed after HBA address rename settings are configured.
Not displayed when Fujitsu M10/SPARC Enterprise are selected.

Hardware Maintenance Mode

The hardware maintenance mode of the server is displayed.
Displayed only for PRIMEQUEST servers.

Boot option

The boot option setting specified when registering servers is displayed.

Displayed only when a PRIMEQUEST server is selected.

Extended Partitioning Mode

The Extended Partitioning Mode status of the PPAR is displayed.

It is only displayed when the PPAR of a PRIMEQUEST 2000 series is selected.

Dynamic Reconfiguration

The status of Dynamic Reconfiguration is displayed.

It is only displayed when the PPAR of a PRIMEQUEST 2000 series is selected.

See
. . . .

- Refer to the Management Blade's manual for details on management blades' product names.

- Refer to the ServerView Operation Manager manual for details on the server models displayed and obtained from ServerView Operation Manager.

- Refer to "11.2 Resource Status" in the "Operation Guide VE" for details on resource statuses.
. . . .

Hardware Details Area

Server management software

The link to the web interface of a server management software is displayed.
Displayed only for the following servers:

- PRIMERGY Series

- PRIMEQUEST Servers

- SPARC M10/SPARC Enterprise

Remote Management Controller IP address

IP address of the remote management controller is displayed.
Displayed only for servers other than PRIMERGY BX servers and PRIMEQUEST servers.

I/O Virtualization Management Software

The link to the web interface of external I/O virtualization management software is displayed.
Displayed only if coordinated up with external I/O virtualization management software.

VIOM server profile

The assigned VIOM server profile name is displayed.
Displayed only if managed by VIOM and a server profile has been set.

Network Properties Area

Physical Connections

The list of physical connections between the server's network interfaces and LAN switch ports is displayed.
When a column heading in the list is clicked, the color of the selected column will change and the resources can be sorted in either ascending or descending order.

Hardware Maintenance Area

NIC Summary

The MAC addresses and IP addresses of each server are displayed.
For servers other than PRIMERGY BX servers and PRIMEQUEST servers, only admin LAN information is displayed.
For Fujitsu M10/SPARC Enterprise, only the IP address is displayed.

Information

. . . .

The IP address displayed is the one set within the server's operating system.
For network interfaces that were made redundant using BACS software, the information set in BACS (within the operating system) is displayed.

. . . .

Partition Configuration

The following information is displayed only when a PRIMEQUEST 1000 series, or a SPARC Enterprise M4000/M5000/M8000/M9000 server, or a server in a FUJITSU M10-4S is selected.

Partition name

The name used to identify a partition is displayed.

SB

The ID of the system board used to configure a partition is displayed.

IOB

The ID of the IO board used to configure a partition is displayed.

GSPB (Giga-LAN SAS and PCI_Box Interface Board)

The ID of the GSPB used to configure a partition is displayed.

Reserved SB

The ID of the Reserved SB assigned to a partition is displayed.

LSB

The partition logical system board (LSB) number is displayed.
Only displayed for SPARC Enterprise M4000/M5000/M8000/M9000 or FUJITSU M10-4S.

XSB

The partition eXtended System Board (XSB) number is displayed.
Only displayed for SPARC Enterprise M4000/M5000/M8000/M9000 servers.

PSB

The partition physical system board (PSB) number is displayed.
Only displayed for SPARC M10-4S.

The following information is only displayed when the PPAR of a PRIMEQUEST 2000 series is selected.

Partition name

The name used to identify a partition is displayed.

SB

The ID of the system board used to configure a partition is displayed.

IOU

The ID of the IOU used to configure a partition is displayed.

DU

The ID of the DU used to configure a partition is displayed.

LPCI_Box

The ID of the PCI_BOX used to configure a partition is displayed.

Reserved SB

The ID of the Reserved SB assigned to a partition is displayed.

The following information is only displayed when the Extended Partition of a PRIMEQUEST 2000 series is selected.

Partition name

The name used to identify a partition is displayed.

Partition ID (PPAR)

The partition number is displayed.

Partition name (PPAR)

The name of the PPAR partition is displayed.

Physical server name (PPAR)

The physical server name of the PPAR is displayed.

Memory EXCL

The information of memory EXCL is displayed.

SKT Binding

The information of SKT Binding is displayed.

PCI Express Slot

PCI Express slot information is displayed.

On-board VGA/USB

The information of on-board VGA/USB is displayed.

GbE

GbE information is displayed.

Disk Unit

Disk unit information is displayed.

Extended Partitioning Configuration

It is only displayed for PPAR of the PRIMEQUEST 2000 series.

Partition ID

The partition number is displayed.

Physical server name

The name used to identify a server is displayed.

Partition name

The name used to identify a partition is displayed.

Availability

The availability of the Extended Partition is displayed. When usable, "OK" is displayed. When not usable, "NG" is displayed.

PPAR ID

The number of the PPAR to which the Extended Partition is allocated is displayed.

CPU core count

The CPU core count is displayed.

Memory capacity (DIMM)

The total capacity of server memory is displayed.

Memory EXCL

The information of memory EXCL is displayed.

SKT Binding

The information of SKT Binding is displayed.

PCI Express Slot

PCI Express slot information is displayed.

On-board VGA/USB

The information of on-board VGA/USB is displayed.

GbE

GbE information is displayed.

Disk Unit

Disk unit information is displayed.

A.6.3 Physical OS, VM Host, and VM Guest Attributes

General Area

Server name

The name used to identify a physical OS, VM host, or VM guest is displayed.

Admin LAN (IP Address)

The IP address on the admin LAN is displayed.
VM guests are shown using hyphens ("-").

Status

The status of the physical OS, VM host, or VM guest is displayed.

Type

The type of the OS running on the server is displayed.

One of the following is displayed:

- Physical OS

- VM Host

- VM Guest

OS

The type of the OS running on the server is displayed.

Physical server name

The name of the server on which the physical OS, VM host, or VM guest is operating is displayed.
VM guests are shown using hyphens ("-").

See
. . . .
Refer to "11.2 Resource Status" in the "Operation Guide VE" for details on resource statuses.
. . . .

VM Host Information Area

The following information is displayed only for VM Hosts.

VM type

The type of the VM is displayed.

VM software name

The name of the VM software used is displayed.

VM software VL

The version and level of the VM software used is displayed.

Number of VM guests

The number of VM guests is displayed.

VM management software

The link to the web interface of a server virtualization software is displayed.

OVM Configuration Information's XML Saving Status

OVM configuration information is displayed as information saved in XML file.

For details on OVM configuration information's XML saving, refer to "Chapter 18 Server Switchover Settings".

Column	Value	Explanation
OVM configuration XML preservation condition	-	unsaved situation (never have an acquisition operation. Or had acquisition operation but never be successful)
	Success (Last success time: 2013-08-27 11:36:47)	Saved situation. Saving time is also displayed. Display the saving time in the following operations. - automatic saving - GUI/CLI
	Failure(Last success time:2013-05-16 02:50:30)	When last saving operation fails, the output time will displayed as last saving success time.

VM guests

A list of hosted VM guests is displayed.

VM Home Positions (VM Guests)

A list of the VM guests with the selected VM host set as their VM Home Position is displayed.

VM Guest Information Area

The following information is displayed only for VM guests.

VM type

The type of the VM is displayed.

VM host name

The name of the VM host on which the VM guest is stored is displayed.

VM name

The name of the VM is displayed.

VM management software

The link to the web interface of a server virtualization software is displayed.

Hardware Details Area

The following information is not displayed for VM guests.

Server management software

The link to the web interface of a server management software is displayed.
Displayed only for the following servers:

- PRIMERGY Series

- PRIMEQUEST

- SPARC M10/SPARC Enterprise

Remote Management Controller IP address

IP address of the remote management controller is displayed.
Displayed only for servers other than PRIMERGY BX servers.

Latest System Image Area

The following information is not displayed for VM guests or Fujitsu M10/SPARC Enterprise.

Version

The latest version of the system image is displayed.

Backup date

The date and time of the most recent system image backup is displayed.

Comment

Comments describing the system image are displayed.

Spare Server Settings Area

The following information is not displayed for VM guests.

Primary server

Displays the name of the physical server that will be replaced when server switchover occurs.

Active server

Displays the name of the physical server that is currently running.

Server switchover method

The method used to perform server switchover is displayed.

Server boot method

The boot type of the system disk is displayed.

Automatic server recovery

Shows whether automatic server recovery is enabled or not.

Network switchover

Shows whether network settings will be automatically adjusted during server switchover.

Force spare server to power off during switchover

The setting whether the spare server is turned off forcibly when switching over to the spare server is displayed.

Switch over to spare server running VM guests

The setting whether the server is switched to a VM host on which a VM guest exists is displayed.

Spare server

Displays the name of the physical server that will replace the current active server when server switchover occurs.

HBA Address Rename Settings Area

The following information is not displayed for VM guests or Fujitsu M10/SPARC Enterprise.

WWNN

The WWNN set on the HBA is displayed.

WWPN 1

The first WWPN set on the HBA is displayed.
The WWPN should be set to the I/O address of each HBA (in descending order).
Therefore, for rack mount or tower servers, the order may not correspond with port number order described for the HBA.

WWPN 2

The second WWPN set on the HBA is displayed.

The WWPN should be set to the I/O address of each HBA (in descending order).

Therefore, for rack mount or tower servers, the order may not correspond with port number order described for the HBA.

Network Properties Area (VLAN)

The following information is not displayed for VM guests.

Index

The mounted position (index) of each network interface on the server is displayed.

Port VLAN

The port VLAN IDs set on the LAN switch ports connected to each network interface are displayed.

When connected to a PRIMERGY BX900/BX400 LAN switch blade operating in IBP mode, "(IBP)" is displayed.

When connected to a PRIMERGY BX900/BX400 LAN switch blade operating in Converged Fabric mode, "(Converged Fabric)" is displayed.

Tagged VLAN

The tagged VLAN IDs set on the LAN switch ports connected to each network interface are displayed.

When connected to a PRIMERGY BX900/BX400 LAN switch blade operating in IBP mode, "(IBP)" is displayed.

When connected to a PRIMERGY BX900/BX400 LAN switch blade operating in Converged Fabric mode, "(Converged Fabric)" is displayed.

Port Groups Area (IBP)

NIC Index

The mounted position (index) of each network interface on the server is displayed.

Group

The names of the port groups set on the LAN switch ports connected to each network interface (for LAN switch blades operating in IBP mode) are displayed.

Only "-" is displayed under the following conditions.

- The corresponding LAN switch is not registered

- The corresponding LAN switch is not operating in IBP mode

- The corresponding LAN switch port has not been assigned to a port group

Monitoring Information

Timeout(sec)

The time-out value (in seconds) for ping monitoring is displayed.

Recovery method

The recovery performed when an error is detected is displayed.

Number of reboots

The number of times reboot is performed during recovery is displayed.

WWN Settings Area

The following information is not displayed for VM guests or servers other than Fujitsu M10/SPARC Enterprise.

WWPN of port *n* (*n*:1-8)

The WWPN value of the port *n* is displayed.
Values set by users are reflected on WWPN.

Target CA WWPN

The WWPN for the CA connected to the port *n* is displayed.

Target CA AffinityGroup

The AffinityGroup for the CA connected to the port *n* is displayed.

Automatic Network Configuration

The following information is displayed when the VM host is a target of network auto configuration and only when automatic network configuration has been performed.

Network resource name

The network resource name for which automatic network configuration is performed is displayed.

VLAN ID

The VLAN ID configured for the network resource is displayed.

Subnet Address

The subnet address configured for the network resource is displayed.
When it is not configured, "-" is displayed.

Subnet Mask

The subnet mask configured for the network resource is displayed.
When it is not configured, "-" is displayed.

A.6.4 LAN Switch Blade Attributes

General Area

LAN switch name

The name used to identify a LAN switch blade is displayed.

System Name (sysName)

The name of the device specified as a LAN switch blade is displayed.

Admin port

The Admin port to be used for communication with the admin server is displayed.

IP address

The IP address to be used for communication with the admin server is displayed.

For PY CB 10Gb FEX Nexus B22, a hyphen ("-") is displayed.

Device name (Product name)

The product name of a LAN switch blade is displayed.

Model

The model name of a LAN switch blade is displayed.

Serial number

The serial number of a LAN switch blade is displayed.

Firmware version

The firmware version of a LAN switch blade is displayed.

Device status

The status of a LAN switch blade is displayed.

One of the following is displayed:

- normal

- error

- warning

- unknown

Slot

A slot number representing the mounted location is displayed.

VCS ID

A VCS ID is displayed.

When VCS is not configured, a hyphen ("-") is displayed.

RBridge ID

An RBridge ID is displayed.

When VCS is not configured, a hyphen ("-") is displayed.

Fabric ID

A Fabric ID is displayed.

When Converged Fabric is not configured, a hyphen ("-") is displayed.

Domain ID

A Domain ID is displayed.

When Converged Fabric is not configured, a hyphen ("-") is displayed.

Switch ID

A Switch ID is displayed.

When Converged Fabric is not configured, a hyphen ("-") is displayed.

Hardware Details Area

Launch Switch Blade Web UI

A link to the Web interface of the LAN switch blade is displayed.

Note

If no Web interface is available for the selected LAN switch blade, the following message is displayed: "There is no information to display".
Refer to the LAN switch blade manual to confirm whether or not a Web interface is provided.

Port Properties Area

Port Number

The number of the port of the selected LAN switch blade is displayed.

Port Name

The name assigned to the port of the selected LAN switch blade is displayed.

For PY CB 10Gb FEX Nexus B22, internal ports are displayed as 1/1 - 1/16, external ports (from number 1 to 8) are displayed as -/17 - -/24.

Link Status

The operational status of the port is displayed.

One of the following is displayed:

- up

- down

- unknown

For a LAN switch blade operating in Converged Fabric mode or PY CB 10Gb FEX Nexus B22, a hyphen ("-") is displayed.

Speed/DuplexMode

The speed and duplex mode of the operating port are displayed.

For a LAN switch blade operating in Converged Fabric mode or PY CB 10Gb FEX Nexus B22, a hyphen ("-") is displayed.

Link aggregation group name

The name of the link aggregation group to which the port of the selected LAN switch blade belongs.
If it does not belong to link aggregation, a hyphen ("-") is displayed.

Link aggregation information

The following information is only displayed when LAN switch blades (*) are selected.

Link aggregation group name

The name of the link aggregation group to which the port of the selected LAN switch blade belongs is displayed.

Port name

The link aggregation port name is displayed.

- For PY-SWB104 (PG-SW109)

    LAG/Link aggregation group number

- For PY-SWB101 (PG-SW201) or PY-SWB102(PG-SW111)

    Logical port number of the LAG/port channel

Member port:Link status

The physical port names and the link status (up or down) of the physical ports are displayed for the ports in the link aggregation.

VLAN

VLAN ID

A list of VLAN IDs set in the selected LAN switch blade is displayed.

Untagged Port(s)

A list of ports set with a port VLAN ID is displayed.
The logical port for link aggregation is only displayed for LAN switch blades (*).

Tagged Port(s)

A list of ports set with tagged VLAN ID(s) is displayed.

The logical port for link aggregation is only displayed for LAN switch blades (*).

* Note: The following LAN switch blades are included:

- PY CB Eth Switch/IBP 10Gb 18/8

- PY CB Eth Switch/IBP 1Gb 36/8+2

- PY CB Eth Switch/IBP 1Gb 36/12

- PY CB Eth Switch/IBP 1Gb 18/6

Port Groups Area (IBP)

The following information is only displayed for a LAN switch blade operating in IBP mode.

Group

The name of a port group configured on the selected LAN switch blade is displayed.

Group Type

The type of this port group is displayed.

One of the following is displayed:

- Port Group

- VLAN Port Group

- Service LAN

- Service VLAN

VLAN IDs

VLAN IDs assigned to this port group are displayed.

Downlink Ports

The name of the downlink ports assigned to this port group is displayed.

Uplink Set

The name of the UplinkSet assigned to this port group is displayed.

Uplink Sets(IBP)

The following information is only displayed for a LAN switch blade operating in IBP mode.

Uplink Set

The name of an UplinkSet (set of external ports) configured on the selected LAN switch blade is displayed.

Active Ports

The name of the active port within the port backup configuration of this UplinkSet is displayed.

Backup Ports

The name of the backup port within the port backup configuration of this UplinkSet is displayed.

Link State

Displays whether link state functionality is enabled or not for this UplinkSet.

- enable

- disable

Port Backup

Displays whether port backup functionality is enabled or not for this UplinkSet.

- enable

- disable

IGMP Snooping

Displays whether IGMP snooping is enabled or not for this UplinkSet.

- enable

- disable

LACP

Displays whether LACP is enabled or not for this UplinkSet.

- enable

- disable

Network links

Resource Name (left side)

The name of the selected LAN switch blade is displayed.

I/F (left side)

The port name of the LAN switch blade is displayed.

For PY CB 10Gb FEX Nexus B22, internal ports are displayed as 1/1 - 1/16, external ports (from number 1 to 8) are displayed as -/17 - -/24.

I/F (right side)

The interface name of the resource connected to the LAN switch blade is displayed.

Resource Name (right side)

The name of the resource connected to the LAN switch blade is displayed.

![Note icon] Note

Information about connections with network devices is not displayed.

A.6.5 Network Device Attributes

General Area

Network device name

The name used to identify a network device is displayed.

System Name (sysName)

The name of the device specified as a network device is displayed.

IP address

The IP address to be used for communication with the admin server is displayed.

Device name (Product name)

The product name of the network device is displayed.

Model

The model name of a network device is displayed.

Vendor

The vendor name of a network device is displayed.

Serial number

A hyphen ("-") is displayed.

Firmware version

The firmware version of a network device is displayed.

Device status

The status of a network device is displayed.

One of the following is displayed:

- normal

- unknown

Slot

A hyphen ("-") is displayed.

Hardware Details Area

Launch Network Device Web UI

A link to the Web interface of the network device is displayed.

 Note

. . . .

If no Web interface is available for the selected network device, the following message is displayed: "There is no information to display". Refer to the manual of the network device to confirm whether a Web interface is provided.

. . . .

Port Properties Area

Port Number

The number of the port of the selected network device is displayed.

Port Name

The name assigned to the port of the selected network device is displayed.

Member Port

When the name of a port with link aggregation is displayed for the port name, the port names of the physical port with link aggregation are displayed separated by commas (",").
When the physical port name is displayed as the port name, a hyphen ("-") is displayed.
This is not displayed when an Ethernet Fabric is selected.

Link Status

The operational status of the port is displayed.

One of the following is displayed:

- up

- down

- testing

- unknown

- dormant

- notPresent

- lowerLayerDown

Speed/DuplexMode

The speed and duplex mode of the operating port are displayed.

VLAN Area

VLAN ID

A list of VLAN IDs set in the selected network device is displayed.
When an Ethernet Fabric is selected, only VLANs that are defined for the default VFAB are displayed.

Untagged Port(s)

A list of ports set with a port VLAN ID is displayed.
The logical port for link aggregation is not displayed.
When an Ethernet Fabric is selected, only VLANs that are defined for the default VFAB are displayed.

Tagged Port(s)

A list of ports set with tagged VLAN ID(s) is displayed.
The logical port for link aggregation is not displayed.
When an Ethernet Fabric is selected, only VLANs that are defined for the default VFAB are displayed.

A.6.6 Virtual Fabric Attributes

General Area

VFAB name

The name of VFAB is displayed.

VFAB ID

1 - 3,000 is displayed for VFAB ID.

S-TAG

101 - 3,100 is displayed for VFAB S-TAG.

Operation mode

The operation mode of VFAB is displayed.

- host

- network

VFAB auto configuration

Whether the VFAB is automatically configured is displayed.

- true

- false

Tenants

The name of the tenant belonging to the VFAB is displayed.
When it belongs to multiple tenants, there is a line for each tenant.

Port Properties Area

Port Number

The numbers of the ports related to the selected virtual fabric is displayed.

Port Name

The name assigned to the port related to the selected virtual fabric is displayed.

Link Status

The operational status of the port is displayed.
One of the following is displayed:

- up

- down

- testing

- unknown

- dormant

- notPresent

- lowerLayerDown

Speed/Duplex Mode

The speed and duplex mode of the operating port are displayed.

Link Aggregation Group

When the name of the port which comprises the link aggregation is displayed as the port name, the link aggregation name is displayed.
When the name of the port which comprises the link aggregation is not displayed as the port name, a hyphen ("-") is displayed.

Port Type

The port type of the network device is displayed.
One of the following is displayed:

- EP

- CIR

- EP(dot1ad)

  Displayed when using the EP port for sending and receiving of the IEEE802.1ad frame.

- CIR(dot1ad)

  Displayed when using the CIR port for sending and receiving of the IEEE802.1ad frame.

Link Aggregation Properties Area

Link Aggregation Group

The link aggregation group name is displayed.

Port Name

A hyphen ("-") is displayed as the port name of the link aggregation port.

Member Port:Link Status

The name of the port and the link status which comprise the link aggregation are displayed in the link status "Port Name: Link Status".

VLAN Area

VLAN ID

A list of the VLAN IDs set in the selected virtual fabric is displayed.

Untagged Port(s)

A list of ports set with a port VLAN ID is displayed.
The logical port for link aggregation is not displayed.

Tagged Port(s)

A list of ports set with tagged VLAN ID(s) is displayed.
The logical port for link aggregation is not displayed.

A.6.7   Power Monitoring Devices (PDU or UPS) Attributes

General Area

Device name

The name used to identify a PDU or UPS is displayed.

Admin LAN (IP address)

The IP address on the admin LAN is displayed.

Device type

The device type (PDU or UPS) is displayed.

Model

The model name of the PDU or UPS is displayed.

Comment

Comments entered when registering a PDU or UPS are displayed.

Hardware Details Area

Serial number

The serial number of the PDU or UPS is displayed.

Voltage

The voltage supplied to the PDU or UPS is displayed.

Hardware version

The hardware version of the PDU is displayed.
This is not displayed for UPSs.

Firmware version

The firmware version of the device (PDU or UPS) is displayed.

Date of manufacture

The date of manufacture of the PDU or UPS is displayed.

Outlets

The number of outlets provided by the PDU is displayed.
This is not displayed for UPSs.

Intended orientation

The intended orientation (horizontal or vertical) of the PDU is displayed.
This is not displayed for UPSs.

A.6.8   Management Software Attributes

General Area

Management software name

The name used to identify the management software is displayed.

Type

The type of the management software is displayed.

One of the following is displayed:

- vCenter Server

- SCVMM

- VIOM

IP address

The IP address used to connect to the management software is displayed.

Status

The status of the management software is displayed.

Note

....

For the following management software, "normal" is always displayed.

- VIOM

- SVFAB

- VDI management software

....

Management software

A link to the web interface of the management software is displayed.

A.7 [Recovery Settings] Tab

The [Recovery Settings] tab displays a list of spare servers assigned to the resource selected in the server resource tree.
The table below shows the information displayed in the [Recovery Settings] tab.

[Recovery Settings] Tab

Server Name

The name used to identify a physical OS or VM host is displayed.

Admin LAN IP Address

The IP address on the admin LAN is displayed.

Primary Server

The name of the server on which the physical OS or VM host is operating is displayed.

Switchover State

The current switchover state is displayed.

Spare Server

The configured spare server is displayed.

The switchover state is indicated by an arrow shown next to the currently active Primary Server. The messages "Switchover in progress", "Failback in progress", or "Takeover in progress" are displayed respectively during a server switchover, failback, or takeover process.
If more than one spare server has been set, the first server listed is the one that is currently running.

Clicking a column heading in this list will change the color of the selected column and sort the displayed recovery settings in either ascending or descending order.
In each page of the list, 10 items can be displayed. It is possible to move forwards and backwards by single pages, and to the first or last page.

A.8 [Image List] Tab

The [Image List] tab displays information regarding available images.
Those lists can be used to manage both system images and cloning images.

The following two tables list the items that are displayed in System Image List and Cloning Image List.

System Image List

Server Name

The name used to identify a physical OS or VM host is displayed.

Version

The latest version of the system image is displayed.

Backup Date

The date and time of the most recent system image backup is displayed.

Comment

Comments describing the system image are displayed.

Cloning Image List Area

Cloning Image Name

The name used to identify a cloning image is displayed.

Version

The version of the cloning image is displayed.

Collection Date

The name used to identify a cloning image is displayed.

OS

The name of the operating system stored in the cloning image is displayed.

Comment

Comments describing the cloning image are displayed.

Right-clicking a resource in the list displays a list of available operations in a popup menu.
Refer to "A.2.2 Popup Menus" for details on the operations available from popup menus.
Clicking a column heading in this list will change the color of the selected column and sort images in either ascending or descending order.
In each page of the list, 10 items can be displayed. It is possible to move forwards and backwards by single pages, and to the first or last page.

A.9 Event

This section describes the event area of the ROR console.

Figure A.12 Event

The event log displays a history of events that have occurred on managed resources. These events are added to the log automatically. Each event provides the following information.

Event Information

Status

Displays the level of the event.
There are three levels: "Error", "Warning", or "Info".

Date

Date and time at which the event occurred.

Resource Name

Name of the resource associated with the event.

Event ID

Identifier related to the event.
No event ID is displayed for network resources.

Event Log

Content of the event.

When the link in the [Event Log] column is clicked, an error dialog is displayed. The error dialog provides detailed information of events.

Events can be filtered using the checkboxes displayed in the window.
Selecting a checkbox will show the events whose status corresponds to that of the selected checkbox. Clearing a checkbox will hide such events.
When <Filter> is clicked in the window, the [Filter Settings] dialog is displayed. For the events displayed in the list, the necessary conditions can be set after selecting "match all" or "match any":

 - Event Log

 - Date

The conditions set for events are displayed above the list. To clear the conditions, click <x> displayed on the right of the list.

Clicking a column heading will change the color of the selected column and sort events in either ascending or descending order.
In each page of the list, 10 items can be displayed. It is possible to specify the page to display, move forwards and backwards by single pages, and move to the first or last page.

📝 Note

. . . .

When a resource's status becomes "fatal", its related event shows an "Error" status in the [Status] column. For this reason, the actual status of a resource should be confirmed from either the resource tree or the [Resource List] tab.

. . . .

📖 Information

. . . .

For the SPARC Enterprise T series, the following levels are displayed for SEVERITY values of hardware SNMP Trap MIBs (SUN-HW-TRAP-MIB.mib).

- When SEVERITY is Critical or Major:

  "Error" is displayed.

- When SEVERITY is Minor:

  "Warning" is displayed.

- When SEVERITY is Informational:

  "Info" is displayed.

. . . .

A.10 Recent Operations

This section describes the recent operations area of the ROR console.

Figure A.13 Recent Operations

The recent operations area shows the status of operations that were recently performed. The result of a completed operation shows the operation's completion time and the related resource name. For operations that are still running, a progress bar is shown to indicate the current progress state.

Each operation displayed in the recent operation area provides the following information.

Information Displayed in the Recent Operations Area

Operation

    The executed operation and the target resource name are displayed.
    The process name is displayed while the process is being executed.

Started

    The date and time at which the operation was started is displayed.

Status

    The status of the executed operation is displayed.
    The date and time at which the process was completed is displayed.

 ⓟ **Point**

. . . .

When an operation is executed in a tab other than the [Resource] tab, e.g., the [L-Platform] tab, multiple entries might be displayed in the Recent Operations for that single operation.

When multiple entries are displayed, match the resource name displayed in the tab on which the operation has been executed, to the resource name in the [Operation] column to locate the operation in concern.

. . . .

When the link in the [Operation] column is clicked, the [Progress Details] dialog is displayed.

The [Progress Details] dialog displays the following information:

Progress List

The list of the executed processes and the status are displayed for the selected operation.

If an operation is performed simultaneously for multiple resources, the processes are displayed in a tree view for each target resource.

Message List

The list of any error messages that occurred during the operation is displayed.

Detailed information is displayed under the list when each message is selected.

For the operation that can be canceled, the <Cancel> link is displayed to the right of the [Status] column.

Clicking this link displays a confirmation dialog for canceling the operation.

A.11 Dialogs

This section explains how to enable or disable display of some of the confirmation (or warning) dialogs used by the ROR console.

Use the following procedure to change dialog display settings:

1. Select [Tools]-[Options] from the ROR console menu.

   The [Options] dialog is displayed.

2. Click the "Dialog" category title, and change the following settings in the displayed area.

   Dialog display options (checkboxes)

   To disable further display of a confirmation or warning dialog, select its corresponding checkbox.
   To restore display of a disabled dialog, deselect its corresponding checkbox.

   <Select All> button

   Selects all dialog checkboxes.

   <Deselect All> button

   Deselects all dialog checkboxes.

3. Click <Apply>.

The new settings are applied.

Appendix B Format of CSV System Configuration Files

This appendix explains the format of the CSV system configuration files used by Resource Orchestrator's pre-configuration function.

B.1 Obtaining the System Configuration File (CSV Format)

The system configuration files can be obtained as follows.

- From the selection window of the Resource Orchestrator DVD-ROM [Windows]

  Setting the Resource Orchestrator DVD-ROM in the CD-ROM drive automatically displays the screen below. Select "Tool" and click "System Configuration Template (CSV format)". The CSV file will be opened from the associated application (such as Excel). Check the file content and save it.

Figure B.1 Selection Window

Information

If the above window does not open, execute "RcSetup.exe" from the DVD-ROM drive.

- From the Resource Orchestrator DVD-ROM

  Set the Resource Orchestrator DVD-ROM in the DVD-ROM drive and copy the following file.

  [Windows]
  DVD-ROM_drive\template\ja\template.csv

  [Linux]
  DVD-ROM_mount_point/template/ja/template.csv

- From the ROR console

  The System Configuration Template can be obtained from a Resource Orchestrator manager installation.

1. Open and log in to the ROR console according to "Chapter 1 Login and Logout".

2. Select [File]-[System Configuration File]-[Download Template] from the ROR console menu.

   Displays the [File Download] window.

3. Click <Save>.

4. Specify the destination directory and the file name.

5. Click <Save>.

B.2 File Format

The system configuration files (CSV format) used for pre-configuration are comma (",") delimited.
The format of each line is given below:

- File Format Definition

  The first line of the file must begin with the following:

  ```
  RCXCSV,V3.5
  ```

P Point

....

Resource Orchestrator can import the following system configuration file formats.

- RCXCSV,V1.0

- RCXCSV,V2.0

- RCXCSV,V3.0

- RCXCSV,V3.1

- RCXCSV,V3.2

- RCXCSV,V3.3

- RCXCSV,V3.4

- RCXCSV,V3.5

However, system definition files are always exported in the most recent format: importing a file in an older format and re-exporting it will produce a file in the latest format.

....

Note

....

Although each RCXCSV version has a different format, those formats are retro-compatible (newer formats include all the information defined in older formats).
As detailed below, some sections (described in "B.3 Resource Definitions") are only available with the latest format(s).

- RCXCSV V2.0 and Later

  "LanSwitchNet", "ServerAgent", "ServerVMHost", "PowerDevice", "Memo"

- RCXCSV V3.0 and Later

  "VMManager"

- RCXCSV V3.1 and Later

  "SPARCEnterprise"

- RCXCSV V3.2 and Later

  "PRIMERGYPartitionModelChassis", "PRIMERGYPartitionModelServer"

- RCXCSV V3.3 and Later

  "Subnet", "SPARCEnterprisePartitionModelChassis", "SPARCEnterprisePartitionModelServer", "MonitorSetting"

- RCXCSV V3.4 and Later

  "VIOManager"

- RCXCSV V3.5 and Later

  "SPARC", "SPARCM10PartitionModelChassis", "SPARCM10", "SPARCM10PartitionModelServer"

  SPARC Enterprise (M3000-/T series) performs import/export of a system configuration file (CSV format) by a section name [SPARC].
  The section name [SPARCEnterprise] only imports a system configuration file (CSV format).

- Comment

  The following lines are assumed to be comments and are skipped:

  - Lines that begin with the symbol ("#")

  ## Example

  ```
  #Development environment
  definition
  ```

  - Lines that consist of only blank spaces (" "), tab characters, or linefeed code

  - Lines that contain only commas (",")

  - Unrecognized resource definition

- Resource Definitions

  Create the resource definition using the following format. Describe the same type of resource in the same section.

  - Resource Definition Format

    ```
    [Section name]
    Section Header
    Operation column, Parameter [,parameter]...
    ```

  - Section Name

    This describes the resource type.

  - Section Header

    This describes the parameter type unique to the resource.

  ## Note

  Do not enter any comments between the section name and section header.

  - Operation Column

    This describes the operation type for the resource. The following characters can be used in the operation column.

    - new

      Register

    - change

      Modification

- Hyphens, ("-")

  Do nothing

- Parameters

  This describes the parameter value to be set.

Note

The order of operation and parameter columns should follow the order defined in section header under "B.3 Resource Definitions".

Allowed Characters

For details on the characters allowed for each resource definition, refer to "B.3 Resource Definitions". Optional parameters can be omitted by using hyphens ("-").
However, hyphens ("-") are seen as valid characters for user names, passwords, and SNMP communities. Note that if extra commas (",") are added to the end of a line, those will be simply ignored without errors.

Backslashes ("\") and double quotations (") will be displayed differently in the ROR console from how they appear in the system configuration file.
Refer to the following table for details on such differences.

Table B.1 Differences between System Configuration Files' Contents and Display in the ROR Console

Content of a System Configuration File (CSV)	Display in the ROR Console
\\	\
\n	Line break
""	"
, (*)	,

* Note: The whole value must be enclosed by double quotations (").

Example

- CSV Content

  "a\nb,\\n"

- Display in the ROR Console

  A
  b,\n

Order of Section Definition

Section order and section name are shown below.
Moreover, the section definition order is fixed.

Table B.2 Section Order and Section Names

Order	Section Name
1	Subnet
2	VIOManager
3	Chassis
4	PRIMERGYPartitionModelChassis
5	SPARCEnterprisePartitionModelChassis

Order	Section Name
6	SPARCM10PartitionModelChassis
7	LanSwitch
8	LanSwitchNet
9	Server
10	SPARCEnterprise
11	PRIMERGYPartitionModelServer
12	ServerNet
13	SPARCEnterprisePartitionModelServer
14	SPARC
15	SPARCM10
16	SPARCM10PartitionModelServer
17	ServerWWNN (*1)
18	SpareServer (*1)
19	VMManager
20	ServerAgent (*2, *3)
21	ServerVMHost (*2, *3)
22	MonitorSetting
23	PowerDevice
24	Memo (*2)

*1: When loading from the system configuration template in the Excel format, the operation column information will be skipped.

*2: When loading from the system configuration template in the Excel format, the whole section will be skipped.

*3: Do not enter the information of the same physical server both in the "ServerAgent" and "ServerVMHost" section.

System backup information is automatically added to the end of the system configuration file when exporting in the CSV format. The sections after the line below contain the backup information. The backup information is skipped when loading from the system configuration template in the Excel format.

```
#Do not edit the following information, which is used to recover the manager.
```

Do not modify the backup information, as it is automatically created. Note that these sections do not have to be defined if the system configuration file is created for new system configuration.

Note

....

- If a system configuration file (CSV format) is imported and then exported, the line order after export may differ from the line order before import.

    The following information will also be deleted:

    - Comments lines

    - Strings enclosed in parenthesis "( )" indicating omitted values

    - Extra commas at the end of lines (",")

- As with chassis for server blades, and chassis for LAN switch blades, items that need to be registered in advance to enable registration of other should be defined in the system configuration file or registered in advance.

....

Character Code

The system configuration files (CSV format) used for pre-configuration are saved using ASCII (often referred to as "ANSI" in Windows systems). When files that use a character code other than ASCII are imported, the system may not operate correctly.
When directly editing configuration files using a text editor, please do not save the file using a character code other than ASCII.

B.3 Resource Definitions

This section explains the resource definition information specified system configuration files.

Admin LAN Subnet Data

- **Section Name**

Enter [Subnet] as the section name.

- **Section Header**

operation

Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

subnet_name

Enter the subnet name.
Enter a character string beginning with an alphabetic character and containing up to 16 alphanumeric characters, underscores ("_"), hyphens ("-"), and periods (".").

network_address

Enter the network address for the subnet used as the admin LAN.
Enter valid values for the network address.

subnet_mask

Enter valid values for the subnet mask.

gateway

Enter the settings for the gateway used for communication with the admin server on the admin LAN.

VIOM Data

- **Section Name**

Enter [VIOManager] as the section name.

- **Section Header**

operation

Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

name

Specify "VIOM".

ip_address

Enter the IP address of the terminal on which VIOM is installed.
Specify "127.0.0.1".

login_name

Enter the name of a VIOM user account.
When specifying a domain, use the following syntax: "*domain_name**user_name*".

login_passwd

 Enter the password of the above VIOM user account.

passwd_enc

 Enter one of the following.

  - If login_passwd is plain text

   "plain"

  - If the password is encrypted

   "encrypted"

Chassis Data

- **Section Name**

 Enter [Chassis] as the section name.

- **Section Header**

operation

 Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

chassis_name

 Enter the name that will be used to identify the chassis.
 Enter a character string beginning with an alphabetical character and containing up to 10 alphanumeric characters and hyphens ("-").

Note

....

Chassis names should be unique between all chassis. Names are not case-sensitive.

....

ip_address

 Enter the same IP address as that set on the management blade.
 Enter a string of numeric values (between 0 and 255) and periods.

Note

....

IP addresses should be unique between all resources.

....

snmp_community_name

 Enter the same SNMP community (read-write permission) as that set on the management blade.
 Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

PRIMEQUEST Chassis Management Data

- **Section Name**

 Enter [PRIMERGYPartitionModelChassis] as the section name.

- **Section Header**

operation

 Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

chassis_name

Enter the name that will be used to identify the chassis.
Enter a character string beginning with an alphabetical character and containing up to 10 alphanumeric characters and hyphens ("-").

📋 **Note**
. . . .

Chassis names should be unique between all chassis.
Names are not case-sensitive.
. . . .

ip_address

Enter the same IP address as that set on the management board.
Enter a string of numeric values (between 0 and 255) and periods.

📋 **Note**
. . . .

IP addresses should be unique between all resources.
. . . .

snmp_community_name

Enter the same SNMP community (read-write permission) as that set on the management board.
Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

mgmt_user_name

Enter the name of a remote server management user account with administrative privileges.
This user name must be between 8 and 16 alphanumeric characters long.

mgmt_passwd

Enter the password of the remote server management account.
This password must be between 8 and 16 alphanumeric characters long.

mgmt_passwd_enc

Enter one of the following.

  - If mgmt_passwd is plain text

    "plain"

  - If the password is encrypted

    "encrypted"

SPARC Enterprise M4000/M5000/M8000/M9000 Chassis Management Data

- **Section Name**

Enter [SPARCEnterprisePartitionModelChassis] as the section name.

- **Section Header**

operation

Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

chassis_name

Enter the name that will be used to identify the chassis.
Enter a character string beginning with an alphabetical character and containing up to 10 alphanumeric characters and hyphens ("-").

ip_address

Enter the same IP address as that configured on the XSCF.
Enter a string of numeric values (between 0 and 255) and periods.

snmp_community_name

Enter the name of a SNMP community (with read permission) configured on this server's remote management controller (XSCF).
Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

mgmt_user_name

Enter the name of a remote management controller (XSCF) user account with administrative privileges ("platadm" privileges).
Enter a string of up to 31 alphanumeric characters, hyphens ("-"), and underscores ("_"). This name must start with an alphabet character.

mgmt_passwd

Enter the password of the remote management controller (XSCF) user account.
Enter up to 32 characters, including alphanumeric characters, blank spaces (" "), and any of the following symbols.
"!", "@", "#", "$", "%", "^", "&", "*", "[", "]", "{", "}", "(", ")", "-", "+", "=", "~", ",", ">", "<", "/", "'", "?", ";", ":"

mgmt_passwd_enc

Enter one of the following.

- If mgmt_passwd is plain text

  "plain"

- If the password is encrypted

  "encrypted"

SPARC M10-4S Chassis Management Data

- **Section Name**

Enter [SPARCM10PartitionModelChassis] as the section name.

- **Section Header**

operation

Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

chassis_name

Enter the name that will be used to identify the chassis.
Enter a character string beginning with an alphabetical character and containing up to 10 alphanumeric characters and hyphens ("-").

> **Note**
> ....
> Chassis names should be unique between all chassis.
> Names are not case-sensitive.
> ....

ip_address

Enter the same IP address as that configured on the XSCF.
Enter a string of numeric values (between 0 and 255) and periods.

> **Note**
> ....
> IP addresses should be unique between all resources.
> ....

snmp_community_name

Enter the name of a SNMP community (with read permission) configured on this server's remote management controller (XSCF).
Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

mgmt_user_name

Enter the name of a remote management controller (XSCF) user account with administrative privileges ("platadm" privileges).
Enter a string of up to 31 alphanumeric characters, hyphens ("-"), and underscores ("_"). This name must start with an alphabet character.

mgmt_passwd

Enter the password of the remote management controller (XSCF) user account.
Enter up to 32 characters, including alphanumeric characters, blank spaces (" "), and any of the following symbols.
"!", "@", "#", "$", "%", "^", "&", "*", "[", "]", "{", "}", "(", ")", "-", "+", "=", "~", ",", ">", "<", "/", "'", "?", ";", ":"

mgmt_passwd_enc

Enter one of the following.

- If mgmt_passwd is plain text

  "plain"

- If the password is encrypted

  "encrypted"

LAN Switch Blade Data

- **Section Name**

  Enter [LanSwitch] as the section name.

- **Section Header**

  operation

  Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

  chassis_name

  Enter the chassis name (the value of "chassis_name" in the [Chassis] section).

  slot_no

  Enter the slot number where the LAN switch blade is installed. Enter a number between 1 and 8.

  switch_name

  Enter the name to assign to this LAN switch blade.
  Enter a string of up to 15 alphanumeric characters, underscores ("_"), and hyphens ("-").

ip_address

Enter the same IP address as that set on the LAN switch blade.

Enter a string of numeric values (between 0 and 255) and periods.

For a LAN switch blade PY CB 10Gb FEX Nexus B22, do not enter anything.

When using LAN switch blade PY CB Eth Switch 10/40Gb 18/8+2, enter the IP address of oob.

cfab_ip_address

When using LAN switch blade PY CB Eth Switch 10/40Gb 18/8+2, enter the value.

Enter the same virtual IP address of Converged Fabric as that set on the LAN switch blade.

Enter a string of numeric values (between 0 and 255) and periods.

snmp_community_name

Enter the same SNMP community (read-only permission) as that set on the LAN switch blade.

Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

For a LAN switch blade PY CB 10Gb FEX Nexus B22, do not enter anything.

user_name

Enter the name of the user account used to remotely log into the LAN switch blade.

For a LAN switch blade PY CB DCB SW 10Gb 18/6/6, enter the name of the administrator account for the LAN switch blade.

Enter up to 64 characters, including alphanumeric characters (upper or lower case), underscores ("_"), or hyphens ("-").

For a LAN switch blade PY CB 10Gb FEX Nexus B22, do not enter anything.

passwd

Enter the password of the above user account (for remote login).

Enter a string of up to 80 alphanumeric characters and symbols (ASCII character codes: 0x20, 0x21 or 0x23 to 0x7e) and no double-quotations ("). Passwords entered in this field are seen as plain text passwords.

For a LAN switch blade PY CB 10Gb FEX Nexus B22, do not enter anything.

passwd_enc

Enter one of the following. For a LAN switch blade PY CB 10Gb FEX Nexus B22, do not enter anything.

- If passwd is plain text

  "plain"

- If the password is encrypted

  "encrypted"

privileged_passwd

    Enter the admin password of the above user account.

    Enter a string of up to 80 alphanumeric characters and symbols (ASCII character codes: 0x20, 0x21 or 0x23 to 0x7e) and no double-quotations ("). Passwords entered in this field are seen as plain text passwords.

    For a LAN switch blade PY CB 10Gb FEX Nexus B22, do not enter anything.

privileged_passwd_enc

    Enter one of the following. For a LAN switch blade PY CB 10Gb FEX Nexus B22, do not enter anything.

    - If privileged_passwd is plain text

     "plain"

    - If the password is encrypted

     "encrypted"

product_name

    Enter the model of the LAN switch blade. Note that if a hyphen ("-") is entered, it is treated as "BX600 GbE Switch Blade 30/12". One of the following models can be entered.

    - PY CB Eth Switch/IBP 1Gb 36/12

    - PY CB Eth Switch/IBP 1Gb 36/8+2

    - PY CB Eth Switch/IBP 1Gb 18/6

    - PY CB Eth Switch/IBP 10Gb 18/8

    - PY CB Eth Switch 10/40Gb 18/8+2

    - PY CB DCB SW 10Gb 18/6/6

    - PY CB 10Gb FEX Nexus B22

    - BX600 GbE Switch Blade 30/12

    - PRIMERGY BX600 GbE Switch 16/2x10Gb

    - PRIMERGY BX600 GbE Switch 16x1Gb

    - Cisco Catalyst Blade Switch 3040

connection_type

    Enter the connection method to use for the LAN switch blade.

    If you configure "ssh" for a LAN switch blade which does not support SSH, or specify a character string other than ssh, the configuration is regarded as "telnet".

    If "PY CB DCB SW 10Gb 18/6/6" or "PY CB Eth Switch 10/40Gb 18/8+2" is specified for the product name (product_name) and connection_type is specified as a character string other than telnet, the configuration is regarded as being "ssh".

    - For telnet

     "telnet"

    - For SSH

     "ssh"

VLAN Data for LAN Switch Blades

- **Section Name**

Enter [LanSwitchNet] as the section name.

- **Section Header**

  operation

  Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

  chassis_name

  Enter the chassis name (the value of "chassis_name" in the [Chassis] section).

  port_no

  Enter the port number of an external LAN switch blade port. Enter numeric characters. The port number that can be specified is different depending on the model type.
  For details, refer to the manual of the LAN switch blade to be used.

  vlan_id (optional)

  Enter the VLAN ID and tag type ("/T" for tagged or "/U" for untagged) to be assigned to the specified LAN switch blade port. Enter a VLAN ID followed by tag types. To specify multiple VLAN IDs, separate each set of VLAN settings using semicolons (";"). Both tagged ("/T") and untagged ("/U") VLAN IDs can be used together, but only one untagged ("/U") type is allowed.

  ## Example
  ···
  10/U
  10/U;20/T;30/T
  10/T;20/T
  ···

  ## Note
  ···
  If a hyphen ("-") is entered, VLAN settings will not be performed.
  The settings in this section will be ignored for PRIMERGY BX900/BX400 LAN switch blades operating in IBP mode or Converged Fabric mode.

  The settings in this section will be ignored for a LAN switch blade PY CB DCB SW 10Gb 18/6/6 or PY CB 10Gb FEX Nexus B22.
  ···

Server Management Information

- **Section Name**

  Enter [Server] as the section name.

- **Section Header**

  operation

  Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

  chassis_name

  Enter the chassis name (the value of "chassis_name" in the [Chassis] section).

  ## Note
  ···
  This field is only required for PRIMERGY BX servers.
  ···

  slot_no

  Enter the slot number where the server blade is installed. Enter a number between 1 and 18.

> 📝 **Note**
> ....
>
> - This field is only required for PRIMERGY BX servers.
>
> - When a server blade is registered, Resource Orchestrator does not check the actual slot position, or whether it has been installed properly.
>
> - When registering multi-slot servers, enter only the master slot number.
> ....

server_name

Enter the resource name that will be used to identify the server. Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-"). If enclosed by parentheses "( )", this server will be seen as being in a switched over state, and this line will be ignored when importing the system definition file.

> 📝 **Note**
> ....
>
> Server names should be unique between all servers. Names are not case-sensitive.
> ....

ip_address

Enter the same IP address as that set within the server's operating system.
Enter a string of numeric values (between 0 and 255) and periods.

> 📝 **Note**
> ....
>
> IP addresses should be unique between all resources.
> ....

mac_address

Enter the MAC address of the admin LAN network interface: NIC1 (Index1).
Enter a string delimited by hyphens ("-") or colons (":") ("xx-xx-xx-xx-xx-xx" or "xx:xx:xx:xx:xx:xx").

second_mac_address

Enter the MAC address of the network interface used for the HBA address rename setup service or for admin LAN redundancy.

The second network interface (Index 2) should be used.

Enter a string delimited by hyphens ("-") or colons (":") ("xx-xx-xx-xx-xx-xx" or "xx:xx:xx:xx:xx:xx").

> 📝 **Note**
> ....
>
> - This field can be omitted in the following cases.
>
>   - When not using the HBA address rename setup service
>
>   - When not using GLS for admin LAN redundancy on the managed server
>
>   - For a spare server whose primary servers are not using admin LAN redundancy
>
> - The "second_mac_address" header is the equivalent of the "hbaar_mac_address" header defined in RCXCSV V3.0.
>
>   "hbaar_mac_address" can only be used when "RCXCSV,V3.0" is specified at the top of the imported system configuration file.
>
>   However, this header is automatically changed to "second_mac_address" when exporting a new system configuration file.
> ....

snmp_community_name

Enter the name of the SNMP community (read permission) assigned to this server.
Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

ipmi_ip_address

Enter the IP address of this server's remote management controller.
Enter a string of numeric values (between 0 and 255) and periods.

ipmi_user_name

Enter the name of a remote management controller user account with administrative privileges.
Enter a string of up to 16 alphanumeric characters and symbols (ASCII character codes: 0x20 to 0x7e).

ipmi_passwd

Enter the password of the remote management controller user account.
Enter a string of up to 16 alphanumeric characters and symbols (ASCII character codes: 0x20 to 0x7e).
This field can be omitted if no password has been set for this user account.

ipmi_ passwd_enc

Enter one of the following.

- If ipmi_passwd is plain text

  "plain"

- If the password is encrypted

  "encrypted"

admin_lan1_nic_number

The index of the NIC to use for the admin LAN.
Enter a number (1 or larger).

admin_lan2_nic_number

> The Index number of NICs used for the HBA address rename setup service or for admin LAN redundancy.
>
> Enter a number (1 or larger).
>
> For the following cases, enter a hyphen ("-").
>
> - When not using the HBA address rename setup service
>
> - When redundancy of the admin LAN for managed servers does not use GLS
>
> - When not using as the spare server of a managed server with redundancy configured

Note

··

This field is only required for PRIMERGY BX servers.

··

admin_lan_nic_redundancy

> Enter one of the following.
>
> - When using the NIC specified in the admin_lan2_nic_number as the backup for admin LAN redundancy
>
>   "ON"
>
> - When not using the NIC specified in the admin_lan2_nic_number as the backup for admin LAN redundancy
>
>   "OFF"

SPARC Enterprise M3000/T Series Management Data

- **Section Name**

  Enter [SPARC] as the section name.

- **Section Header**

  operation

  > Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

  server_name

  > Enter the resource name that will be used to identify the server. Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

  ip_address

  > Enter the same IP address as that set within the server's operating system. Enter a string of numeric values (between 0 and 255) and periods.

  mgmt_snmp_community_name

  > Enter the name of a SNMP community (with read permission) configured on this server's remote management controller (ILOM/ XSCF).
  >
  > Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

  mgmt_ip_address

  > Enter the IP address of this server's remote management controller (ILOM/XSCF).
  >
  > Enter a string of numeric values (between 0 and 255) and periods.

Note

··

IP addresses should be unique between all resources.

··

mgmt_protocol

Enter the type of the remote management controller (ILOM/XSCF) to manage servers.

- For SPARC Enterprise M3000 servers

"XSCF"

- For T Series

"ILOM"

mgmt_user_name

Enter the user name (For ILOM, Admin privileges, and for XSCF, platadm privileges) of a remote management controller to manage servers (ILOM/XSCF).

- For XSCF

Enter up to 31 characters, including alphanumeric characters, underscores ("_"), or hyphens ("-"). This name should start with an alphabet character.

- For ILOM

Enter between 4 and 16 characters, including alphanumeric characters, underscores ("_"), or hyphens ("-"). This name should start with an alphabet character.

mgmt_passwd

Enter the password of the remote management controller (ILOM/XSCF) to manage a server.

- For XSCF

Enter up to 32 characters, including alphanumeric characters, blank spaces (" "), and any of the following symbols.

- For ILOM

Enter between 8 and 16 characters, including alphanumeric characters, blank spaces (" "), and any of the following symbols.

"!", "@", "#", "$", "%", "^", "&", "*", "[", "]", "{", "}", "(", ")", "-", "+", "=", "~", ",", ">", "<", "/", "", "?", ";", ":"

mgmt_passwd_enc

Enter one of the following.

- If mgmt_passwd is plain text

"plain"

- If the password is encrypted

"encrypted"

SPARC M10-1/M10-4 Management Data

- **Section Name**

Enter [SPARCM10] as the section name.

- **Section Header**

operation

Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

server_name

Enter the resource name that will be used to identify the server. Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

ip_address

Enter the same IP address as that set within the server's operating system. Enter a string of numeric values (between 0 and 255) and periods.

mgmt_snmp_community_name

Enter the name of a SNMP community (with read permission) configured on this server's remote management controller (XSCF). Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

mgmt_ip_address

Enter the IP address of this server's remote management controller (XSCF).
Enter a string of numeric values (between 0 and 255) and periods.

Note

. . . .

IP addresses should be unique between all resources.

. . . .

mgmt_protocol

Enter the type of the remote management controller (XSCF) to manage servers.
Enter "XSCF".

mgmt_user_name

Enter the name of a remote management controller (XSCF) user account with administrative privileges (platadm privileges).

- For XSCF

Enter up to 31 characters, including alphanumeric characters, underscores ("_"), or hyphens ("-"). This name should start with an alphabet character.

mgmt_passwd

Enter the password of the remote management controller (XSCF) user account.

- For XSCF

Enter up to 32 characters, including alphanumeric characters, blank spaces (" "), and any of the following symbols.

mgmt_passwd_enc

Enter one of the following.

- If mgmt_passwd is plain text

"plain"

- If the password is encrypted

"encrypted"

PRIMEQUEST Server Management Data

- **Section Name**

Enter [PRIMERGYPartitionModelServer] as the section name.

- **Section Header**

operation

Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

chassis_name

Enter the chassis name (the value of "chassis_name" in the [PRIMERGYPartitionModelChassis] section).

partition_no

The number of a partition. Enter a number between 0 and 3.

server_name

Enter the resource name that will be used to identify the server. Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-"). If enclosed by parentheses "( )", this server will be seen as being in a switched over state, and this line will be ignored when importing the system definition file.

ℹ️ **Note**

Server names should be unique between all servers. Names are not case-sensitive.

ip_address

Enter the same IP address as that set within the server's operating system.
Enter a string of numeric values (between 0 and 255) and periods.

ℹ️ **Note**

IP addresses should be unique between all resources.

boot_option

Specify the boot option configured from BIOS when installing the OS.

- When installing using a legacy boot

  "legacy"

- When installing using UEFI

  "uefi"

Server Blade VLAN Data

- **Section Name**

  Enter [ServerNet] as the section name.

- **Section Header**

  operation

  Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

  server_name

  Enter the server name (the value of "server_name" in the [Server] section).

  nic_no

  This is the index number of the server blade's network interface. Enter a number between 1 and 12.

  vlan_id (optional)

  Enter the VLAN ID and tag type ("/T" or "/U") to be assigned to the LAN switch blade port connected to this server's network interface.
  Enter a VLAN ID followed by tag types. To specify multiple VLAN IDs, separate each set of VLAN settings using semicolons (";"). Both tagged ("/T") and untagged ("/U") VLAN IDs can be used together, but only one untagged ("/U") type is allowed.

....

10/U
10/U;20/T;30/T
10/T;20/T

....

....

If a hyphen ("-") is entered, VLAN settings will not be performed.

Use the following NIC indexes to specify LAN expansion cards (if any was mounted).

- PRIMERGY BX600 Servers

  7, 8

- PRIMERGY BX900/BX400 Servers

  5 to 12

For the following cases, this section will be ignored.

- PRIMERGY BX900/BX400 LAN switch blades operating in IBP mode or Converged Fabric mode

- A LAN switch blade PY CB 10Gb FEX Nexus B22

- Internal ports of a LAN switch blade PY CB DCB SW 10Gb 18/6/6 for which an Automatic Migration of Port Profile (AMPP) has been configured.

....

SPARC Enterprise M4000/M5000/M8000/M9000 Server Management Data

- **Section Name**

  Enter [SPARCEnterprisePartitionModelServer] as the section name.

- **Section Header**

  operation

  Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

  chassis_name

  Enter the chassis name (the "chassis_name" in the [SPARCEnterprisePartitionModelChassis] section).

  partition_no

  The number of a partition. Enter a number between 0 and 23.

  server_name

  Enter the resource name that will be used to identify the server.
  Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

....

Server names should be unique between all servers.
Names are not case-sensitive.

....

ip_address

Enter the same IP address as that set within the server's operating system.

Enter a string of numeric values (between 0 and 255) and periods.

📄 **Note**

. . . .

IP addresses should be unique between all resources.

. . . .

SPARC M10-4S Server Management Data

- **Section Name**

  Enter [SPARCM10PartitionModelServer] as the section name.

- **Section Header**

  ### operation

  Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

  ### chassis_name

  Enter the chassis name (the value of "chassis_name" in the [SPARCM10PartitionModelServer] section).

  ### partition_no

  The number of a partition. Enter a number between 0 and 23.

  ### server_name

  Enter the resource name that will be used to identify the server.

  Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

📄 **Note**

. . . .

Server names should be unique between all servers.

Names are not case-sensitive.

. . . .

  ### ip_address

  Enter the same IP address as that set within the server's operating system.

  Enter a string of numeric values (between 0 and 255) and periods.

📄 **Note**

. . . .

IP addresses should be unique between all resources.

. . . .

HBA address rename Information of a Server

- **Section Name**

  Enter [ServerWWNN] as the section name.

- **Section Header**

  ### operation

  Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

server_name

Enter the server name (the value of "server_name" in the [Server] section).

port_count

This is the number of ports that use HBA address rename. Enter a number between 1 and 2.

wwnn

Enter the 16-digit hexadecimal WWNN string of the physical server which uses the HBA address rename function.
Enter a hexadecimal string using alphanumeric characters, with "20 0" as the first three characters.

Note

All WWNNs should be unique between all resources (WWNNs are not case-sensitive). Names are not case-sensitive.

Server Switchover Management Information

- **Section Name**

Enter [SpareServer] as the section name.

- **Section Header**

operation

Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

server_name

Enter the server name (the value of "server_name" in the [Server] section).

spare_server

Enter the physical server name of a server to be assigned as a spare server.
To specify multiple spare servers, separate each server name using semicolons (";"). To remove current spare server settings, enter "-DELETE".

vlan_switch (optional)

Specify whether VLAN settings or port group settings should be automatically transferred to the spare server when a server switchover occurs. Enter "ON", "OFF" or a hyphen ("-").

auto_switch (optional)

This value defines whether to trigger an automatic switchover upon detection of a server failure. Enter "ON", "OFF" or a hyphen ("-").

boot_type

Enter the boot type of the server. Enter one of the following.

   - SAN boot

     "SAN"

   - For local boot

     "local"

   - When using the VIOM server profile to conduct boot settings

     Hyphens, ("-")

spare_server_force_off

Enter whether the spare server is turned off forcibly, when switching over to the spare server. Enter "ON", "OFF" or a hyphen ("-").

spare_server_with_vm_guest

Enter whether the server is switched to a VM host on which a VM guest exists. Enter "ON", "OFF" or a hyphen ("-").

VM Management Software Information

- **Section Name**

Enter [VMManager] as the section name.

- **Section Header**

operation

Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

name

Enter the name used to identify this VM management software. Enter one of the following.

- When using VMware vCenter Server as VM management software.

"vCenterServer"

- When using System Center Virtual Machine Manager as VM management software.

"SCVMM"

ip_address

Enter the IP address used to connect to this VM management software or a hyphen ("-").
Enter a string of numeric values (between 0 and 255) and periods.
If a hyphen ("-") is entered, this VM management software will be seen as being installed on the admin server.

product

Enter the name of this VM management software. Enter one of the following.

- When using VMware vCenter Server as VM management software.

"vmware-vc"

- When using System Center Virtual Machine Manager as VM management software.

"ms-scvmm"

login_name

Enter the name of the user account set for this VM management software.
Use a string of up to 84 alphanumeric characters and symbols (ASCII character codes: from 0x21 to 0x7e). When specifying a domain, use the following syntax: "*domain_name\user_name*".

login_passwd

Enter the password for this VM management software.
Use a string of up to 128 alphanumeric characters and symbols (ASCII character codes: from 0x21 to 0x7e).

passwd_enc

Enter one of the following.

- If login_passwd is plain text

"plain"

- If the password is encrypted

"encrypted"

Server Agent Management Information

- **Section Name**

  Enter [ServerAgent] as the section name.
  This is required when registering multiple agents together (for Windows or Linux managed servers).

- **Section Header**

  operation

    Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.
    The "change" operation cannot be used for this section.

  server_name

    Enter the server name (the value of "server_name" in the [Server] section).

VM Host Management Information

- **Section Name**

  Enter [ServerVMHost] as the section name.
  This is required when registering multiple agents together (for VM host managed servers).

- **Section Header**

  operation

    Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

  server_name

    Enter the server name (the value of "server_name" in the [Server] section).

  vm_login_name

    Enter the name of the user account used to remotely log into the VM Host.

  vm_login_passwd

    Enter the password of the above user account (for remote login).

  vm_passwd_enc

    Enter one of the following.

      - If the password is plain text

        "plain"

      - If the password is encrypted

        "encrypted"

Monitoring Settings

- **Section Name**

  Enter [MonitorSetting] as the section name.

- **Section Header**

  operation

    Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

  server_name

    Enter the server name (the value of "server_name" in the [Server] section).

ping_timeout

Enter the time-out value (in seconds) for ping control.
Enter a number from 5 to 3,600.

recovery_action

Enter a recovery process. Enter one of the following.

- Reboot

    "reboot"

- Reboot (Forced)

    "force_reboot"

- Switchover

    "switchover"

- Reboot and Switchover

    "reboot_and_switchover"

- Reboot (Forced) and Switchover

    "force_reboot_and_switchover"

reboot_count

Enter the number of times to reboot. Enter a number from 1 to 3.

Power Monitoring Device Data

- **Section Name**

Enter [PowerDevice] as the section name.

- **Section Header**

operation

Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

device_name

Enter the name that will be used to identify the power monitoring device.
Enter a character string beginning with an alphabetical character and containing up to 15 alphanumeric characters and hyphens ("-").

Note

Device names should be unique between all power monitoring devices. The names are case-sensitive.

ip_address

Enter the same IP address as that set on the power monitoring device.
Enter a string of numeric values (between 0 and 255) and periods.

Note

IP addresses should be unique between all resources.

snmp_community_name

Enter the same SNMP community (read-only permission) as that set on the power monitoring device.
Enter a string of up to 32 alphanumeric characters, underscores ("_"), and hyphens ("-").

voltage

Enter the voltage (V) that is being supplied to the power monitoring device. Enter a number between 10 and 999.

📒 Note

Resource Orchestrator calculates power consumption data using the electrical current value obtained from the power monitoring device and its specified voltage.

comment (optional)

Enter any comments for the power monitoring device.
Enter up to 128 alphanumeric characters or symbols (ASCII characters 0x20 to 0x7e).

📒 Note

A line break is counted as one character. Use "Alt+Enter" to enter line breaks.

Memo

- **Section Name**

    Enter [Memo] as the section name.
    This is required when registering the labels, comments, and contact information (displayed in BladeViewer) using the pre-configuration function.

- **Section Header**

    operation

    Enter the desired operation for the current line. Enter a hyphen ("-") to skip this line.

    resource_type

    Enter the type of the resource for which to set this memo. Enter one of the following.

    - When a physical server including a VM host is specified

        "physical_server"

    - When a VM guest is specified

        "vm_guest"

    - When contact information is specified

        "common"

    resource_name

    Enter the name of the resource name for which to set this memo. Enter one of the following.

    - When "resource_type" is "physical_server"

        Enter one of the following.

        - Server name ("server_name" of [ServerAgent] section)

        - VM host name ("server_name" of [ServerVMHost] section)

- When "resource_type" is "vm_guest"

  Enter the registered VM guest name

- When "resource_type" is "common"

  Do not enter any characters.

label (optional)

This label is used to identify the applications running on each server. Enter up to 32 alphanumeric characters or symbols (ASCII characters 0x20 to 0x7e). Note that if the value of "resource_type" is "common", do not enter anything.

Note
. . . .
Line breaks ("\n") are not available.
. . . .

comment (optional)

This is a comment that can be set as an option for each application. If the "resource_type" is "common", this can be used for the contact details, maintenance information, or other information. Enter up to 256 alphanumeric characters or symbols (ASCII characters 0x20 to 0x7e).

B.4 Examples of CSV Format

This section shows an example of the system configuration file in the CSV format.

```
RCXCSV,V3.5

# ServerView Resource Orchestrator
# System configuration file

[Subnet]
operation,subnet_name,network_address,subnet_mask,gateway
-,subnet1,172.16.0.0,255.255.0.0,172.16.0.1
-,subnet2,192.168.1.0,255.255.255.0,192.168.1.1

[VIOManager]
operation,name,ip_address,login_name,login_passwd,passwd_enc
-,VIOM,127.0.0.1,administrator,administrator,plain

[Chassis]
operation,chassis_name,ip_address,snmp_community_name
-,chassis01,192.168.3.150,public

[PRIMERGYPartitionModelChassis]
operation,chassis_name,ip_address,snmp_community_name,mgmt_user_name,mgmt_passwd,mgmt_passwd_enc
-,pqchassis0,192.168.3.207,public,administrator,administrator,plain
-,pqchassis1,192.168.3.208,public,administrator,administrator,plain

[SPARCEnterprisePartitionModelChassis]
operation,chassis_name,ip_address,snmp_community_name,mgmt_user_name,mgmt_passwd,mgmt_passwd_enc
-,spechassis,192.168.3.212,public,fujitsu,fujitsu,plain

[SPARCM10PartitionModelChassis]
operation,chassis_name,ip_address,snmp_community_name,mgmt_user_name,mgmt_passwd,mgmt_passwd_enc
-,sparcm10-1,192.168.10.26,public,xscf,Xk8n5z6MfEg=,encrypted

[LanSwitch]
operation,chassis_name,slot_no,switch_name,ip_address,snmp_community_name,user_name,passwd,passwd_enc,privile
```

ged_passwd,privileged_passwd_enc,product_name,connection_type
-,chassis01,1,switch-01,192.168.3.161,public,admin,admin,plain,admin,plain,BX600 GbE Switch Blade 30/12,telnet
-,chassis01,2,switch-02,192.168.3.162,public,admin,admin,plain,admin,plain,BX600 GbE Switch Blade 30/12,telnet

[LanSwitchNet]
operation,chassis_name,slot_no,port_no,vlan_id
-,chassis01,1,31,1/U;10/T;20/T
-,chassis01,1,32,1/U
-,chassis01,1,33,1/U
-,chassis01,1,34,1/U
-,chassis01,1,35,1/U
-,chassis01,1,36,1/U
-,chassis01,1,37,1/U
-,chassis01,1,38,1/U
-,chassis01,1,39,1/U
-,chassis01,1,40,1/U
-,chassis01,1,41,1/U
-,chassis01,1,42,1/U
-,chassis01,1,43,1/U
-,chassis01,1,44,1/U
-,chassis01,2,31,1/U;10/T;20/T
-,chassis01,2,32,1/U
-,chassis01,2,33,1/U
-,chassis01,2,34,1/U
-,chassis01,2,35,1/U
-,chassis01,2,36,1/U
-,chassis01,2,37,1/U
-,chassis01,2,38,1/U
-,chassis01,2,39,1/U
-,chassis01,2,40,1/U
-,chassis01,2,41,1/U
-,chassis01,2,42,1/U
-,chassis01,2,43,1/U
-,chassis01,2,44,1/U

[Server]
operation,chassis_name,slot_no,server_name,ip_address,mac_address,second_mac_address,snmp_community_name,ipmi_ip_address,ipmi_user_name,ipmi_passwd,ipmi_passwd_enc,admin_lan1_nic_number,admin_lan2_nic_number,admin_lan_nic_redundancy
-,chassis01,1,blade001,192.168.3.151,,,,,,,,,1,4,ON
-,chassis01,7,blade002,192.168.3.157,,,,,,,,,1,4,ON
-,chassis01,9,blade003,192.168.3.159,,,,,,,,,1,4,ON
-,,,rackmount001,192.168.3.200,00:E5:35:0C:34:AB,,public,192.168.3.199,admin,admin,plain,,,OFF
-,,,rackmount002,192.168.3.202,00:E5:35:0C:34:AC,,public,192.168.3.201,admin,admin,plain,,,OFF

[SPARC]
operation,server_name,ip_address,mgmt_snmp_community_name,mgmt_ip_address,mgmt_protocol,mgmt_user_name,mgmt_passwd,mgmt_passwd_enc
-,spe001,192.168.3.203,public,192.168.3.204,XSCF,fujitsu,fujitsu,plain
-,spe002,192.168.3.205,public,192.168.3.206,ILOM,fujitsu,fujitsu,plain

[SPARCM10]

operation,server_name,ip_address,mgmt_snmp_community_name,mgmt_ip_address,mgmt_protocol,mgmt_user_name,mgmt_passwd,mgmt_passwd_enc
-,Sparcm10-1-11,192.168.10.162,public,192.168.10.22,XSCF,xscf,Xk8n5z6MfEg=,encrypted
-,Sparcm10-1-12,192.168.10.163,public,192.168.10.23,XSCF,xscf,Xk8n5z6MfEg=,encrypted

[SPARCM10PartitionModelServer]
operation,chassis_name,partition_no,server_name,ip_address
-,sparcm10-1,0,sparcm10-1-0,192.168.10.166

[PRIMERGYPartitionModelServer]
operation,chassis_name,partition_no,server_name,ip_address,boot_option
-,pqchassis0,0,pqserver01,192.168.3.209,legacy
-,pqchassis0,1,pqserver02,192.168.3.210,legacy
-,pqchassis0,2,pqserver03,192.168.3.211,legacy

[ServerNet]
operation,server_name,nic_no,vlan_id
-,blade001,1,1/U;10/T;20/T
-,blade001,3,1/U
-,blade001,5,1/U
-,blade002,1,1/U;10/T;20/T
-,blade002,3,1/U
-,blade002,5,1/U
-,blade003,1,1/U
-,blade003,3,1/U
-,blade003,5,1/U
-,blade001,2,1/U
-,blade001,4,1/U
-,blade001,6,1/U
-,blade002,2,1/U
-,blade002,4,1/U
-,blade002,6,1/U
-,blade003,2,1/U
-,blade003,4,1/U
-,blade003,6,1/U

[SPARCEnterprisePartitionModelServer]
operation,chassis_name,partition_no,server_name,ip_address
-,spechassis,3,speserver3,192.168.3.213
-,spechassis,4,speserver4,192.168.3.214

[ServerWWNN]
operation,server_name,port_count,wwnn
-,blade001,1,20 00 00 17 42 51 00 01
-,blade002,1,20 00 00 17 42 51 00 02

[SpareServer]
operation,server_name,spare_server,vlan_switch,auto_switch,boot_type,spare_server_force_off,spare_server_with_vm_g
uest
-,blade001,blade003,ON,ON,local,OFF,OFF

[VMManager]
operation,name,ip_address,product,login_name,login_passwd,passwd_enc
-,vCenterServer,127.0.0.1,vmware-vc,Administrator,admin,plain

[ServerAgent]
operation,server_name
-,blade001
-,rackmount001
-,rackmount002

[ServerVMHost]
operation,server_name,vm_login_name,vm_login_passwd,vm_passwd_enc

-,blade002,admin,admin,plain

[MonitorSetting]
operation,server_name,ping_timeout,recovery_action,reboot_count
-,blade001,600,reboot_and_switchover,3

[PowerDevice]
operation,device_name,ip_address,snmp_community_name,voltage,comment
-,ups1,192.168.3.196,public,100,SmartUPS
-,ups2,192.168.3.197,public,100,SmartUPS

[Memo]
operation,resource_type,resource_name,label,comment
-,common,,,"TEL:0000-0000"

Appendix C Maintenance Mode

This appendix explains the maintenance mode available in Resource Orchestrator and how to use it.

Maintenance mode is used during hardware maintenance of managed servers. It is also used during the installation and maintenance of physical OSs and VM hosts. Maintenance mode avoids unwanted error notifications and disables execution of Auto-Recovery upon server failure.

The following operations can be performed on a server that has been placed into maintenance mode:

- Maintenance LED

  Maintenance LEDs can be controlled.

- Backup and restore

  System images can be backed up and restored.

- Cloning

  Cloning images can be collected and deployed.

Use the following procedures to set and release maintenance mode:

- Setting Maintenance Mode

  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.

- Releasing Maintenance Mode

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

Note

- When using ServerView Deployment Manager, depending on the operation, servers may be rebooted or temporarily shut down. This also affects servers managed using Resource Orchestrator.
  It is recommended to place affected servers into maintenance mode before running operations from ServerView Deployment Manager. Then, the maintenance mode should be released once finished.

- L-Servers cannot be created for physical servers that are in maintenance mode.